



DVWA web scanning

Report generated by Tenable Nessus™

Mon, 31 Mar 2025 13:03:57 EDT

TABLE OF CONTENTS

Vulnerabilities by Host

• 192.168.235.134.....	4
------------------------	---

Nessus Essentials

Vulnerabilities by Host

192.168.235.134



Vulnerabilities

Total: 114

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
CRITICAL	9.8	8.9	0.8897	45004	Apache 2.2.x < 2.2.15 Multiple Vulnerabilities
CRITICAL	9.8	6.7	0.7044	100995	Apache 2.2.x < 2.2.33-dev / 2.4.x < 2.4.26 Multiple Vulnerabilities
CRITICAL	9.8	6.7	0.7044	101787	Apache 2.2.x < 2.2.34 Multiple Vulnerabilities
CRITICAL	9.8	6.7	0.71	158900	Apache 2.4.x < 2.4.53 Multiple Vulnerabilities
CRITICAL	9.8	6.7	0.0004	193421	Apache 2.4.x < 2.4.54 Authentication Bypass
CRITICAL	9.8	6.7	0.9002	172186	Apache 2.4.x < 2.4.56 Multiple Vulnerabilities
CRITICAL	9.8	6.7	0.4003	153584	Apache < 2.4.49 Multiple Vulnerabilities
CRITICAL	9.8	7.4	0.0835	45039	OpenSSL 0.9.8 < 0.9.8m Multiple Vulnerabilities
CRITICAL	9.8	5.9	0.0343	200190	OpenSSL 0.9.8 < 0.9.8p Vulnerability
CRITICAL	9.8	5.9	0.155	57459	OpenSSL 0.9.8 < 0.9.8s Multiple Vulnerabilities
CRITICAL	9.8	6.7	0.0628	58799	OpenSSL 0.9.8 < 0.9.8v Vulnerability
CRITICAL	9.8	3.6	0.3256	78552	OpenSSL 0.9.8 < 0.9.8zc Multiple Vulnerabilities
CRITICAL	9.8	5.9	0.1678	200191	OpenSSL 0.9.8h < 0.9.8o Vulnerability
CRITICAL	9.8	5.9	0.0172	125855	phpMyAdmin prior to 4.8.6 SQLi vulnerability (PMASA-2019-3)
CRITICAL	9.1	5.2	0.0054	161948	Apache 2.4.x < 2.4.54 Multiple Vulnerabilities
CRITICAL	9.1	5.2	0.0167	200193	OpenSSL 0.9.8h < 0.9.8r Vulnerability
CRITICAL	9.0	6.5	0.2314	170113	Apache 2.4.x < 2.4.55 Multiple Vulnerabilities
CRITICAL	9.0	8.1	0.9443	153583	Apache < 2.4.49 Multiple Vulnerabilities
CRITICAL	10.0	-	-	171356	Apache HTTP Server SEoL (2.1.x <= x <= 2.2.x)

CRITICAL	10.0	-	-	58987	PHP Unsupported Version Detection
CRITICAL	10.0*	7.3	0.5723	55925	PHP 5.3 < 5.3.7 Multiple Vulnerabilities
CRITICAL	10.0*	5.9	0.505	60085	PHP 5.3.x < 5.3.15 Multiple Vulnerabilities
HIGH	8.3	-	-	42424	CGI Generic SQL Injection (blind)
HIGH	7.5	3.6	0.5469	193422	Apache 2.4.x < 2.4.54 HTTP Request Smuggling Vulnerability
HIGH	7.5	3.6	0.1508	193423	Apache 2.4.x < 2.4.54 Multiple Vulnerabilities
HIGH	7.5	3.6	0.0139	193424	Apache 2.4.x < 2.4.54 Multiple Vulnerabilities (mod_lua)
HIGH	7.5	4.4	0.8196	183391	Apache 2.4.x < 2.4.58 Multiple Vulnerabilities
HIGH	7.5	4.4	0.0035	193419	Apache 2.4.x < 2.4.58 Out-of-Bounds Read (CVE-2023-31122)
HIGH	7.5	4.4	0.8849	192923	Apache 2.4.x < 2.4.59 Multiple Vulnerabilities
HIGH	7.5	4.4	0.2191	45359	OpenSSL 0.9.8 < 0.9.8n Multiple Vulnerabilities
HIGH	7.5	3.6	0.0589	200204	OpenSSL 0.9.8 < 0.9.8q Vulnerability
HIGH	7.5	3.6	0.0335	58564	OpenSSL 0.9.8 < 0.9.8u Vulnerability
HIGH	7.5	5.9	0.0608	59076	OpenSSL 0.9.8 < 0.9.8x Vulnerability
HIGH	7.5	3.6	0.0415	64532	OpenSSL 0.9.8 < 0.9.8y Multiple Vulnerabilities
HIGH	7.5	3.6	0.6603	77086	OpenSSL 0.9.8 < 0.9.8zb Multiple Vulnerabilities
HIGH	7.5	3.6	0.3162	82030	OpenSSL 0.9.8 < 0.9.8zf Multiple Vulnerabilities
HIGH	7.5	3.6	0.1522	84151	OpenSSL 0.9.8 < 0.9.8zg Multiple Vulnerabilities
HIGH	7.5	-	-	142591	PHP < 7.3.24 Multiple Vulnerabilities
HIGH	7.4	7.7	0.9226	74363	OpenSSL 0.9.8 < 0.9.8za Multiple Vulnerabilities
HIGH	7.3	6.7	0.8915	77531	Apache 2.2.x < 2.2.28 Multiple Vulnerabilities
HIGH	7.3	5.9	0.0333	66584	PHP 5.3.x < 5.3.23 Multiple Vulnerabilities
HIGH	7.3	4.2	0.4829	71426	PHP 5.3.x < 5.3.28 Multiple OpenSSL Vulnerabilities
HIGH	7.3	6.0	0.5625	77285	PHP 5.3.x < 5.3.29 Multiple Vulnerabilities
HIGH	7.0	5.9	0.0732	62101	Apache 2.2.x < 2.2.23 Multiple Vulnerabilities

HIGH	7.6*	5.9	0.0343	17766	OpenSSL < 0.9.8p / 1.0.0b Buffer Overflow
HIGH	9.3*	6.7	0.0868	48245	PHP 5.3 < 5.3.3 Multiple Vulnerabilities
HIGH	7.5*	6.7	0.1729	52717	PHP 5.3 < 5.3.6 Multiple Vulnerabilities
HIGH	7.5*	7.4	0.926	59056	PHP 5.3.x < 5.3.13 CGI Query String Code Execution
HIGH	7.5*	7.3	0.1383	59529	PHP 5.3.x < 5.3.14 Multiple Vulnerabilities
HIGH	7.5*	5.9	0.0333	64992	PHP 5.3.x < 5.3.22 Multiple Vulnerabilities
HIGH	7.5*	8.9	0.9442	58988	PHP < 5.3.12 / 5.4.2 CGI Query String Code Execution
HIGH	7.5*	6.3	0.8836	57537	PHP < 5.3.9 Multiple Vulnerabilities
HIGH	7.5*	-	-	40352	phpMyAdmin Installation Not Password Protected
MEDIUM	5.6	5.9	0.4044	68915	Apache 2.2.x < 2.2.25 Multiple Vulnerabilities
MEDIUM	5.3	3.6	0.3052	48205	Apache 2.2.x < 2.2.16 Multiple Vulnerabilities
MEDIUM	5.3	4.4	0.2395	50070	Apache 2.2.x < 2.2.17 Multiple Vulnerabilities
MEDIUM	5.3	4.4	0.3109	53896	Apache 2.2.x < 2.2.18 APR apr_fnmatch DoS
MEDIUM	5.3	2.2	0.5232	56216	Apache 2.2.x < 2.2.21 mod_proxy_ajp DoS
MEDIUM	5.3	6.7	0.9023	57791	Apache 2.2.x < 2.2.22 Multiple Vulnerabilities
MEDIUM	5.3	3.0	0.6143	64912	Apache 2.2.x < 2.2.24 Multiple XSS Vulnerabilities
MEDIUM	5.3	1.4	0.3783	73405	Apache 2.2.x < 2.2.27 Multiple Vulnerabilities
MEDIUM	5.3	1.4	0.0019	193420	Apache 2.4.x < 2.4.54 Out-Of-Bounds Read (CVE-2022-28330)
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	0.8269	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.3	3.6	0.9284	80566	OpenSSL 0.9.8 < 0.9.8zd Multiple Vulnerabilities
MEDIUM	5.3	2.2	0.0204	87219	OpenSSL 0.9.8 < 0.9.8zh Vulnerability
MEDIUM	5.3	-	-	152853	PHP < 7.3.28 Email Header Injection

MEDIUM	5.0*	-	-	33821	.svn/entries Disclosed via Web Server
MEDIUM	5.0*	-	-	11411	Backup Files Disclosure
MEDIUM	5.0*	-	-	10188	Multiple Web Server printenv CGI Information Disclosure
MEDIUM	4.3*	4.2	0.1413	17767	OpenSSL < 0.9.8p / 1.0.0e Double Free Vulnerability
MEDIUM	5.0*	4.4	0.1503	51439	PHP 5.2 < 5.2.17 / 5.3 < 5.3.5 String To Double Conversion DoS
MEDIUM	6.8*	6.7	0.3303	51140	PHP 5.3 < 5.3.4 Multiple Vulnerabilities
MEDIUM	5.0*	3.6	0.2356	66842	PHP 5.3.x < 5.3.26 Multiple Vulnerabilities
MEDIUM	6.8*	5.9	0.2032	67259	PHP 5.3.x < 5.3.27 Multiple Vulnerabilities
MEDIUM	6.8*	6.7	0.1605	58966	PHP < 5.3.11 Multiple Vulnerabilities
MEDIUM	6.4*	5.3	0.0557	44921	PHP < 5.3.2 / 5.2.13 Multiple Vulnerabilities
MEDIUM	5.0*	3.4	0.0016	73289	PHP PHP_RSHUTDOWN_FUNCTION Security Bypass
MEDIUM	5.0*	-	-	46803	PHP expose_php Information Disclosure
MEDIUM	5.0*	-	-	57640	Web Application Information Disclosure
MEDIUM	4.3*	-	-	85582	Web Application Potentially Vulnerable to Clickjacking
MEDIUM	4.3*	3.8	0.0823	51425	phpMyAdmin error.php BBcode Tag XSS (PMASA-2010-9)
MEDIUM	4.3*	3.0	0.0039	49142	phpMyAdmin setup.php Verbose Server Name XSS (PMASA-2010-10)
INFO	N/A	-	-	48204	Apache HTTP Server Version
INFO	N/A	-	-	40406	CGI Generic Tests HTTP Errors
INFO	N/A	-	-	33817	CGI Generic Tests Load Estimation (all tests)
INFO	N/A	-	-	39470	CGI Generic Tests Timeout
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	-	-	11149	HTTP login page
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	-	-	100669	Web Application Cookies Are Expired
INFO	N/A	-	-	85601	Web Application Cookies Not Marked HttpOnly
INFO	N/A	-	-	85602	Web Application Cookies Not Marked Secure
INFO	N/A	-	-	40773	Web Application Potentially Sensitive CGI Parameter Detection
INFO	N/A	-	-	91815	Web Application Sitemap
INFO	N/A	-	-	11032	Web Server Directory Enumeration
INFO	N/A	-	-	10302	Web Server robots.txt Information Disclosure
INFO	N/A	-	-	10662	Web mirroring
INFO	N/A	-	-	11424	WebDAV Detection
INFO	N/A	-	-	17219	phpMyAdmin Detection

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