



## owaspbw

---

Report generated by Nessus™

Thu, 14 Jul 2022 00:29:36 CST

---

---

TABLE OF CONTENTS

---

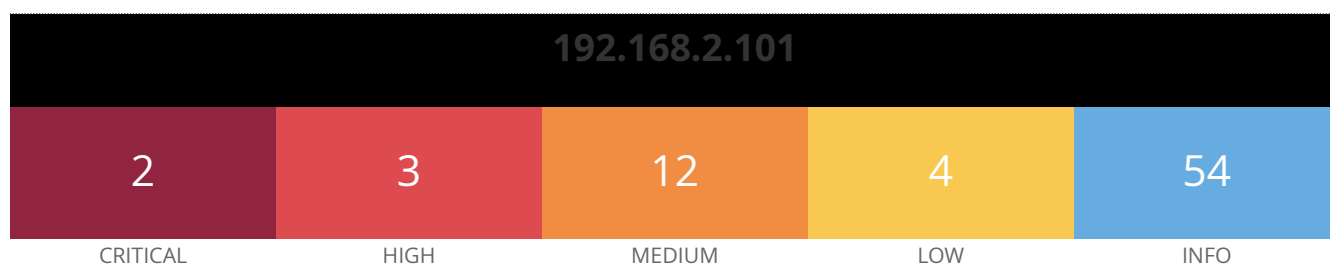
**Vulnerabilities by Host**

- 192.168.2.101.....4

---

## **Vulnerabilities by Host**

---



## Vulnerabilities

Total: 75

SEVERITY	CVSS V3.0	PLUGIN	NAME
CRITICAL	9.8	<a href="#">20007</a>	SSL Version 2 and 3 Protocol Detection
CRITICAL	10.0	<a href="#">33850</a>	Unix Operating System Unsupported Version Detection
HIGH	7.5	<a href="#">35291</a>	SSL Certificate Signed Using Weak Hashing Algorithm
HIGH	7.5	<a href="#">42873</a>	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	<a href="#">90509</a>	Samba Badlock Vulnerability
MEDIUM	6.8	<a href="#">78479</a>	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
MEDIUM	6.5	<a href="#">50686</a>	IP Forwarding Enabled
MEDIUM	6.5	<a href="#">51192</a>	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	<a href="#">57582</a>	SSL Self-Signed Certificate
MEDIUM	6.5	<a href="#">104743</a>	TLS Version 1.0 Protocol Detection
MEDIUM	6.1	<a href="#">136929</a>	jQuery 1.2 < 3.5.0 Multiple XSS
MEDIUM	5.9	<a href="#">65821</a>	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	5.3	<a href="#">88098</a>	Apache Server ETag Header Information Disclosure
MEDIUM	5.3	<a href="#">12085</a>	Apache Tomcat Default Files
MEDIUM	5.3	<a href="#">11213</a>	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.3	<a href="#">57608</a>	SMB Signing not required
MEDIUM	4.3*	<a href="#">90317</a>	SSH Weak Algorithms Supported
LOW	3.7	<a href="#">153953</a>	SSH Weak Key Exchange Algorithms Enabled

LOW	2.6*	<a href="#">70658</a>	SSH Server CBC Mode Ciphers Enabled
LOW	2.6*	<a href="#">71049</a>	SSH Weak MAC Algorithms Enabled
LOW	N/A	<a href="#">69551</a>	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits
INFO	N/A	<a href="#">10114</a>	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	<a href="#">18261</a>	Apache Banner Linux Distribution Disclosure
INFO	N/A	<a href="#">48204</a>	Apache HTTP Server Version
INFO	N/A	<a href="#">39446</a>	Apache Tomcat Detection
INFO	N/A	<a href="#">84574</a>	Backported Security Patch Detection (PHP)
INFO	N/A	<a href="#">39520</a>	Backported Security Patch Detection (SSH)
INFO	N/A	<a href="#">39521</a>	Backported Security Patch Detection (WWW)
INFO	N/A	<a href="#">45590</a>	Common Platform Enumeration (CPE)
INFO	N/A	<a href="#">54615</a>	Device Type
INFO	N/A	<a href="#">35716</a>	Ethernet Card Manufacturer Detection
INFO	N/A	<a href="#">86420</a>	Ethernet MAC Addresses
INFO	N/A	<a href="#">43111</a>	HTTP Methods Allowed (per directory)
INFO	N/A	<a href="#">10107</a>	HTTP Server Type and Version
INFO	N/A	<a href="#">24260</a>	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	<a href="#">11414</a>	IMAP Service Banner Retrieval
INFO	N/A	<a href="#">106658</a>	JQuery Detection
INFO	N/A	<a href="#">10397</a>	Microsoft Windows SMB LanMan Pipe Server Listing Disclosure
INFO	N/A	<a href="#">10785</a>	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	<a href="#">11011</a>	Microsoft Windows SMB Service Detection
INFO	N/A	<a href="#">100871</a>	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	<a href="#">106716</a>	Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)
INFO	N/A	<a href="#">11219</a>	Nessus SYN scanner

INFO	N/A	<a href="#">19506</a>	Nessus Scan Information
INFO	N/A	<a href="#">11936</a>	OS Identification
INFO	N/A	<a href="#">117886</a>	OS Security Patch Assessment Not Available
INFO	N/A	<a href="#">50845</a>	OpenSSL Detection
INFO	N/A	<a href="#">57323</a>	OpenSSL Version Detection
INFO	N/A	<a href="#">48243</a>	PHP Version Detection
INFO	N/A	<a href="#">66334</a>	Patch Report
INFO	N/A	<a href="#">122364</a>	Python Remote HTTP Detection
INFO	N/A	<a href="#">70657</a>	SSH Algorithms and Languages Supported
INFO	N/A	<a href="#">149334</a>	SSH Password Authentication Accepted
INFO	N/A	<a href="#">10881</a>	SSH Protocol Versions Supported
INFO	N/A	<a href="#">153588</a>	SSH SHA-1 HMAC Algorithms Enabled
INFO	N/A	<a href="#">10267</a>	SSH Server Type and Version Information
INFO	N/A	<a href="#">56984</a>	SSL / TLS Versions Supported
INFO	N/A	<a href="#">10863</a>	SSL Certificate Information
INFO	N/A	<a href="#">70544</a>	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	<a href="#">21643</a>	SSL Cipher Suites Supported
INFO	N/A	<a href="#">62563</a>	SSL Compression Methods Supported
INFO	N/A	<a href="#">57041</a>	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	<a href="#">51891</a>	SSL Session Resume Supported
INFO	N/A	<a href="#">156899</a>	SSL/TLS Recommended Cipher Suites
INFO	N/A	<a href="#">25240</a>	Samba Server Detection
INFO	N/A	<a href="#">104887</a>	Samba Version
INFO	N/A	<a href="#">96982</a>	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
INFO	N/A	<a href="#">22964</a>	Service Detection

INFO	N/A	17975	Service Detection (GET 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