1 Executive Security Assessment Report

1.1 Introduction

This report provides a comprehensive overview of the security assessment conducted on the domain **engineering-ch-qa.fiservmobileapps.com**. The evaluation was performed using certified methodologies, including OWASP and OSCP standards, to ensure a thorough analysis of the web application and infrastructure. The assessment was initiated on **July 1st** at **22:00** and concluded in **00h:07m:40s**. The tracking ID for this assessment is **0ef26f4312db**, and the scope was defined as a basic analysis.

1.2 Summary of Findings

The recent security assessment revealed no High, Medium, or Low-risk issues, with three informational findings. Notably, all scanned ports were filtered, indicating robust perimeter security controls such as firewalls and IPS/IDS systems, with **100%** of ports filtered. The analysis confirmed no shared hosting environments, ensuring dedicated infrastructure for all hosts. Geographic distribution analysis showed all servers located in the United States, with no presence in high-risk locations, maintaining a normal risk status. These findings suggest a strong security posture, but manual verification and alternative scanning methods are recommended to ensure comprehensive security coverage.

1.3 Key Security Issues

Title	Risk
No High or Medium Risk Issues	N/A

1.4 Detailed Findings

1.4.1 Description

The security assessment did not identify any High or Medium-risk issues. The findings indicate that the domain benefits from robust security measures, including effective perimeter defenses and dedicated hosting environments. All scanned ports were found to be filtered, which suggests that firewalls and intrusion prevention/detection systems are effectively configured to protect against unauthorized access.

1.4.2 Affected Assets

- **Domain**: engineering-ch-qa.fiservmobileapps.com
- **Geographic Location**: United States
- **Infrastructure**: Dedicated Hosting

1.4.3 Recommendations

1. **Manual Verification**: Conduct manual verification of the automated scan results to ensure no critical vulnerabilities were overlooked.
2. **Alternative Scanning Methods**: Employ alternative scanning techniques to validate the robustness of current security measures.
3. **Regular Security Audits**: Schedule regular security audits to maintain and enhance the security posture over time.
4. **Continuous Monitoring**: Implement continuous monitoring solutions to detect and respond to potential threats in real-time.

1.5 General Recommendation

While the current security posture appears strong, it is crucial to maintain vigilance through regular updates and continuous improvement of security practices. Regular training for staff on security awareness and incident response can further enhance the organization's ability to protect its assets effectively.