1 Executive Security Assessment Report

1.1 Introduction

The security assessment was conducted on the domain `sommfcu-admin.originate.fiservapps.com` using a comprehensive methodology aligned with OWASP and OSCP standards. The analysis commenced on June 14th at **03:45** and concluded in a duration of **00h:10m:36s**. The assessment type was categorized as "Basic," with the tracking ID `071aec63e8eb`. The primary objective was to identify and evaluate potential security vulnerabilities within the web application and infrastructure.

1.2 Short Summary of Main Issues

The security assessment identified several critical issues, including the absence of a Web Application Firewall (WAF) across all analyzed hosts, which significantly increases the risk of injection-based attacks. An open HTTP port (**80**) was detected without encryption, necessitating verification for HTTPS redirection or HSTS implementation. Additionally, the SSL/TLS analysis revealed the lack of TLS **1.3** support, and sensitive subdomains were identified, indicating potential exposure of administrative interfaces.

1.3 Key Security Issues

Title	Risk
Absence of WAF	Medium
Nmap Port Scan Results Analysis	Medium
Subdomain Naming Security Assessment	Medium
SSL/TLS Protocols Security Assessment	Low
SSL Certificate Expiration Analysis	Low

1.4 Absence of WAF

Description:

The absence of a Web Application Firewall (WAF) on the analyzed host significantly elevates the risk of successful cyber-attacks, particularly injection-based attacks. Without WAF protection, there is an increased likelihood of unauthorized data access, data breaches, and potential system compromise.

Affected Assets:

- Host: `sommfcu-admin.originate.fiservapps.com`

Recommendations:

Implement a robust Web Application Firewall to monitor and filter HTTP traffic between the web application and the Internet. This will help mitigate risks associated with injection attacks and unauthorized access attempts.

1.5 Nmap Port Scan Results Analysis

Description:

The Nmap port scan identified an open HTTP port (**80**) without encryption on IP address **167.86.43.25**. This poses a security risk if not redirected to HTTPS or if HSTS is not enabled, as it could allow interception of unencrypted data.

Affected Assets:

- IP Address: **167.86.43.25** - Ports: **80/tcp** (http), **443/tcp** (ssl/https)

Recommendations:

Ensure that HTTP traffic is redirected to HTTPS and implement HSTS to enforce secure connections. Regularly review open ports and services to ensure they are necessary and properly secured.

1.6 Subdomain Naming Security Assessment

Description:

Sensitive subdomains were detected, indicating the presence of administrative interfaces and management panels. These subdomains pose a high risk due to potential access to critical systems and sensitive data.

Affected Assets:

- Subdomain: `sommfcu-admin.originate.fiservapps.com`

Recommendations:

Restrict access to sensitive subdomains using IP whitelisting or VPN access. Regularly audit subdomain configurations and ensure that sensitive interfaces are not exposed to the public Internet.

1.7 General Recommendations

To enhance the overall security posture, it is recommended to implement a comprehensive security strategy that includes regular vulnerability assessments, patch management, and continuous monitoring. Additionally, adopting advanced encryption protocols such as TLS **1.3** will improve data protection and system resilience against emerging threats.