1 Executive Security Assessment Report

1.1 Introduction

The security assessment was conducted on the domain **accountoriginate.universalbank.com**. The analysis was initiated on **October 4th** at **02:45** and completed in a duration of **00h:05m:55s**. The assessment type was categorized as "Basic". The scope of the work focused on identifying potential vulnerabilities within the specified domain, utilizing methodologies aligned with OWASP and OSCP standards.

1.2 Summary of Findings

The recent security assessment identified a total of **three** issues, categorized as **0** High-risk, **1** Medium-risk, and **2** informational findings. The most significant concern is the Medium-risk issue related to a shared hosting environment, where one host, accountoriginate.universalbank.com, shares its IP with **28** other domains, potentially increasing exposure to cross-domain vulnerabilities. Additionally, the assessment noted that all scanned ports (**11** in total) are filtered, indicating robust perimeter security controls, such as firewalls and IPS/IDS systems. The geographic distribution analysis confirmed that all servers are located in the United States, with no presence in high-risk locations, ensuring a normal risk status. It is recommended to further investigate the shared hosting environment to mitigate potential risks and maintain strong security postures.

1.3 Issues Table

Title	Risk
Shared Hosting Environment	Medium

1.4 Detailed Findings

1.4.1 Shared Hosting Environment Analysis

Description The analysis identified that the domain **accountoriginate.universalbank.com** is part of a shared hosting environment, sharing its IP address with **28** other domains. This configuration poses a Medium risk due to potential cross-domain vulnerabilities that could arise from shared resources and configurations.

Affected Assets

- **Hostname:** accountoriginate.universalbank.com

Recommendations

- Conduct a thorough review of the shared hosting environment to ensure that adequate isolation measures are in place between domains.
- Implement strict access controls and monitoring to detect any unauthorized access or anomalous activities.
- Consider migrating to a dedicated hosting environment if feasible, to reduce exposure to shared hosting risks.

1.5 General Recommendations

To enhance the security posture of the domain, it is recommended to regularly perform comprehensive security assessments and implement continuous monitoring solutions. Additionally, maintaining up-to-date security patches and configurations will help mitigate potential vulnerabilities. Engaging in regular training and awareness programs for staff can further strengthen the overall security framework.