1 Executive Security Assessment Report

1.1 Introduction

This report presents the findings from a security assessment conducted on the domain **hopewellcfcu-dc.cert.fec-dc.fiservapps.com**. The assessment was initiated on **March 26th** at **16:45** and completed in **00h:09m:56s**. The analysis was performed using a basic scan methodology, focusing on identifying high and medium-risk vulnerabilities. The scope of the work included a comprehensive evaluation of the domain's web application and infrastructure security posture.

1.2 Summary of Findings

The security assessment identified a total of **18** issues, categorized as **0** High, **1** Medium, **1** Low, and **16** informational. The most significant finding is a Medium-risk issue related to open port **80**, which lacks encryption and poses potential security risks if not redirected to HTTPS. This could expose sensitive data to interception, impacting data confidentiality. Additionally, the Low-risk finding involves the use of TLS **1.2** without TLS **1.3**, which is acceptable but not optimal for modern security standards. The assessment also confirmed that all services are running on standard ports, with no unusual port assignments detected. No shared hosting environments or brute-force vulnerable services were found, indicating a generally secure infrastructure. Immediate actions should focus on addressing the Medium-risk port issue and planning for TLS upgrades 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 assessment identified an open port **80** running HTTP without encryption on IP address **66.6.29.16**. This configuration poses a Medium risk as it may allow sensitive data to be intercepted by unauthorized parties if not properly redirected to HTTPS or if HTTP Strict Transport Security (HSTS) is not enabled.

Affected Assets:

- IP Address: **66.6.29.16** - Ports: **80/tcp** (http), **443/tcp** (ssl/https)

Recommendations:

- Implement a redirection from HTTP to HTTPS to ensure all traffic is encrypted. - Enable HSTS to enforce secure connections. - Regularly review and update security configurations to adhere to best practices.

1.4.2 SSL/TLS Protocols Security Assessment

Description:

The analysis revealed that TLS **1.2** is in use, which is currently an acceptable minimum standard. However, TLS **1.3**, which offers improved security and performance, was not detected. The absence of SSLv3, TLS **1.0**, and TLS **1.1** is positive, as these protocols are vulnerable or deprecated.

Affected Assets:
- **1** endpoint using TLS **1.2** - **0** endpoints using TLS **1.3**, TLS **1.1**, TLS **1.0**, or SSLv3

Recommendations:
- Plan for an upgrade to TLS **1.3** to enhance security and performance. - Continue monitoring for deprecated protocols and ensure they remain disabled.

1.5 General Recommendations

To maintain a robust security posture, it is recommended that the organization prioritizes the implementation of HTTPS across all services and plans for future upgrades to TLS **1.3**. Regular security assessments should be conducted to identify and mitigate emerging threats promptly. Additionally, maintaining up-to-date security configurations and adhering to industry best practices will further strengthen the organization's defenses against potential vulnerabilities.