tenable Nessus

Report generated by Nessus™

Lab1 DVWA Web

Wed, 17 Apr 2024 23:14:34 PDT

TABLE OF CONTENTS

Vulnerabilities by Host

Collapse All | Expand All

10.0.2.5

14	23	41	3	28
CRITICAL	HIGH	MEDIUM	LOW	INFO

Severity	CVSS v3.0	VPR Score	Plugin	Name

CRITICAL	9.8	9.2	45004	Apache 2.2.x < 2.2.15 Multiple Vulnerabilities
CRITICAL	9.8	6.7	100995	Apache 2.2.x < 2.2.33-dev / 2.4.x < 2.4.26 Multiple Vulnerabilities
CRITICAL	9.8	6.7	101787	Apache 2.2.x < 2.2.34 Multiple Vulnerabilities
CRITICAL	9.8	6.7	158900	Apache 2.4.x < 2.4.53 Multiple Vulnerabilities
CRITICAL	9.8	5.9	193421	Apache 2.4.x < 2.4.54 Authentication Bypass
CRITICAL	9.8	6.7	172186	Apache 2.4.x < 2.4.56 Multiple Vulnerabilities
CRITICAL	9.8	6.7	153584	Apache < 2.4.49 Multiple Vulnerabilities
CRITICAL	9.8	5.9	125855	phpMyAdmin prior to 4.8.6 SQLi vulnerablity (PMASA-2019-3)
CRITICAL	9.0	6.5	170113	Apache 2.4.x < 2.4.55 Multiple Vulnerabilities
CRITICAL	9.0	8.1	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*	6.1	55925	PHP 5.3 < 5.3.7 Multiple Vulnerabilities
CRITICAL	10.0*	5.9	60085	PHP 5.3.x < 5.3.15 Multiple Vulnerabilities
HIGH	7.5	3.6	193422	Apache 2.4.x < 2.4.54 HTTP Request Smuggling Vulnerability
HIGH	7.5	3.6	193423	Apache 2.4.x < 2.4.54 Multiple Vulnerabilities
HIGH	7.5	4.4	193424	Apache 2.4.x < 2.4.54 Multiple Vulnerabilities (mod_lua)
HIGH	7.5	4.4	183391	Apache 2.4.x < 2.4.58 Multiple Vulnerabilities

HIGH	7.5	4.4	193419	Apache 2.4.x < 2.4.58 Out-of-Bounds Read (CVE-2022-31122)
HIGH	7.5	4.4	192923	Apache 2.4.x < 2.4.59 Multiple Vulnerabilities
HIGH	7.5	-	142591	PHP < 7.3.24 Multiple Vulnerabilities
HIGH	7.3	6.7	77531	Apache 2.2.x < 2.2.28 Multiple Vulnerabilities
HIGH	7.3	5.9	66584	PHP 5.3.x < 5.3.23 Multiple Vulnerabilities
HIGH	7.3	6.7	71426	PHP 5.3.x < 5.3.28 Multiple OpenSSL Vulnerabilities
HIGH	7.3	5.9	77285	PHP 5.3.x < 5.3.29 Multiple Vulnerabilities
HIGH	7.0	5.9	62101	Apache 2.2.x < 2.2.23 Multiple Vulnerabilities
HIGH	7.6*	5.9	17766	OpenSSL < 0.9.8p / 1.0.0b Buffer Overflow
HIGH	9.3*	5.9	57459	OpenSSL < 0.9.8s Multiple Vulnerabilities
HIGH	7.5*	6.7	58799	OpenSSL < 0.9.8w ASN.1 asn1_d2i_read_bio Memory Corruption
HIGH	9.3*	6.7	48245	PHP 5.3 < 5.3.3 Multiple Vulnerabilities
HIGH	7.5*	6.7	52717	PHP 5.3 < 5.3.6 Multiple Vulnerabilities
HIGH	7.5*	7.4	59056	PHP 5.3.x < 5.3.13 CGI Query String Code Execution
HIGH	7.5*	6.7	59529	PHP 5.3.x < 5.3.14 Multiple Vulnerabilities
HIGH	7.5*	5.9	64992	PHP 5.3.x < 5.3.22 Multiple Vulnerabilities
HIGH	7.5*	8.9	58988	PHP < 5.3.12 / 5.4.2 CGI Query String Code Execution
HIGH	7.5*	6.3	57537	PHP < 5.3.9 Multiple Vulnerabilities

HIGH	7.5*	-	40352	phpMyAdmin Installation Not Password Protected
MEDIUM	5.6	3.4	68915	Apache 2.2.x < 2.2.25 Multiple Vulnerabilities
MEDIUM	5.3	3.6	48205	Apache 2.2.x < 2.2.16 Multiple Vulnerabilities
MEDIUM	5.3	4.4	50070	Apache 2.2.x < 2.2.17 Multiple Vulnerabilities
MEDIUM	5.3	2.9	53896	Apache 2.2.x < 2.2.18 APR apr_fnmatch DoS
MEDIUM	5.3	2.2	56216	Apache 2.2.x < 2.2.21 mod_proxy_ajp DoS
MEDIUM	5.3	6.6	57791	Apache 2.2.x < 2.2.22 Multiple Vulnerabilities
MEDIUM	5.3	3.0	64912	Apache 2.2.x < 2.2.24 Multiple XSS Vulnerabilities
MEDIUM	5.3	1.4	73405	Apache 2.2.x < 2.2.27 Multiple Vulnerabilities
MEDIUM	5.3	5.2	161948	Apache 2.4.x < 2.4.54 Multiple Vulnerabilities
MEDIUM	5.3	1.4	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	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.3	2.2	87219	OpenSSL 0.9.8 < 0.9.8zh X509_ATTRIBUTE Memory Leak DoS
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	4.3*	-	44136	CGI Generic Cookie Injection Scripting
MEDIUM	4.3*	-	49067	CGI Generic HTML Injections (quick test)
MEDIUM	4.3*	-	39466	CGI Generic XSS (quick test)
MEDIUM	5.0*	-	10188	Multiple Web Server printenv CGI Information Disclosure
MEDIUM	5.0*	5.9	59076	OpenSSL 0.9.8 < 0.9.8x DTLS CBC Denial of Service
MEDIUM	6.8*	7.7	74363	OpenSSL 0.9.8 < 0.9.8za Multiple Vulnerabilities
MEDIUM	4.3*	3.6	77086	OpenSSL 0.9.8 < 0.9.8zb Multiple Vulnerabilities
MEDIUM	5.0*	4.5	80566	OpenSSL 0.9.8 < 0.9.8zd Multiple Vulnerabilities (FREAK)
MEDIUM	6.8*	5.2	82030	OpenSSL 0.9.8 < 0.9.8zf Multiple Vulnerabilities
MEDIUM	6.8*	5.9	84151	OpenSSL 0.9.8 < 0.9.8zg Multiple Vulnerabilities
MEDIUM	4.3*	4.2	17767	OpenSSL < 0.9.8p / 1.0.0e Double Free Vulnerability
MEDIUM	5.0*	3.6	58564	OpenSSL < 0.9.8u Multiple Vulnerabilities
MEDIUM	5.0*	4.4	51439	PHP 5.2 < 5.2.17 / 5.3 < 5.3.5 String To Double Conversion DoS
MEDIUM	6.8*	6.7	51140	PHP 5.3 < 5.3.4 Multiple Vulnerabilities
MEDIUM	5.0*	3.6	66842	PHP 5.3.x < 5.3.26 Multiple Vulnerabilities
MEDIUM	6.8*	5.9	67259	PHP 5.3.x < 5.3.27 Multiple Vulnerabilities
MEDIUM	6.8*	6.7	58966	PHP < 5.3.11 Multiple Vulnerabilities

MEDIUM	6.4*	5.3	44921	PHP < 5.3.2 / 5.2.13 Multiple Vulnerabilities
MEDIUM	5.0*	3.4	73289	PHP PHP_RSHUTDOWN_FUNCTION Security Bypass
MEDIUM	5.0*	-	46803	PHP expose_php Information Disclosure
MEDIUM	4.3*	-	85582	Web Application Potentially Vulnerable to Clickjacking
MEDIUM	4.3*	3.8	51425	phpMyAdmin error.php BBcode Tag XSS (PMASA-2010-9)
MEDIUM	4.3*	3.0	49142	phpMyAdmin setup.php Verbose Server Name XSS (PMASA-2010-7)
LOW	3.4	5.1	78552	OpenSSL 0.9.8 < 0.9.8zc Multiple Vulnerabilities (POODLE)
LOW	2.6*	3.6	64532	OpenSSL < 0.9.8y Multiple Vulnerabilities
LOW	2.6*	-	26194	Web Server Transmits Cleartext Credentials
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	-	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	-	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

Hide