



Lab1 OWASP Network

Wed, 17 Apr 2024 20:39:15 PDT

TABLE OF CONTENTS

Vulnerabilities by Host

- 10.0.2.4

Vulnerabilities by Host

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

10.0.2.4



Severity	CVSS v3.0	VPR Score	Plugin	Name
----------	-----------	-----------	--------	------

CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection
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	7.5	5.9	90509	Samba Badlock Vulnerability
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	6.1	5.7	136929	JQuery 1.2 < 3.5.0 Multiple XSS
MEDIUM	5.9	3.6	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	5.3	1.4	88098	Apache Server ETag Header Information Disclosure
MEDIUM	5.3	-	12085	Apache Tomcat Default Files
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	4.3*	-	90317	SSH Weak Algorithms Supported
LOW	3.7	3.6	70658	SSH Server CBC Mode Ciphers Enabled
LOW	3.7	-	153953	SSH Weak Key Exchange Algorithms Enabled

LOW	3.4	5.1	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
LOW	2.6*	-	71049	SSH Weak MAC Algorithms Enabled
LOW	N/A	-	69551	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
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	-	39520	Backported Security Patch Detection (SSH)
INFO	N/A	-	39521	Backported Security Patch Detection (WWW)
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	-	84502	HSTS Missing From HTTPS Server
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	-	11414	IMAP Service Banner Retrieval
INFO	N/A	-	106658	JQuery 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	-	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	-	122364	Python Remote HTTP Detection
INFO	N/A	-	70657	SSH Algorithms and Languages Supported

INFO	N/A	-	149334	SSH Password Authentication Accepted
INFO	N/A	-	10881	SSH Protocol Versions Supported
INFO	N/A	-	153588	SSH SHA-1 HMAC Algorithms Enabled
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	-	62563	SSL Compression Methods Supported
INFO	N/A	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	51891	SSL Session Resume Supported
INFO	N/A	-	156899	SSL/TLS Recommended Cipher Suites
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	-	11153	Service Detection (HELP Request)

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	-	135860	WMI Not Available
INFO	N/A	-	32318	Web Site Cross-Domain Policy File Detection
INFO	N/A	-	10150	Windows NetBIOS / SMB Remote Host Information Disclosure

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

Hide