



Web Application Paper Scan

Report generated by Nessus™

Sun, 10 Apr 2022 18:49:16 EDT

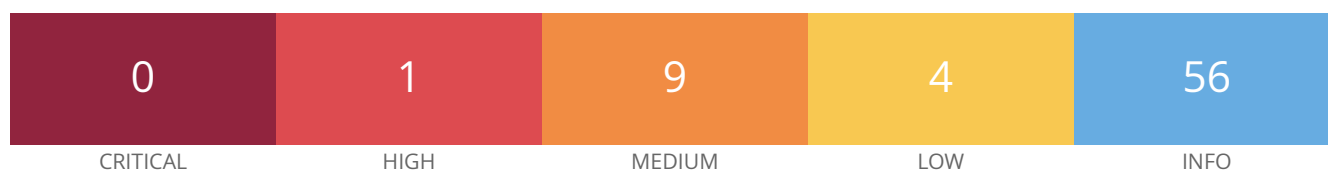
TABLE OF CONTENTS

Vulnerabilities by Host

• 10.10.11.143.....	4
---------------------	---

Vulnerabilities by Host

10.10.11.143



Vulnerabilities

Total: 70

SEVERITY	CVSS V3.0	PLUGIN	NAME
HIGH	7.5*	42423	CGI Generic SSI Injection (HTTP headers)
MEDIUM	6.5	51192	SSL Certificate Cannot Be Trusted
MEDIUM	5.3	40984	Browsable Web Directories
MEDIUM	5.3	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.0*	11411	Backup Files Disclosure
MEDIUM	6.4*	57582	SSL Self-Signed Certificate
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
MEDIUM	5.0*	12218	mDNS Detection (Remote Network)
LOW	3.7	153953	SSH Weak Key Exchange Algorithms Enabled
LOW	2.6*	70658	SSH Server CBC Mode Ciphers Enabled
LOW	N/A	42057	Web Server Allows Password Auto-Completion
LOW	2.6*	26194	Web Server Transmits Cleartext Credentials
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	48204	Apache HTTP Server Version
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	47830	CGI Generic Injectable Parameter
INFO	N/A	40406	CGI Generic Tests HTTP Errors
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	54615	Device Type
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	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	46215	Inconsistent Hostname and IP Address
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	117886	OS Security Patch Assessment Not Available
INFO	N/A	57323	OpenSSL Version Detection
INFO	N/A	48243	PHP Version 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	45410	SSL Certificate 'commonName' Mismatch
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	156899	SSL/TLS Recommended Cipher Suites
INFO	N/A	22964	Service Detection
INFO	N/A	25220	TCP/IP Timestamps Supported
INFO	N/A	84821	TLS ALPN Supported Protocol Enumeration
INFO	N/A	136318	TLS Version 1.2 Protocol Detection
INFO	N/A	138330	TLS Version 1.3 Protocol Detection
INFO	N/A	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	10287	Traceroute Information
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	49705	Web Server Harvested Email Addresses
INFO	N/A	10662	Web mirroring

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