1 Executive Security Assessment Report

1.1 Scan Overview

The security assessment was conducted on the domain **kemba-admin.originate.fiservapps.com**. The analysis commenced on **April 25th** at **13:45** and concluded in **00h:09m:57s**. The assessment was performed using a Basic scan type, focusing on identifying potential vulnerabilities within the web application and its infrastructure, adhering to OWASP and OSCP methodologies.

1.2 Summary of Findings

The security assessment identified a total of **18** issues, categorized as **0** High, **2** Medium, **3** Low, and **13** informational. Notably, medium-risk findings include open HTTP ports without encryption, which could expose sensitive data, and sensitive subdomain names indicating potential access to administrative interfaces. These vulnerabilities could lead to unauthorized access and data breaches if not addressed. The SSL/TLS analysis revealed that while TLS 1.2 is in use, there is no support for the more secure TLS 1.3, and SSL certificates are set to expire in **175** days, requiring monitoring. The assessment also confirmed no shared hosting environments or brute-force susceptible services, indicating a generally secure infrastructure. Immediate actions should focus on securing HTTP traffic and reviewing access controls on sensitive subdomains.

1.3 Key Security Issues

Title	Risk
Nmap Port Scan Results Analysis	Medium
Subdomain Naming Security Assessment	Medium
SSL/TLS Protocols Security Assessment	Low
SSL Certificate Expiration Analysis	Low
Login Form Detection Analysis	Low

2 Detailed Findings

2.1 Nmap Port Scan Results Analysis

Description:
The scan identified **2** open ports, with port **80** running HTTP without encryption. This poses a risk if not redirected to HTTPS or if HSTS is not enabled, potentially exposing sensitive data to interception.

Affected Assets:

- IP: **66.6.16.37** - Ports: **80/tcp** (http), **443/tcp** (ssl/https)

Recommendations:

Implement HTTPS with strong encryption protocols for all web traffic. Ensure HTTP traffic is redirected to HTTPS and enable HTTP Strict Transport Security (HSTS) to prevent protocol downgrade attacks.

2.2 Subdomain Naming Security Assessment

Description:
A sensitive subdomain, **kemba-admin.originate.fiservapps.com**, was identified, indicating the presence of administrative interfaces and management panels. These are high-risk due to potential access to critical systems and sensitive data.

Affected Assets:
- Subdomain: **kemba-admin.originate.fiservapps.com**

Recommendations:
Restrict access to administrative interfaces using IP whitelisting or VPNs. Implement strong authentication mechanisms and regularly audit access logs for unauthorized attempts.

---

3 General Recommendations

To enhance the security posture of the domain, it is recommended to transition all services to support TLS 1.3 for improved security and performance. Regularly monitor SSL certificate expiration dates to ensure timely renewals. Conduct periodic security assessments to identify and mitigate emerging threats. Implement comprehensive access control measures for sensitive subdomains and interfaces. By addressing these recommendations, the organization can significantly reduce the risk of unauthorized access and data breaches, thereby safeguarding its digital assets.