1 Executive Security Assessment Report

1.1 Analysis Overview

The security assessment was conducted on the domain **torchlakefederal-dn.financial-net.com**. The analysis commenced on **March 31st at 18:45** and concluded in a duration of **13 minutes and 3 seconds**. The assessment was identified with the tracking ID **06bb2187be56** and was performed using a Basic scan type. The evaluation focused on identifying High and Medium-risk vulnerabilities within the domain's infrastructure.

1.2 Summary of Findings

The security assessment identified a total of **18 issues**, categorized as **0 High-risk**, **1 Medium-risk**, **1 Low-risk**, and **16 informational**. The most significant finding is a Medium-risk issue related to open port **80**, which lacks encryption, potentially exposing data to interception unless redirected to HTTPS or secured with HSTS. This vulnerability could impact data confidentiality and integrity. Additionally, the Low-risk SSL/TLS assessment revealed the use of TLS **1.2**, which is acceptable but lacks the enhanced security of TLS **1.3**. The analysis showed no evidence of shared hosting environments, High-risk geographic server locations, or services vulnerable to brute force attacks. Actionable insights include securing HTTP traffic and considering an upgrade to TLS **1.3** to enhance security posture.

1.3 Issues Table

Title	Risk
Nmap Port Scan Results Analysis	Medium
SSL/TLS Protocols Security Assess.	Low

1.4 Detailed Findings

1.4.1 Nmap Port Scan Results Analysis

Description:

The scan identified **2 open ports** on the target IP address, with port **80/tcp** running an HTTP service without encryption. This configuration poses a risk as it may allow data interception during transmission, compromising data confidentiality and integrity.

Affected Assets:

- **IP Address:** 107.162.143.82
- **Ports:** 80/tcp (HTTP), 443/tcp (SSL/HTTPS)

Recommendations:

It is recommended to ensure that HTTP traffic is redirected to HTTPS or that HTTP Strict Transport Security (HSTS) is enabled to enforce secure connections. This will mitigate the risk of data interception and enhance overall security.

1.4.2 SSL/TLS Protocols Security Assessment

Description:

The assessment revealed that the endpoint is using **TLS 1.2**, which is currently acceptable but does not provide the enhanced security features of **TLS 1.3**. No endpoints were found using deprecated protocols such as SSLv3, TLS 1.0, or TLS 1.1.

Affected Assets:

- **Endpoint:** 1 using TLS 1.2

Recommendations:

Consider upgrading to **TLS 1.3** to benefit from improved security and performance features. This upgrade will align with current best practices and provide stronger cryptographic protection.

1.5 General Recommendations

To enhance the security posture of the domain, it is advised to implement HTTPS redirection for all HTTP traffic and enable HSTS where applicable. Additionally, upgrading to TLS **1.3** should be prioritized to leverage its advanced security capabilities. Regular security assessments should be conducted to ensure ongoing protection against emerging threats and vulnerabilities.