



Lab1 DVWA Network

Wed, 17 Apr 2024 13:43:05 PDT

TABLE OF CONTENTS

Vulnerabilities by Host

- 10.0.2.5

Vulnerabilities by Host

[Collapse All](#) | [Expand All](#)

10.0.2.5



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	161948	Apache 2.4.x < 2.4.54 Multiple Vulnerabilities
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	-	20007	SSL Version 2 and 3 Protocol Detection
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	-	33850	Unix Operating System 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	4.4	183391	Apache 2.4.x < 2.4.58 Multiple Vulnerabilities
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	7.5	4.9	35291	SSL Certificate Signed Using Weak Hashing Algorithm
HIGH	7.5	6.1	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
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
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted

MEDIUM	6.5	-	57582	SSL Self-Signed Certificate
MEDIUM	6.5	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	5.9	4.4	89058	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)
MEDIUM	5.9	3.6	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
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	-	10678	Apache mod_info /server-info Information Disclosure
MEDIUM	5.3	-	10677	Apache mod_status /server-status Information Disclosure
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	5.3	-	15901	SSL Certificate Expiry

MEDIUM	5.3	-	26928	SSL Weak Cipher Suites Supported
MEDIUM	5.0*	-	33821	.svn/entries Disclosed via Web Server
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	4.3*	4.5	81606	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)
LOW	3.7	3.9	83875	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)
LOW	3.7	3.9	83738	SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)
LOW	3.4	5.1	78552	OpenSSL 0.9.8 < 0.9.8zc Multiple Vulnerabilities (POODLE)
LOW	3.4	5.1	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
LOW	2.6*	3.6	64532	OpenSSL < 0.9.8y Multiple Vulnerabilities
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	48204	Apache HTTP Server Version
INFO	N/A	-	39520	Backported Security Patch Detection (SSH)
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	54615	Device Type
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	10092	FTP Server Detection
INFO	N/A	-	84502	HSTS Missing From HTTPS Server
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	10719	MySQL Server Detection

INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	181418	OpenSSH Detection
INFO	N/A	-	50845	OpenSSL Detection
INFO	N/A	-	57323	OpenSSL Version Detection
INFO	N/A	-	48243	PHP Version Detection
INFO	N/A	-	66334	Patch Report
INFO	N/A	-	10267	SSH Server Type and Version Information
INFO	N/A	-	56984	SSL / TLS Versions Supported
INFO	N/A	-	10863	SSL Certificate Information
INFO	N/A	-	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	-	21643	SSL Cipher Suites Supported
INFO	N/A	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	94761	SSL Root Certification Authority Certificate Information
INFO	N/A	-	51891	SSL Session Resume Supported
INFO	N/A	-	156899	SSL/TLS Recommended Cipher Suites

INFO	N/A	-	22964	Service Detection
INFO	N/A	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	10302	Web Server robots.txt Information Disclosure
INFO	N/A	-	11424	WebDAV Detection

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

Hide