tenable® Nessus

META

Vulnerabilities by Host

Vulnerabilities by Host

192.168.1.101

6	**8**	**29**	**3**	**72**
CRITICAL	HIGH	MEDIUM	LOW	INFO
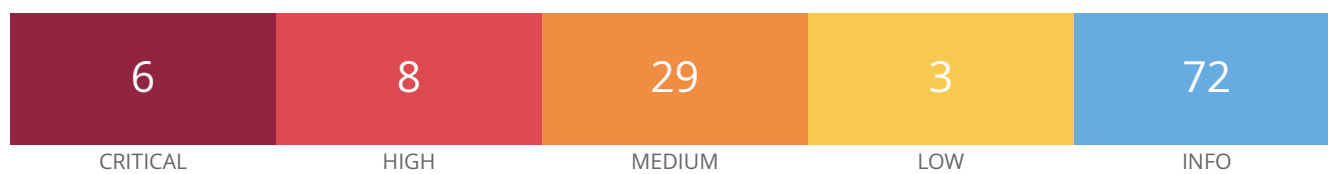
Vulnerabilities   Total: 118

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	8.9	70728	Apache PHP-CGI Remote Code Execution
CRITICAL	9.8	9.0	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	5.9	125855	phpMyAdmin prior to 4.8.6 SQLi vulnerablity (PMASA-2019-3)
CRITICAL	10.0	-	171340	Apache Tomcat SEoL (<= 5.5.x)
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	5.1	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
HIGH	8.8	7.4	19704	TWiki 'rev' Parameter Arbitrary Command Execution
HIGH	8.6	5.2	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	8.3	-	42424	CGI Generic SQL Injection (blind)
HIGH	7.5	5.9	90509	Samba Badlock Vulnerability
HIGH	7.5*	-	39465	CGI Generic Command Execution
HIGH	7.5*	-	39469	CGI Generic Remote File Inclusion
HIGH	7.5*	8.9	59088	PHP PHP-CGI Query String Parameter Injection Arbitrary Code Execution
HIGH	7.5*	6.7	36171	phpMyAdmin Setup Script Configuration Parameters Arbitrary PHP Code Injection (PMASA-2009-4)
MEDIUM	6.5	3.6	139915	ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	57582	SSL Self-Signed Certificate

MEDIUM	6.1	3.8	10815	Web Server Generic XSS
MEDIUM	5.9	4.4	136808	ISC BIND Denial of Service
MEDIUM	5.3	-	12085	Apache Tomcat Default Files
MEDIUM	5.3	-	40984	Browsable Web Directories
MEDIUM	5.3	-	39467	CGI Generic Path Traversal
MEDIUM	5.3	4.0	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.3	-	57608	SMB Signing not required
MEDIUM	5.3	-	15901	SSL Certificate Expiry
MEDIUM	5.3	-	45411	SSL Certificate with Wrong Hostname
MEDIUM	5.3	2.9	58751	SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability (BEAST)
MEDIUM	5.3	-	11229	Web Server info.php / phpinfo.php Detection
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	6.8*	-	42872	CGI Generic Local File Inclusion (2nd pass)
MEDIUM	5.0*	-	46195	CGI Generic Path Traversal (extended test)
MEDIUM	4.3*	-	47831	CGI Generic XSS (comprehensive test)
MEDIUM	4.3*	-	55903	CGI Generic XSS (extended patterns)
MEDIUM	4.3*	-	39466	CGI Generic XSS (quick test)
MEDIUM	5.0*	-	46803	PHP expose_php Information Disclosure
MEDIUM	4.0*	6.3	52611	SMTP Service STARTTLS Plaintext Command Injection
MEDIUM	5.0*	-	57640	Web Application 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	5.0*	-	36083	phpMyAdmin file_path Parameter Vulnerabilities (PMASA-2009-1)

MEDIUM	4.3*	3.0	49142	phpMyAdmin setup.php Verbose Server Name XSS (PMASA-2010-7)
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	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	21186	AJP Connector Detection
INFO	N/A	-	18261	Apache Banner Linux Distribution Disclosure
INFO	N/A	-	48204	Apache HTTP Server Version
INFO	N/A	-	39446	Apache Tomcat Detection
INFO	N/A	-	84574	Backported Security Patch Detection (PHP)
INFO	N/A	-	39521	Backported Security Patch Detection (WWW)
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	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	10028	DNS Server BIND version Directive Remote Version Detection
INFO	N/A	-	11002	DNS Server Detection
INFO	N/A	-	35371	DNS Server hostname.bind Map Hostname Disclosure
INFO	N/A	-	53333	Detect RPC over TCP
INFO	N/A	-	54615	Device Type
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
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	-	14788	IP Protocols Scan
INFO	N/A	-	11156	IRC Daemon Version Detection
INFO	N/A	-	10397	Microsoft Windows SMB LanMan Pipe Server Listing Disclosure
INFO	N/A	-	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	-	11011	Microsoft Windows SMB Service Detection
INFO	N/A	-	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	-	106716	Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)
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	-	19506	Nessus Scan Information
INFO	N/A	-	10335	Nessus TCP scanner
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	50845	OpenSSL Detection
INFO	N/A	-	48243	PHP Version Detection
INFO	N/A	-	66334	Patch Report
INFO	N/A	-	118224	PostgreSQL STARTTLS Support
INFO	N/A	-	26024	PostgreSQL Server Detection
INFO	N/A	-	40665	Protected Web Page Detection
INFO	N/A	-	22227	RMI Registry Detection
INFO	N/A	-	10263	SMTP Server Detection
INFO	N/A	-	42088	SMTP Service STARTTLS Command Support
INFO	N/A	-	56984	SSL / TLS Versions Supported
INFO	N/A	-	45410	SSL Certificate 'commonName' Mismatch

INFO	N/A	-	10863	SSL Certificate Information
INFO	N/A	-	25240	Samba Server Detection
INFO	N/A	-	104887	Samba Version
INFO	N/A	-	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	17975	Service Detection (GET request)
INFO	N/A	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	19941	TWiki Detection
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	11154	Unknown Service Detection: Banner Retrieval
INFO	N/A	-	135860	WMI Not Available
INFO	N/A	-	72771	Web Accessible Backups
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	-	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 | - | 10150 | Windows NetBIOS / SMB Remote Host Information Disclosure |
| INFO | N/A | - | 17219 | phpMyAdmin Detection |

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