



Acunetix Website Audit
14 November, 2014

# **Executive Summary**

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

### Scan details

Scan information		
Starttime	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

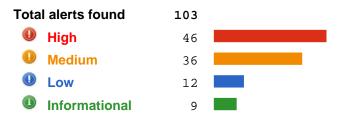
#### **Threat level**



#### **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



## **Executive summary**

Alert group	Severity	Alert count
Blind SQL Injection	High	3
Code execution	High	1
Cross site scripting	High	16
Cross site scripting (verified)	High	23
Directory traversal	High	1
SQL injection (verified)	High	2
Apache httpd remote denial of service	Medium	1
Application error message	Medium	2
Directory listing	Medium	19
HTML form without CSRF protection	Medium	7
Password field submitted using GET method	Medium	2
PHPinfo page found	Medium	1
User credentials are sent in clear text	Medium	4
Clickjacking: X-Frame-Options header missing	Low	1
Documentation file	Low	1
File upload	Low	1
Login page password-guessing attack	Low	1
Possible sensitive directories	Low	1
Possible sensitive files	Low	1

Sensitive page could be cached	Low	1
Session Cookie without HttpOnly flag set	Low	2
Session Cookie without Secure flag set	Low	2
TRACE method is enabled	Low	1
Email address found	Informational	1
Error page web server version disclosure	Informational	1
GHDB	Informational	5
Possible internal IP address disclosure	Informational	1
Possible username or password disclosure	Informational	1