1 Executive Security Assessment Report

1.1 Introduction

The security assessment was conducted on the domain **coopaee-dn.financial-net.com**. The analysis commenced on **06-09 at 01:45** and concluded in a duration of **00h:09m:48s**. The assessment was identified with tracking ID **0d1e28db572d** and involved a basic scan type. 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**, **1 Medium**, **2 Low**, and **15 informational**. The most significant finding is the Medium-risk issue related to an open HTTP port (**80**) without encryption, which could expose sensitive data if not redirected to HTTPS. This vulnerability requires immediate attention to ensure data integrity and confidentiality. Additionally, the SSL/TLS analysis revealed that while TLS **1.2** is in use, there is no support for the more secure TLS **1.3**, suggesting an opportunity for protocol enhancement. The SSL certificate is set to expire in **132 days**, necessitating monitoring to avoid service disruptions. Overall, the assessment indicates a generally secure environment with specific areas for improvement to bolster security posture.

1.3 Key Security Issues

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

1.3.1 Nmap Port Scan Results Analysis

Description:
The assessment identified an open HTTP port (**80**) operating without encryption. This configuration poses a risk of exposing sensitive data unless mitigated by redirection to HTTPS or implementation of HTTP Strict Transport Security (HSTS).

Affected Assets:
- **IP Address:** 6[redacted].22.57.134 - **Ports:** 80/tcp (http), 443/tcp (ssl/https)

Recommendations:
Immediate action should be taken to configure the server to redirect HTTP traffic to HTTPS. Implementing HSTS will further enhance security by ensuring all communications are encrypted.

1.3.2 SSL/TLS Protocols Security Assessment

Description:
The analysis revealed that the domain supports TLS **1.2** but lacks support for the more secure TLS **1.3** protocol. While TLS **1.2** is currently acceptable, adopting TLS **1.3** would provide improved security and performance.

Affected Assets:
- **Endpoint using TLS 1.2**

Recommendations:
Upgrade the server configuration to support TLS **1.3** to align with current best practices and enhance cryptographic security.

1.3.3 SSL Certificate Expiration Analysis

Description:
The SSL/TLS certificate for the domain coopaee-dn.financial-net.com is set to expire in **132 days**, placing it in a “Monitor” status. Although not immediately critical, proactive monitoring is essential to prevent service disruptions.

Affected Assets:

- **Domain:** coopaee-dn.financial-net.com

Recommendations:
Implement a monitoring system to track certificate expiration dates and plan for timely renewal processes to ensure continuous secure communication.

1.4 General Recommendations

To enhance the overall security posture, it is recommended to address the Medium-risk issue by enforcing HTTPS across all endpoints and upgrading to TLS **1.3** where possible. Regularly monitor SSL certificate expiration dates to avoid potential service interruptions. Continuous security assessments should be conducted to identify and mitigate emerging threats promptly.