3MTT Cybersecurity Project Report

\*\*Author:\*\* Ebieme Bassey

\*\*Track:\*\* Cybersecurity – 3MTT Cohort 3

\*\*Project Title:\*\* Security Assessment for Infinity FinTech Ltd

\*\*Date:\*\* July 2025

# Table of Contents

1. Executive Summary

2. Company Profile

3. Assessment Methodology

4. Findings

5. Recommendations

6. Conclusion

7. Tools Used

8. References

# 1. Executive Summary

This report presents a basic cybersecurity assessment of a fictional company, Infinity FinTech Ltd. The assessment simulates techniques to identify potential vulnerabilities and outlines mitigation strategies based on best practices. This project demonstrates the application of cybersecurity principles learned during the 3MTT program.

# 2. Company Profile

Infinity FinTech Ltd is a fictional online banking startup that provides mobile and web-based payment services. The company operates on a cloud-based infrastructure with a public-facing website, an internal admin panel, and customer login portals.

# 3. Assessment Methodology

The assessment utilized both passive and simulated active scanning techniques, including domain lookups, port scanning (via Nmap), and manual analysis of web application exposure. The approach was non-intrusive and focused on identifying common vulnerabilities.

# 4. Findings

| Vulnerability | Description | Risk Level |
| --- | --- | --- |
| Open Ports | Ports 22 (SSH), 80 (HTTP), and 3306 (MySQL) were accessible. | Medium |
| No SSL Encryption | Website runs on HTTP, allowing data to be intercepted. | High |
| Weak Passwords | Default or simple passwords used on admin panels. | High |
| Outdated Software | CMS and plugins not updated, exposing known vulnerabilities. | High |
| No Multi-Factor Authentication | Lack of MFA for user and admin logins. | High |

# 5. Recommendations

- Implement strong password policies and enforce regular changes.

- Install SSL certificates to secure web traffic (e.g., HTTPS).

- Close unused ports using firewall configurations.

- Update all software, CMS, and plugins to the latest versions.

- Enable Multi-Factor Authentication (MFA) for all logins.

- Conduct regular vulnerability assessments and penetration tests.

# 6. Conclusion

The assessment revealed several critical and high-risk vulnerabilities that must be addressed to secure Infinity FinTech Ltd’s systems. Implementing the recommendations provided can greatly enhance the company’s security posture. This simulation reinforces the importance of regular assessments for early detection and prevention of cyber threats.

# 7. Tools Used

- Nmap – for port scanning simulation

- Whois – to retrieve domain ownership details

- Nslookup – for DNS and IP resolution

- Markdown / Word – for documentation

- GitHub – for project version control and submission

# 8. References

- OWASP Top 10 – https://owasp.org/www-project-top-ten/

- Nmap Manual – https://nmap.org/book/man.html

- 3MTT Cybersecurity Training Resources – Darey.io