1 Executive Security Assessment Report

1.1 Analysis Overview

The security assessment was conducted on the domain **pioneercommunitybank-admin.originate.fiservapps.c** The analysis commenced on **April 1st at 11:00 AM** and concluded in **10 minutes and 28 seconds**. The assessment was classified as a "Basic" type scan. The evaluation focused on identifying High and Medium-risk vulnerabilities using OWASP and OSCP methodologies.

1.2 Summary of Findings

The security assessment identified a total of **18 issues**, categorized as **0 High-risk**, **2 Medium-risk**, **3 Low-risk**, and **13 informational**. The most critical findings include Medium-risk vulnerabilities such as open HTTP ports (port **80**) without encryption, which could expose sensitive data, and sensitive subdomain names indicating potential access to administrative interfaces. These issues pose a risk of unauthorized access and data breaches. Additionally, the SSL/TLS assessment 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 **100 days**, requiring monitoring. The analysis also highlighted that all services are running on standard ports, and no brute-force vulnerable services were detected, indicating a generally secure configuration. Immediate attention should be given to securing open ports and monitoring SSL certificate expiration to mitigate potential security threats.

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

1.3.1 Nmap Port Scan Results Analysis

Description:
The scan identified **2 open ports** on the IP address **66.22.86.68**, specifically port **80/tcp** (HTTP) and port **443/tcp** (SSL/HTTPS). Port **80** is running HTTP without encryption, which poses a risk unless there is a redirection to HTTPS or HSTS is enabled.
- **Affected Assets:**
- IP: **66.22.86.68** - Ports: **80/tcp** (HTTP), **443/tcp** (SSL/HTTPS)
- **Recommendations:**
- Implement HTTPS redirection for all HTTP traffic. - Enable HTTP Strict Transport Security (HSTS) to ensure secure connections.

1.3.2 Subdomain Naming Security Assessment

Description:
A sensitive subdomain was detected: **pioneercommunitybank-admin.originate.fiservapps.com**. This subdomain may provide access to critical systems and sensitive data through administrative interfaces.

Affected Assets:

- Subdomain: **pioneercommunitybank-admin.originate.fiservapps.com**

Recommendations:

- Restrict access to administrative interfaces using IP whitelisting or VPN. - Regularly review and update access controls for sensitive subdomains.

1.4 General Recommendations

To enhance the security posture of the analyzed domain, it is recommended to prioritize the implementation of HTTPS across all services, ensure regular monitoring of SSL certificate expiration dates, and secure administrative interfaces with robust access controls. Additionally, consider upgrading to TLS **1.3** for improved security and performance. Regular security assessments should be conducted to identify and mitigate emerging threats promptly.