acunetix

Executive Summary Report

Acunetix website audit

25 November 2016

WEB APPLICATION SECURITY

Generated by Acunetix Reporter

Scan of http://testphp.vulnweb.com

Scan details

Scan information	
Start time	17/11/2016, 19:22:12
Start url	http://testphp.vulnweb.com
Host	http://testphp.vulnweb.com
Scan time	14 minutes, 35 seconds
Profile	Full Scan

Threat level

Acunetix Threat Level 3

Alerts distribution

Total alerts found	151
High	75
Medium	48
Low	9
Informational	19

Executive summary

Alert group	Severity	Alert count
Blind SQL Injection	High	24
SQL injection	High	24
Cross site scripting	High	19
Directory traversal	High	1
Macromedia Dreamweaver remote database scripts	High	1
nginx SPDY heap buffer overflow	High	1
PHP allow_url_fopen enabled (AcuSensor)	High	1
Remote file inclusion XSS	High	1
Script source code disclosure	High	1
Server side request forgery	High	1
Weak password	High	1
Directory listing	Medium	12
Error message on page	Medium	7
HTML form without CSRF protection	Medium	6
Application error message	Medium	5
Backup files	Medium	2
HTTP parameter pollution	Medium	2
Source code disclosure	Medium	2
User credentials are sent in clear text	Medium	2
.htaccess file readable	Medium	1
CRLF injection/HTTP response splitting	Medium	1
Cross domain data hijacking	Medium	1
Cross site scripting (content-sniffing)	Medium	1
Insecure crossdomain.xml file	Medium	1

JetBrains .idea project directory	Medium	1
PHP errors enabled (AcuSensor)	Medium	1
PHPinfo page found	Medium	1
URL redirection	Medium	1
WS_FTP log file found	Medium	1
Possible sensitive directories	Low	3
MySQL username disclosure	Low	2
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