

1. Name: Sunday Dorcas Idorenyin

Date: 24/06/2025

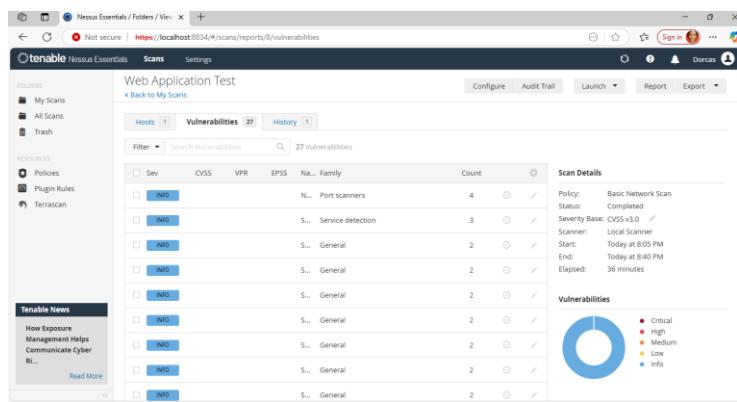
Title: Web Application Security Testing With Nessus

2. Introduction

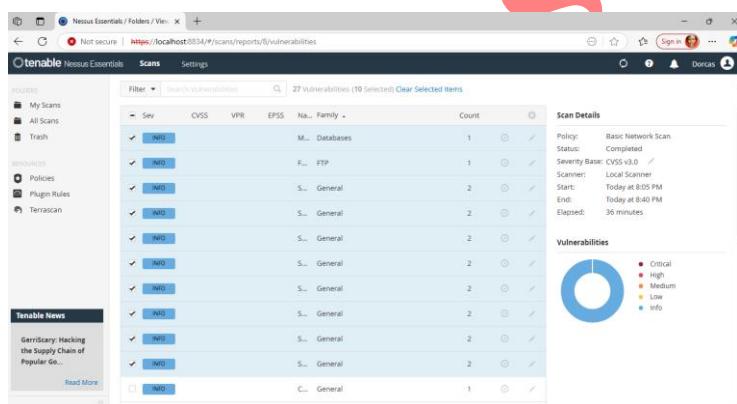
This report entails using Nessus essential (free) in Windows to test web application security for wilsescyberresearch.com, potential security risks was identified and mitigation strategies would be recommended to keep the web application security safe.

3. Screenshots of Nessus Scan Results

The results show that there are 27 vulnerabilities found on wilsescyberresearch.com when a web application was done.



OWASP Top 10 search



MySQL was detected by Nessus

This screenshot shows the Nessus Essentials interface. On the left, there's a sidebar with 'Folders' (My Scans, All Scans, Trash), 'Resources' (Policies, Plugin Rules, TenableScan), and 'Tenable News'. The main area displays a 'MySQL Server Detection' report for host 46.202.145.15. The 'Description' section states: 'The remote host is running MySQL, an open source database server.' The 'Output' section contains detailed log entries from MySQL, including: 'Version: 5.5.5-10.11.10-MariaDB-log', 'Protocol: 10', 'Server Status: SERVER_STATUS_AUTOCOMMIT', 'Server Capabilities: CLIENT_FOUND_ROWS (Found instead of affected rows)', 'CLIENT_LONG_FLAG (Set all column flags)', 'CLIENT_MULTI_STATEMENTS (Supports multiple statements per connection)', 'CLIENT_NO_SCHEMA (Don't allow database.table.column)', 'CLIENT_TRANSACTIONS (Supports transactions)', and 'CLIENT_RESERVED (Don't use reserved identifiers)'. A note at the bottom says 'To see debug logs, please visit individual host'. The 'Plugin Details' section includes fields like Severity: Info, ID: 10719, Version: 1.44, Type: remote, Family: Databases, Published: August 13, 2001, and Modified: October 12, 2022. The 'Risk Information' section shows Risk Factor: None. The 'Vulnerability Information' section lists CPE: cpe:/a:mysql:mysql and Asset Inventory: True. The 'Reference Information' section shows IAVI: 00011-0892.

FTP is showing blank

This screenshot shows the Nessus Essentials interface. The main area displays a 'Web Application Test' report for host 46.202.145.15. The 'Vulnerabilities' table shows one entry for 'FTP' with a severity of 'Info'. The 'Scan Details' panel indicates a 'Basic Network Scan' completed at 8:05 PM today, with a duration of 36 minutes. The 'Vulnerabilities' chart shows a single blue segment labeled 'Info'.

Security misconfiguration

This screenshot shows the Nessus Essentials interface. The main area displays a 'TLS NPN Supported Protocol Enumeration' report for host 46.202.145.15. The 'Vulnerabilities' table shows one entry for 'TLS NPN Supported Protocol Enumeration' with a severity of 'Info'. The 'Plugin Details' section includes fields like Severity: info, ID: 87242, Version: 1.10, Type: remote, Family: Misc., Published: December 8, 2015, and Modified: September 11, 2024. The 'Risk Information' section shows Risk Factor: None.

Second misconfiguration

Nessus Essentials / Folders / Vulnerabilities

Web Application Test / Plugin #87242

Description: The remote host supports the TLS NPN (Transport Layer Security Next Protocol Negotiation) extension. This plugin enumerates the protocols the extension supports.

Output:

HTTP Supported Protocols:	http
To see debug logs, please visit individual host	
Port:	Hosts
21/tcp / ftp	46.202.145.15

Plugin Details:

- Severity: Info
- ID: 87242
- Version: 1.0
- Type: remote
- Family: Misc
- Published: December 8, 2015
- Modified: September 11, 2024

Risk Information:

- Risk Factor: None

Cross-site scripting

Nessus Essentials / Folders / Vulnerabilities

Web Application Test / Plugin #156899

Description: The remote host has open SSL/TLS ports which advertise discouraged cipher suites. It is recommended to only enable support for the following cipher suites:

TLSv1.3:
- 0x13001 TLS13_AES_128_GCM_SHA256
- 0x13002 TLS13_AES_256_GCM_SHA384

TLSv1.2:
- 0xC0280 ECDHE-RSA-AES128-GCM-SHA256
- 0xC0282 ECDHE-RSA-AES256-GCM-SHA384
- 0xC0283 ECDHE-RSA-AES256-GCM-SHA384
- 0xC0284 ECDHE-RSA-CHACHA20-POLY1305
- 0xC0285 ECDHE-RSA-CHACHA20-POLY1305

This is the recommended configuration for the vast majority of services, as it is highly secure and compatible with nearly every client released in the last five (or more) years.

Solution:

Only enable support for recommended cipher suites.

Nessus Essentials / Folders / Vulnerabilities

Web Application Test / Plugin #10863

Description: This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

Output:

Subject Name:	Common Name: *.hatgr.io
Issuer Name:	Country: GB
State/Province: Greater Manchester	
Locality: Warrington	
Organization: hatgr	
Organizational Unit: hatgr	
To see debug logs, please visit individual host.	
Port:	Hosts
443/tcp	46.202.145.15
21/tcp / ftp	46.202.145.15

Plugin Details:

- Severity: Info
- ID: 10863
- Version: 1.22
- Type: remote
- Family: General
- Published: May 19, 2008
- Modified: February 3, 2021

Risk Information:

- Risk Factor: None

Nessus Essentials / Folders / Vulnerabilities

Web Application Test / Plugin #95631

Description: The remote service uses a known CA certificate in the SSL certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g., MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks (CVE-2004-2761, for example). An attacker can exploit this to generate another certificate with the same digital signature, allowing the attacker to masquerade as the affected service.

Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as vulnerable. This is in accordance with Google's gradual sunsetting of the SHA-1 cryptographic hash algorithm.

Note that this plugin will only fire on root certificates that are known certificate authorities as listed in Tenable Community Knowledge Article 200001752. That is what differentiates this plugin from plugin 35291, which will fire on any certificate, not just known certificate authority root certificates.

Known certificate authority root certificates are inherently trusted and so any potential issues with the signature, including it being signed using a weak hashing algorithm, are not considered security issues.

Solution:

Contact the Certificate Authority to have the certificate reissued.

See Also:

- <http://www.nessus.org/t/ue636478>
- <https://tools.ietf.org/html/rfc3227>
- <http://www.nessus.org/t/998b87bf2>

Output:

The following known CA certificates were part of the certificate chain:

unday

4. Vulnerabilities Detected on Nessus

Detected	MySQL	Misconfiguration	Port scanning	Service detection	Web servers	Settings	FTP	General
Vulnerability	Yes	Yes	No	Yes	Yes	No	No	Yes
Count	1	3	4	8	2	1	1	22

5. Explanation of the Top 3 Vulnerabilities and Their Impact

MySQL – Client (threat actor) is fully aware of all the transactions that take place in the database so therefore the system was compromised, sensitive information such as financial transaction was accessed and data modified.

Cross-site scripting – Attacker took advantage of a vulnerability found in the website code that was not written properly and injects their malicious scripts. They could steal sensitive information (data theft) in order to impersonate and access users account. These could lead the organisation to loss of reputation damage.

Security misconfiguration – Different factors contributes to security misconfiguration which includes using default settings such as username and password, human error during configuration changes, and failure to update out-dated software. These security misconfiguration could lead to financial loss, reputation destroyed, malware infection spread to compromise system and service disruption.

Nessus Essentials / Folders / View - +

Not secure | https://localhost:8534/#/scans/reports/0/vulnerabilities/10719

Tenable Nessus Essentials Scans Settings

Hosts 1 Vulnerabilities 27 History 1

MySQL Server Detection

Description

The remote host is running MySQL, an open source database server.

Output

```
Version: 5.5.5-51.11.10-MariaDB-1-log
Protocol: 10
Server Status: SERVER_STATUS_AUTOCOMMIT
Server Version: 5.5.5
    CLIENT_FOUND_ROWS (found instead of affected rows)
    CLIENT_IGNORE (ignore all errors)
    CLIENT_CONNECT_WITH_DB (One can specify db on connect)
    CLIENT_PLUGIN_AUTH (can use a plugin for authentication)
    CLIENT_CONNECT_BY_USER (can use a user and password)
    CLIENT_GONE_ERROR (GONE client)
    CLIENT_PROTOCOL_41 (use LOAD DATA LOCAL)
    CLIENT_SECURE_CONNECTION (use SSL after handshake)
    CLIENT_INTERACTIVE (This is an interactive client)
    CLIENT_PIPES (uses pipes)
    CLIENT_TRANSACTIONS (Client knows about transactions)
    CLIENT_RESERVED (use reserved names for A.I. protocol)
    CLIENT_SECURE_CONNECTION (use SSL authentication)
    ...
```

To see debug logs, please visit individual host

Port - Hosts

Plugin Details

Severity: Info
ID: 10719
Version: 1.44
Type: remote
Family: Databases
Published: August 13, 2001
Modified: October 12, 2022

Risk Information

Risk Factor: None

Vulnerability Information

CPE: cpe:/o:mysql:mysql
Asset inventory: True

Reference Information

IVR: 0001-7-0802

FTP – it was not found.

Nessus Essentials / Folders / View - +

Not secure | https://localhost:8534/#/scans/reports/0/vulnerabilities/56984

Tenable Nessus Essentials Scans Settings

Hosts 1 Vulnerabilities 27 History 1

SSL / TLS Versions Supported

Description

This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.

Output

```
This port supports TLSv1.3/TLSv1.2.
To see debug logs, please visit individual host
```

Port -	Hosts
21 / TCP / IP	46.202.145.15

This port supports TLSv1.2.

To see debug logs, please visit individual host

Port -	Hosts
443 / TCP	46.202.145.15

Plugin Details

Severity: Info
ID: 56984
Version: 1.36
Type: remote
Family: General
Published: December 1, 2011
Modified: June 16, 2025

Risk Information

Risk Factor: None

6. Remediation and recommendation

MySQL – Install web application firewall (WAF), implement least privilege, and use strict input validation and use parameterized.

Cross-site Scripting – Conduct frequent security audits, validate and sanitize all user inputs, use output encoding and implement content security policy to prevent unauthorized script.

Security misconfiguration – Promptly incorporate security patches, use system hardening, conduct regular security audits, apply strong access control, train staff and use security tools to monitor and manage misconfiguration.

XML report exported from Web Application Test



7. Conclusion

In conclusion, it is imperative to incorporate the above recommendations to protect web application device both software and hardware from cybercriminals.