1 Executive Security Assessment Report

1.1 Introduction

The security assessment was conducted on the domain **rochellebank.originate.fiservapps.com**. The analysis was initiated on **06-07** at **18:00** and completed in **00h:09m:34s**. The assessment was identified with tracking ID **094f5f4c5caa** and utilized a Basic scan type. The evaluation focused on identifying potential vulnerabilities within the web application and 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, **1** Medium, **2** Low, and **15** informational. The most significant finding is the Medium-risk issue related to open port **80**, which lacks encryption and poses a potential security risk if not redirected to HTTPS. This could expose sensitive data to interception, impacting data confidentiality. Additionally, 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 the SSL certificate is set to expire in **141** days, requiring monitoring. The assessment also confirmed no shared hosting environments or brute-force vulnerable services, indicating a generally secure infrastructure. Immediate actions should focus on securing the HTTP service and planning for SSL certificate renewal to mitigate potential risks.

1.3 Key Security Issues

Title	Risk
Nmap Port Scan Results Analysis	Medium
SSL/TLS Protocols Security Assessment	Low
SSL Certificate Expiration Analysis	Low

1.3.1 Nmap Port Scan Results Analysis

Description:
The analysis identified **2** open ports on the IP address **66.22.20.178**. Port **80/tcp** is running HTTP without encryption, which poses a risk unless there is a redirection to HTTPS or HSTS is enabled. This lack of encryption can lead to data interception and compromise confidentiality.
Affected Assets:
- IP: **66.22.20.178** - 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 monitor and update web server configurations to adhere to security best practices.

1.3.2 SSL/TLS Protocols Security Assessment

Description:
The SSL/TLS analysis revealed that TLS **1.2** is currently in use, which is acceptable; however, there is no support for TLS **1.3**, which is considered the current best practice for enhanced security and performance.
Affected Assets:
- **1** endpoint using TLS **1.2**

Recommendations:
- Upgrade to support TLS **1.3** to leverage improved security features and performance benefits.
- Regularly review and update cryptographic protocols to align with industry standards.

1.3.3 SSL Certificate Expiration Analysis

Description:
The SSL/TLS certificate for the domain **rochellebank.originate.fiservapps.com** is set to expire in **141** days, categorized under "Monitor" status. This indicates that it should be monitored for timely renewal to avoid service disruption or security warnings.
Affected Assets:
- Domain: **rochellebank.originate.fiservapps.com**
Recommendations:
- Schedule a renewal process for the SSL certificate well before the expiration date. - Implement automated alerts for certificate expiration to prevent oversight.

1.4 General Recommendations

To enhance the overall security posture, it is recommended to prioritize the implementation of HTTPS across all services, upgrade cryptographic protocols to support TLS **1.3**, and establish a proactive certificate management strategy. Regular security assessments should be conducted to identify and mitigate emerging threats promptly.