WebApp Scan

Report generated by Nessus™ Sat, 01 Apr 2023 05:59:05 EDT

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

192.168.56.102

16	17	18	5	33
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 89

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
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	7.4	158900	Apache 2.4.x < 2.4.53 Multiple Vulnerabilities
CRITICAL	9.8	7.4	161948	Apache 2.4.x < 2.4.54 Multiple Vulnerabilities
CRITICAL	9.8	9.2	172186	Apache 2.4.x < 2.4.56 Multiple Vulnerabilities
CRITICAL	9.8	7.4	153584	Apache < 2.4.49 Multiple Vulnerabilities
CRITICAL	9.8	5.9	95438	Apache Tomcat 6.0.x < 6.0.48 / 7.0.x < 7.0.73 / 8.0.x < 8.0.39 / 8.5.x < 8.5.8 / 9.0.x < 9.0.0.M13 Multiple Vulnerabilities
CRITICAL	9.8	6.7	111067	Apache Tomcat 8.0.0 < 8.0.53 Security Constraint Weakness
CRITICAL	9.8	8.9	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.1	5.2	121120	Apache Tomcat 7.0.x < 7.0.76 / 8.0.x < 8.0.42 / 8.5.x < 8.5.12 / 9.0.x < 9.0.0.M18 Improper Access Control
CRITICAL	9.0	7.3	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	-	171342	Apache Tomcat Web Server SEoL (8.0.x)
CRITICAL	10.0	-	171356	Apache httpd SEoL (2.1.x <= x <= 2.2.x)
CRITICAL	10.0	-	58987	PHP Unsupported Version Detection
CRITICAL	10.0*	5.9	60085	PHP 5.3.x < 5.3.15 Multiple Vulnerabilities
HIGH	8.1	9.2	103697	Apache Tomcat 8.0.0.RC1 < 8.0.47 Multiple Vulnerabilities

HIGH	7.5	3.6	96003	Apache Tomcat 6.0.16 < 6.0.50 / 7.0.x < 7.0.75 / 8.0.x < 8.0.41 / 8.5.x < 8.5.9 / 9.0.x < 9.0.0.M15 NIO HTTP Connector Information Disclosure
HIGH	7.5	6.0	94578	Apache Tomcat 6.0.x < 6.0.47 / 7.0.x < 7.0.72 / 8.0.x < 8.0.37 / 8.5.x < 8.5.5 / 9.0.x < 9.0.0.M10 Multiple Vulnerabilities
HIGH	7.5	3.6	99367	Apache Tomcat 6.0.x < 6.0.53 / 7.0.x < 7.0.77 / 8.0.x < 8.0.43 Pipelined Requests Information Disclosure
HIGH	7.5	3.6	121119	Apache Tomcat 7.0.x < 7.0.70 / 8.0.x < 8.0.36 / 8.5.x < 8.5.3 / 9.0.x < 9.0.0.M8 Denial of Service
HIGH	7.5	4.4	100681	Apache Tomcat 7.0.x < 7.0.78 / 8.0.x < 8.0.44 / 8.5.x < 8.5.15 / 9.0.x < 9.0.0.M21 Remote Error Page Manipulation
HIGH	7.5	3.6	121124	Apache Tomcat 8.0.x < 8.0.52 / 8.5.x < 8.5.31 / 9.0.x < 9.0.8 Denial of Service
HIGH	7.5	-	142591	PHP < 7.3.24 Multiple Vulnerabilities
HIGH	7.3	8.4	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	6.7	77285	PHP 5.3.x < 5.3.29 Multiple Vulnerabilities
HIGH	7.0	6.7	62101	Apache 2.2.x < 2.2.23 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
MEDIUM	6.1	3.8	10815	Web Server Generic XSS
MEDIUM	5.6	4.2	68915	Apache 2.2.x < 2.2.25 Multiple Vulnerabilities
MEDIUM	5.3	8.3	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	-	12085	Apache Tomcat Default Files
MEDIUM	5.3	-	40984	Browsable Web Directories
MEDIUM	5.3	4.0	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.3	-	152853	PHP < 7.3.28 Email Header Injection
MEDIUM	4.3	1.4	102588	Apache Tomcat 8.0.0.RC1 < 8.0.45 Cache Poisoning
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	5.0*	3.4	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	5.0*	-	90067	WordPress User Enumeration
LOW	3.7	4.4	106976	Apache Tomcat 8.0.0.RC1 < 8.0.50 Security Constraint Weakness
LOW	3.7	2.2	159462	Apache Tomcat 8.x < 8.5.78 Spring4Shell (CVE-2022-22965) Mitigations
LOW	N/A	-	42057	Web Server Allows Password Auto-Completion
LOW	2.6*	-	26194	Web Server Transmits Cleartext Credentials
LOW	2.6*	-	34850	Web Server Uses Basic Authentication Without HTTPS
INFO	N/A	-	46739	Apache Axis2 Detection
INFO	N/A	-	48204	Apache HTTP Server Version
INFO	N/A	-	39446	Apache Tomcat Detection
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	-	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	-	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	-	14274	Nessus SNMP Scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	48243	PHP Version Detection
INFO	N/A	-	66334	Patch Report
INFO	N/A	-	40665	Protected Web Page Detection
INFO	N/A	-	72771	Web Accessible Backups
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	-	20108	Web Server / Application favicon.ico Vendor Fingerprinting
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	-	11422	Web Server Unconfigured - Default Install Page Present
INFO	N/A	-	10662	Web mirroring
INFO	N/A	-	11424	WebDAV Detection
INFO	N/A	-	24004	WebDAV Directory Enumeration
INFO	N/A	-	18297	WordPress Detection
INFO	N/A	-	101841	WordPress Outdated Plugin Detection

INFO	N/A	-	101842	WordPress Plugin Detection

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

192.168.56.103

Vulnerabilities Total: 66

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	9.8	81510	PHP 5.4.x < 5.4.38 Multiple Vulnerabilities (GHOST)
CRITICAL	9.8	8.8	82025	PHP 5.4.x < 5.4.39 Multiple Vulnerabilities
CRITICAL	9.8	6.7	83033	PHP 5.4.x < 5.4.40 Multiple Vulnerabilities
CRITICAL	9.8	6.7	83517	PHP 5.4.x < 5.4.41 Multiple Vulnerabilities
CRITICAL	9.8	6.7	84362	PHP 5.4.x < 5.4.42 Multiple Vulnerabilities
CRITICAL	9.8	5.9	84671	PHP 5.4.x < 5.4.43 Multiple Vulnerabilities (BACKRONYM)
CRITICAL	9.8	5.9	125855	phpMyAdmin prior to 4.8.6 SQLi vulnerablity (PMASA-2019-3)
CRITICAL	10.0	-	58987	PHP Unsupported Version Detection
CRITICAL	10.0*	-	92626	Drupal Coder Module Deserialization RCE
HIGH	7.5	-	142591	PHP < 7.3.24 Multiple Vulnerabilities
HIGH	7.3	5.9	66585	PHP 5.4.x < 5.4.13 Information Disclosure
HIGH	7.3	5.9	69401	PHP 5.4.x < 5.4.19 Multiple Vulnerabilities
HIGH	7.3	6.7	81080	PHP 5.4.x < 5.4.37 Multiple Vulnerabilities
HIGH	7.3	4.4	85298	PHP 5.4.x < 5.4.44 Multiple Vulnerabilities
HIGH	7.3	6.7	85885	PHP 5.4.x < 5.4.45 Multiple Vulnerabilities
HIGH	7.5*	7.4	78515	Drupal Database Abstraction API SQLi
HIGH	9.3*	-	67260	PHP 5.4.x < 5.4.17 Buffer Overflow
HIGH	7.5*	6.7	71427	PHP 5.4.x < 5.4.23 OpenSSL openssl_x509_parse() Memory Corruption

HIGH	7.2*	6.7	73862	PHP 5.4.x < 5.4.28 FPM Unix Socket Insecure Permission Escalation
HIGH	7.5*	6.7	76281	PHP 5.4.x < 5.4.30 Multiple Vulnerabilities
HIGH	7.5*	6.7	78545	PHP 5.4.x < 5.4.34 Multiple Vulnerabilities
HIGH	7.5*	6.6	80330	PHP 5.4.x < 5.4.36 'process_nested_data' RCE
MEDIUM	5.3	-	40984	Browsable Web Directories
MEDIUM	5.3	2.2	64993	PHP 5.4.x < 5.4.12 Information Disclosure
MEDIUM	5.3	-	152853	PHP < 7.3.28 Email Header Injection
MEDIUM	4.3*	-	47831	CGI Generic XSS (comprehensive test)
MEDIUM	5.0*	3.6	66843	PHP 5.4.x < 5.4.16 Multiple Vulnerabilities
MEDIUM	5.0*	3.6	71927	PHP 5.4.x < 5.4.24 Multiple Vulnerabilities
MEDIUM	5.0*	3.6	72881	PHP 5.4.x < 5.4.26 Multiple Vulnerabilities
MEDIUM	5.0*	4.2	73338	PHP 5.4.x < 5.4.27 awk Magic Parsing BEGIN DoS
MEDIUM	5.0*	3.6	74291	PHP 5.4.x < 5.4.29 'src/cdf.c' Multiple Vulnerabilities
MEDIUM	6.8*	5.9	77402	PHP 5.4.x < 5.4.32 Multiple Vulnerabilities
MEDIUM	5.0*	3.6	79246	PHP 5.4.x < 5.4.35 'donote' DoS
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
LOW	2.6*	-	76791	PHP 5.4.x < 5.4.31 CLI Server 'header' DoS
LOW	N/A	-	42057	Web Server Allows Password Auto-Completion
LOW	2.6*	-	26194	Web Server Transmits Cleartext Credentials
INFO	N/A	-	18261	Apache Banner Linux Distribution Disclosure
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	-	18638	Drupal Software Detection
INFO	N/A	-	19689	Embedded Web Server Detection
INFO	N/A	-	49704	External URLs
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	-	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	-	48243	PHP Version Detection
INFO	N/A	-	66334	Patch Report
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	-	20108	Web Server / Application favicon.ico Vendor Fingerprinting
INFO	N/A	-	11032	Web Server Directory Enumeration
INFO	N/A	-	10662	Web mirroring
INFO	N/A	-	24004	WebDAV Directory Enumeration
INFO	N/A	-	17219	phpMyAdmin Detection

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