1 Executive Security Assessment Report

1.1 Overview

A comprehensive security assessment was conducted on the domain **mygenbankm.architect-cert.fiservapps.com**. The evaluation was initiated on **July 23rd at 19:45** and concluded in **00h:06m:39s**. The assessment employed a Basic scan type, identified by tracking ID **0784fede4dce**. The analysis adhered to OWASP and OSCP methodologies, focusing on identifying High and Medium-risk vulnerabilities within the web application and infrastructure.

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 are 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. Additionally, the geographic distribution of servers is normal, with all servers located in the United States, posing no High-risk location concerns. These findings suggest a strong security posture, but continued vigilance and manual verification are recommended to ensure comprehensive protection against potential threats.

1.3 Key Security Issues

Title	Risk
No High or Medium Risk Issues Found	N/A

1.4 Detailed Findings

1.4.1 Description

The security assessment did not identify any High or Medium-risk issues. This indicates a strong security posture with effective controls in place. The absence of critical vulnerabilities suggests that the current security measures are adequate in mitigating potential threats.

1.4.2 Affected Assets

- Domain: **mygenbankm.architect-cert.fiservapps.com**

1.4.3 Recommendations

1. **Continuous Monitoring**: Implement continuous monitoring solutions to detect any anomalies or potential threats in real-time.
2. **Regular Security Audits**: Conduct regular security audits and penetration tests to ensure that new vulnerabilities are not introduced into the environment.
3. **Security Awareness Training**: Provide ongoing security training for employees to recognize and respond to potential security threats effectively.
4. **Patch Management**: Maintain a robust patch management process to ensure that all systems are up-to-date with the latest security patches.

1.5 General Recommendation

Despite the absence of High or Medium-risk issues, it is crucial to maintain a proactive security stance. Regular updates to security policies, continuous monitoring, and periodic assessments should be conducted to adapt to evolving threats. Additionally, fostering a culture of security awareness within the organization will further enhance the overall security posture.