1 Executive Security Assessment Report

1.1 Overview of the Assessment

This security assessment was conducted on the domain **intqatdmobilews.ft.cashedge.com**. The evaluation was initiated on **July 17th** at **05:45** and concluded in **00h:06m:26s**. The tracking ID for this assessment is **0abffd0e7651**. The scope of the work involved a basic security analysis using 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 a well-configured firewall and active 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 analysis showed all servers located in the United States, with no servers in high-risk locations, maintaining a normal risk status. These findings suggest a strong security posture, but continuous monitoring and manual verification are recommended to ensure ongoing 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 vulnerabilities. The infrastructure demonstrated robust security measures, including effective firewall configurations and active intrusion prevention/detection systems. All scanned ports were found to be filtered, which is indicative of strong perimeter defenses.

1.4.2 Affected Assets

- Domain: **intqatdmobilews.ft.cashedge.com**

1.4.3 Recommendations

- Maintain current security configurations and continue regular security assessments to ensure that new vulnerabilities are promptly identified and mitigated.
- Implement continuous monitoring solutions to detect any anomalies or potential threats in real-time.
- Conduct periodic manual verification to complement automated scans and provide a comprehensive security overview.
- Ensure that all software and systems are kept up-to-date with the latest security patches.

1.5 General Recommendation

Given the absence of High or Medium-risk issues, it is recommended to maintain the current security posture while enhancing monitoring capabilities. Regular updates and continuous improvement of security protocols will help safeguard against emerging threats. Additionally,

consider investing in advanced threat detection technologies to further strengthen the defense mechanisms in place.