



Lex_Retail Web Application Test

Report generated by Tenable Nessus™

Thu, 31 Jul 2025 14:20:48 EDT

TABLE OF CONTENTS

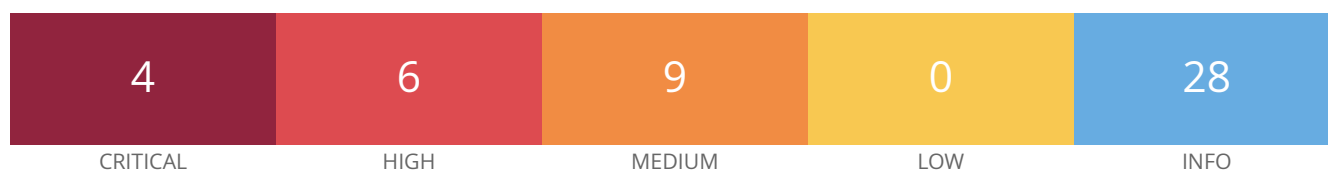
Vulnerabilities by Host

• 192.168.8.250.....	4
----------------------	---

Nessus Essentials

Vulnerabilities by Host

192.168.8.250



Vulnerabilities

Total: 47

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
CRITICAL	9.8	7.7	0.9355	201198	Apache 2.4.x < 2.4.60 Multiple Vulnerabilities
CRITICAL	9.8	9.6	0.9441	200162	PHP 8.2.x < 8.2.20 Multiple Vulnerabilities
CRITICAL	9.8	6.7	0.0014	211671	PHP 8.2.x < 8.2.26 Multiple Vulnerabilities
CRITICAL	9.1	6.0	0.1077	201082	OpenSSL 3.1.0 < 3.1.7 Vulnerability
HIGH	8.8	5.9	0.0217	207822	PHP 8.2.x < 8.2.24 Multiple Vulnerabilities
HIGH	8.6	3.4	0.0013	232707	PHP 8.2.x < 8.2.28 Multiple Vulnerabilities
HIGH	7.5	4.4	0.9036	192923	Apache 2.4.x < 2.4.59 Multiple Vulnerabilities
HIGH	7.5	3.6	0.0044	210450	Apache 2.4.x < 2.4.62 Multiple Vulnerabilities (Windows)
HIGH	7.5	4.4	0.0573	183890	OpenSSL 3.1.0 < 3.1.4 Vulnerability
HIGH	7.5	4.4	0.0165	192974	OpenSSL 3.1.0 < 3.1.6 Multiple Vulnerabilities
MEDIUM	6.5	5.0	0.0274	185161	OpenSSL 3.1.0 < 3.1.5 Multiple Vulnerabilities
MEDIUM	6.5	6.3	0.5461	193191	PHP 8.2.x < 8.2.18 Multiple Vulnerabilities
MEDIUM	5.3	-	-	10678	Apache mod_info /server-info Information Disclosure
MEDIUM	5.3	-	-	10677	Apache mod_status /server-status Information Disclosure
MEDIUM	5.3	-	-	40984	Browsable Web Directories
MEDIUM	5.3	4.0	0.7993	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	4.3	2.2	0.0036	209154	OpenSSL 3.1.0 < 3.1.8 Vulnerability
MEDIUM	5.0*	-	-	46803	PHP expose_php Information Disclosure
MEDIUM	4.3*	-	-	85582	Web Application Potentially Vulnerable to Clickjacking

INFO	N/A	-	-	48204	Apache HTTP Server Version
INFO	N/A	-	-	47830	CGI Generic Injectable Parameter
INFO	N/A	-	-	33817	CGI Generic Tests Load Estimation (all tests)
INFO	N/A	-	-	39470	CGI Generic Tests Timeout
INFO	N/A	-	-	19689	Embedded Web Server Detection
INFO	N/A	-	-	49704	External URLs
INFO	N/A	-	-	84502	HSTS Missing From HTTPS Server
INFO	N/A	-	-	69826	HTTP Cookie 'secure' Property Transport Mismatch
INFO	N/A	-	-	43111	HTTP Methods Allowed (per directory)
INFO	N/A	-	-	10107	HTTP Server Type and Version
INFO	N/A	-	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	-	91634	HyperText Transfer Protocol (HTTP) Redirect Information
INFO	N/A	-	-	50344	Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header
INFO	N/A	-	-	50345	Missing or Permissive X-Frame-Options HTTP Response Header
INFO	N/A	-	-	11219	Nessus SYN scanner
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	57323	OpenSSL Version Detection
INFO	N/A	-	-	48243	PHP Version Detection
INFO	N/A	-	-	66334	Patch Report
INFO	N/A	-	-	49069	Splunk Management API Detection
INFO	N/A	-	-	47619	Splunk Web Detection
INFO	N/A	-	-	85602	Web Application Cookies Not Marked Secure
INFO	N/A	-	-	91815	Web Application Sitemap
INFO	N/A	-	-	11032	Web Server Directory Enumeration
INFO	N/A	-	-	49705	Web Server Harvested Email Addresses

INFO	N/A	-	-	11419	Web Server Office File Inventory
INFO	N/A	-	-	10662	Web mirroring
INFO	N/A	-	-	17219	phpMyAdmin Detection

* indicates the v3.0 score was not available; the v2.0 score is shown