acunetix WEB APPLICATION SECURITY

Acunetix Website Audit

31 October, 2014

Executive Summary

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

Scan of http://testphp.vulnweb.com:80/

Scan details

Scan information	
Starttime	31/10/2014 12:40:34
Finish time	31/10/2014 12:49:30
Scan time	8 minutes, 56 seconds
Profile	Default

Server information	
Responsive	True
Server banner	nginx/1.4.1
Server OS	Unknown
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	190
High	93
Medium	48
Low	8
Informational	41

Executive summary

Alert group	Severity	Alert count
Blind SQL Injection	High	26
CRLF injection/HTTP response splitting (verified)	High	1
Cross site scripting	High	2
Cross site scripting (verified)	High	29
Directory traversal (verified)	High	2
HTTP parameter pollution	High	2
PHP allow_url_fopen enabled	High	1
Script source code disclosure	High	1
Server side request forgery	High	2
SQL injection (verified)	High	26
Weak password	High	1
.htaccess file readable	Medium	1
Application error message	Medium	5
Backup files	Medium	2
Directory listing	Medium	14
Error message on page	Medium	7
HTML form without CSRF protection	Medium	6
Insecure crossdomain.xml file	Medium	1
JetBrains .idea project directory	Medium	1

PHP errors enabled	Medium	1
PHP open_basedir is not set	Medium	1
PHPinfo page found	Medium	2
Source code disclosure	Medium	2
URL redirection	Medium	1
User credentials are sent in clear text	Medium	2
User-controlled form action	Medium	1
WS_FTP log file found	Medium	1
Clickjacking: X-Frame-Options header missing	Low	1
Hidden form input named price was found	Low	1
Login page password-guessing attack	Low	1
Possible virtual host found	Low	1
Session Cookie without HttpOnly flag set	Low	2
Session Cookie without Secure flag set	Low	2
Broken links	Informational	7
Email address found	Informational	17
GHDB	Informational	5
Microsoft Office possible sensitive information	Informational	1
Password type input with auto-complete enabled	Informational	3
Possible internal IP address disclosure	Informational	3
Possible server path disclosure (Unix)	Informational	2
Possible username or password disclosure	Informational	3