1. **Name: Sunday Dorcas Idorenyin** **Date: 24/06/2025**

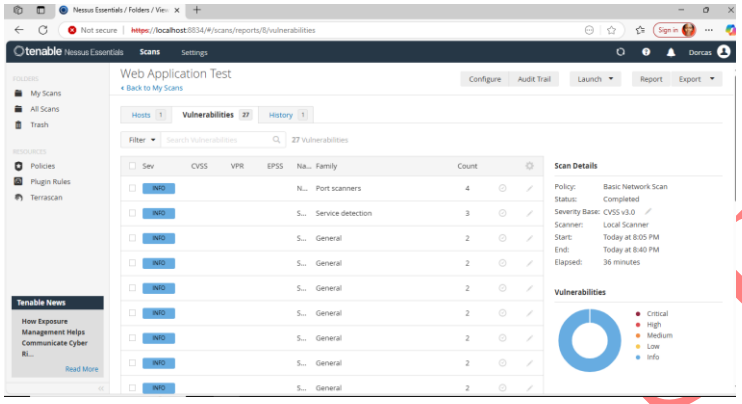
Title: Web Application Security Testing With Nessus

2. Introduction

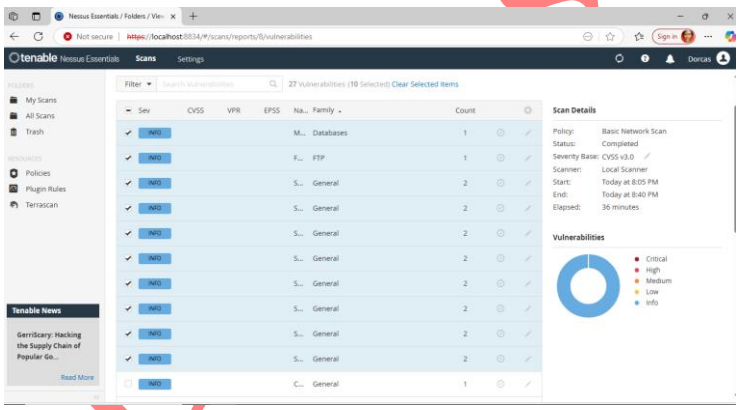
This report entails using Nessus essential (free) in Windows to test web application security for wilsescyberresearch.com, potential security risks was identified and mitigation strategies would be recommended to keep the web application security safe.

3. Screenshots of Nessus Scan Results

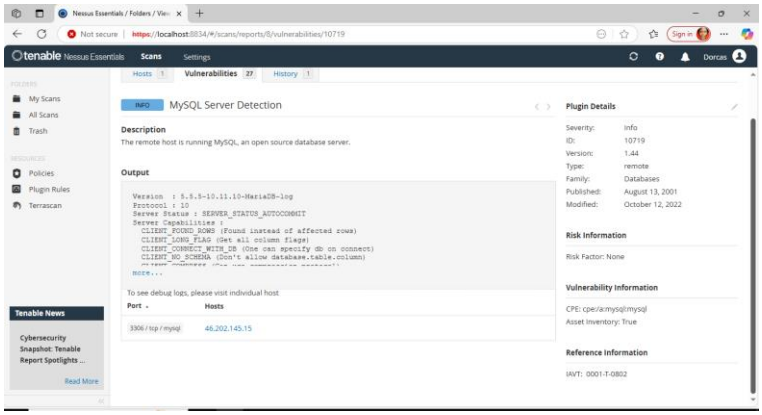
The results show that there are 27 vulnerabilities found on wilsescyberresearch.com when a web application was done.



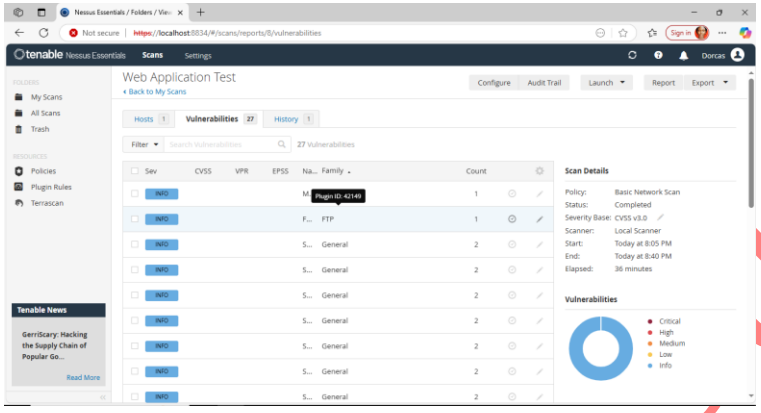
OWASP Top 10 search



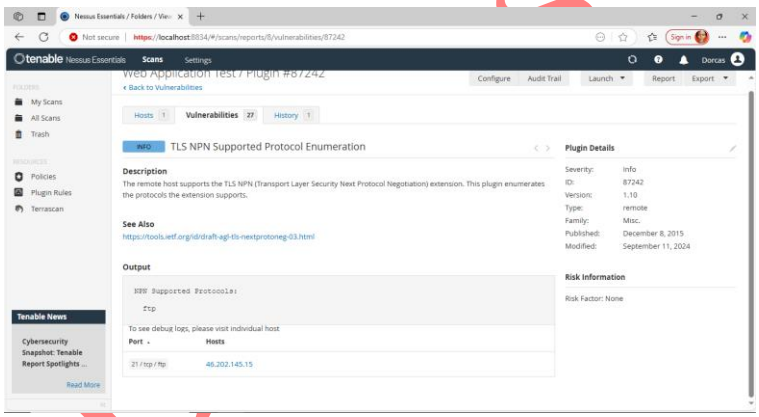
MySQL was detected by Nessus



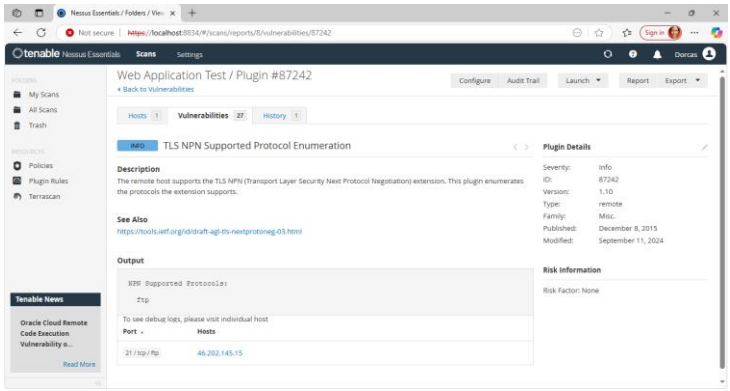
FTP is showing blank



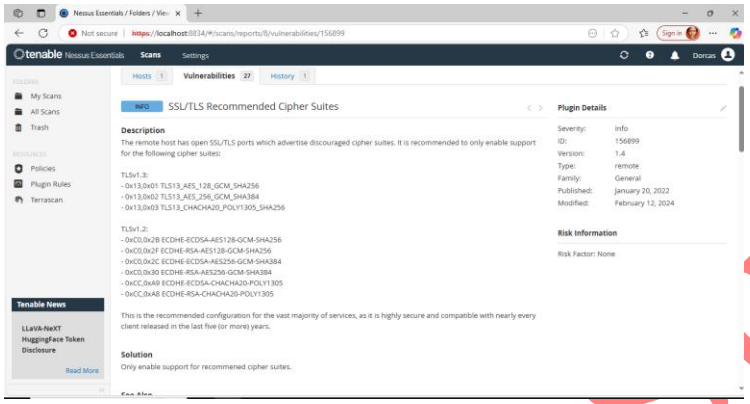
Security misconfiguration

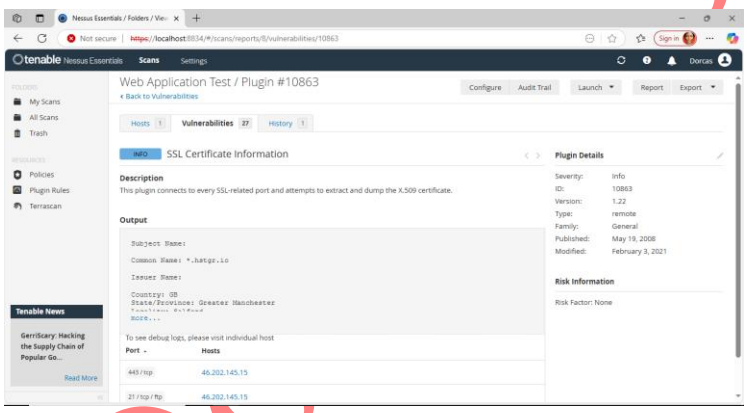


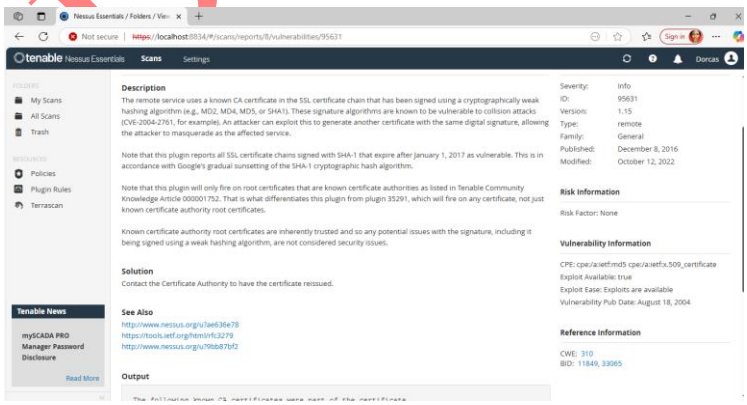
Second misconfiguration



Cross-site scripting







4. Vulnerabilities Detected on Nessus

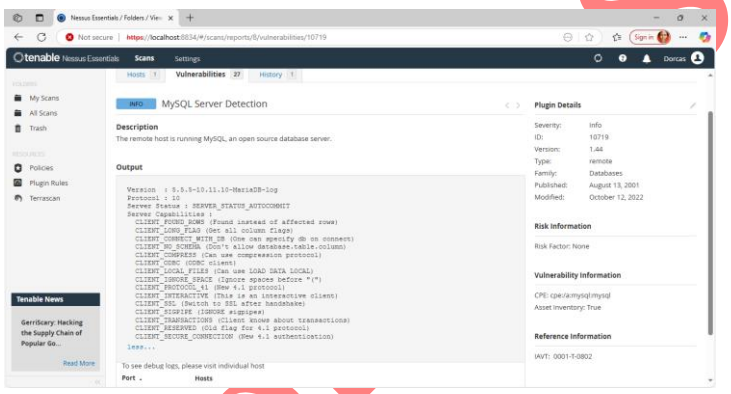
Detected	MySQL	Misconfiguration	Port scanning	Service detection	Web servers	Settings	FTP	General
Vulnerability	Yes	Yes	No	Yes	Yes	No	No	Yes
Count	1	3	4	8	2	1	1	22

5. Explanation of the Top 3 Vulnerabilities and Their Impact

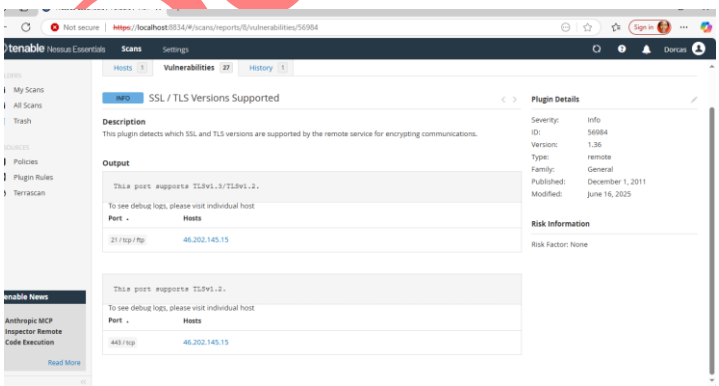
MySQL – Client (threat actor) is fully aware of all the transactions that take place in the database so therefore the system was compromised, sensitive information such as financial transaction was accessed and data modified.

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.



FTP – it was not found.



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

Web Application Test_n035mx.nessus

7. Conclusion

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