1 Executive Security Assessment Report

1.1 Overview

A comprehensive security assessment was conducted on the domain **tmhfcu-dc.cert.fec-dc.fiservapps.com**. The analysis was initiated on **April 5th** at **00:45** and completed in **00h:07m:40s**. The assessment employed a basic scan methodology focusing on identifying potential vulnerabilities within the web application and infrastructure. The evaluation adhered to OWASP and OSCP methodologies, ensuring a thorough examination of security postures.

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 open port **80**, which lacks encryption and poses potential security risks if not redirected to HTTPS or if HSTS is not enabled. This could expose sensitive data to interception, impacting business confidentiality. Additionally, the low-risk issue involves the use of TLS **1.2** without support for the more secure TLS **1.3**, which is recommended for enhanced security. The assessment also confirmed that all services are running on standard ports, with no unusual port assignments or brute-force vulnerabilities detected. It is crucial to address the medium-risk finding promptly to mitigate potential data exposure and enhance overall 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 assessment identified that port **80** is open and running HTTP without encryption. This configuration poses a medium risk as it can lead to potential data interception if not properly managed. The lack of encryption on HTTP traffic could expose sensitive information, compromising business confidentiality.

Affected Assets:

- **IP Address:** 66.22.19.210
- **Open Ports:** 80/tcp (http), 443/tcp (ssl/https)

Recommendations:

- Implement a redirection from HTTP to HTTPS to ensure all traffic is encrypted. - Enable HTTP Strict Transport Security (HSTS) to enforce secure connections. - Regularly review and update security configurations to align with best practices.

1.3.2 SSL/TLS Protocols Security Assessment

Description:

The analysis revealed that the endpoint supports TLS **1.2** but lacks support for TLS **1.3**, which is the current best practice for secure communications. While TLS **1.2** is acceptable, upgrading to TLS **1.3** would provide enhanced security and performance benefits.

Affected Assets:

- **Endpoint using TLS 1.2: 1**

Recommendations:
- Upgrade to TLS **1.3** to leverage improved cryptographic algorithms and enhanced security features. - Ensure all endpoints are configured to support modern protocols and ciphers.

1.4 General Recommendations

To strengthen the overall security posture, it is recommended to prioritize the implementation of HTTPS across all services, ensuring that sensitive data is always transmitted securely. Additionally, upgrading to TLS **1.3** where feasible will enhance both security and performance. Regular security audits and updates should be conducted to maintain alignment with evolving best practices and threat landscapes.