1 Executive Security Assessment Report

1.1 Introduction

A comprehensive security assessment was conducted on the domain **webmail.cbre.ma**. The analysis was initiated on **April 4th at 14:00** and completed in a duration of **00h:06m:15s**. This assessment was performed using a Basic scan type, with the tracking ID **1646ad6e0a3f**. The scope of the work included evaluating the web application and infrastructure security posture, employing methodologies aligned with OWASP and OSCP standards. The objective was to identify any High or Medium-risk vulnerabilities that could potentially impact the security of the domain.

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 a well-configured firewall and active IPS/IDS systems, with **100% of 11 ports filtered**. The analysis confirmed no shared hosting environments, suggesting dedicated infrastructure for all hosts. Additionally, the geographic distribution analysis showed all servers located in Morocco, with no presence in high-risk locations, maintaining a normal risk status. These findings underscore the effectiveness of current security measures, though manual verification and alternative scanning techniques are recommended to ensure comprehensive security validation.

1.3 Key Security Issues

Title	Risk
No High or Medium Risk Issues Detected	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 strong perimeter defenses with all **11 scanned ports** being filtered, indicating effective firewall configurations and active intrusion prevention/detection systems. The absence of shared hosting environments suggests a dedicated infrastructure setup, enhancing security by isolating resources. Furthermore, the exclusive location of servers in Morocco reduces exposure to geopolitical risks associated with high-risk regions.

1.4.2 Affected Assets

- **Domain:** webmail.cbre.ma
- **Ports Scanned: 11** (100% filtered)
- **Server Location:** Morocco

1.4.3 Recommendations

1. **Manual Verification:** Conduct manual penetration testing to validate automated scan results and uncover potential vulnerabilities not detected by automated tools.

2. **Alternative Scanning Techniques:** Utilize different scanning methodologies to ensure comprehensive coverage and identification of any hidden vulnerabilities.

3. **Continuous Monitoring:** Implement continuous monitoring solutions to detect and respond to potential threats in real-time.
4. **Security Awareness Training:** Regularly update and train staff on security best practices to mitigate risks associated with human error.
5. **Review and Update Security Policies:** Ensure that security policies are regularly reviewed and updated to reflect the latest threat landscape and organizational changes.

By maintaining these practices, the organization can continue to safeguard its digital assets effectively against potential threats.