1 Executive Security Assessment Report

1.1 Introduction

This security assessment was conducted on the domain **s1cu-dn.financial-net.com**. The analysis commenced on **April 2nd** at **17:00** and concluded in **11 minutes and 39 seconds**. The assessment was identified with tracking ID **126209e81489** and was categorized as a **Basic** scan. The evaluation focused on identifying potential vulnerabilities within the web application and infrastructure, adhering to OWASP and OSCP methodologies.

1.2 Short Summary of Main Issues

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 the Medium-risk issue related to the Nmap port scan, which detected an open HTTP port (**80**) without encryption, potentially exposing sensitive data if not redirected to HTTPS. This vulnerability could lead to unauthorized data access, impacting business confidentiality. 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. No high-density services or shared hosting environments were detected, indicating a well-segmented infrastructure. It is recommended to address the HTTP port issue promptly and consider upgrading to TLS 1.3 to enhance security posture.

1.3 Key Security Issues

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

1.3.1 Nmap Port Scan Results Analysis

Description

The Nmap port scan identified an open HTTP port (**80**) on IP **107.162.176.72**, which lacks encryption. This configuration poses a risk of unauthorized data access as data transmitted over HTTP is not encrypted, making it susceptible to interception.

Affected Assets

- **IP Address:** 107.162.176.72
- **Ports:** 80/tcp (HTTP), 443/tcp (SSL/HTTPS)

Recommendations

It is recommended to implement a redirection from HTTP to HTTPS to ensure all data is transmitted securely. Additionally, enabling HTTP Strict Transport Security (HSTS) can further enhance security by enforcing secure connections.

1.3.2 SSL/TLS Protocols Security Assessment

Description

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

Affected Assets

- **Endpoints using TLS 1.2: 1**

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 enhanced protection against potential cryptographic vulnerabilities.

1.4 General Recommendation

To maintain a robust security posture, it is crucial to address the identified Medium-risk issue by ensuring all HTTP traffic is securely redirected to HTTPS and implementing 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 identify and mitigate emerging threats promptly.