1 Executive Security Assessment Report

1.1 Overview

A comprehensive security assessment was conducted on the domain **cmsauthoring.cbre.com**. The evaluation commenced on **March 18th at 16:00** and concluded after a duration of **00h:05m:40s**. The assessment was identified with tracking ID **148751da0798** and employed a Basic scan type. The analysis adhered to OWASP and OSCP methodologies, focusing on identifying High and Medium-risk issues within the web application and infrastructure.

1.2 Key Security Issues

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

1.3 Detailed Findings

1.3.1 Description

The recent security assessment revealed no High, Medium, or Low-risk issues. However, three informational findings were noted. All **11** scanned ports were filtered, indicating robust perimeter security controls such as firewalls and IPS/IDS systems. This suggests that automated scans may have been blocked, necessitating manual verification to ensure comprehensive coverage. The assessment confirmed that all hosts are on dedicated infrastructure, eliminating risks associated with shared hosting environments. Additionally, the geographic distribution analysis verified that all servers are located in the United States, with no presence in high-risk areas, maintaining a normal risk status.

1.3.2 Affected Assets

- Domain: **cmsauthoring.cbre.com**
- Total Scanned Ports: **11**
- Geographic Location of Servers: United States

1.4 Recommendations

Manual verification of perimeter security controls is recommended to confirm the effectiveness of automated scan results and ensure no critical vulnerabilities are overlooked. Implement continuous monitoring solutions to detect and respond to potential threats in real-time, enhancing the overall security posture. Schedule regular security audits to maintain up-to-date defenses against evolving threats and ensure compliance with industry standards. Periodically review the geographic distribution of servers to ensure they remain in low-risk areas, minimizing exposure to geopolitical threats.

1.5 General Recommendation

To maintain a robust security posture, it is recommended that the organization continues to invest in advanced security measures, including regular manual assessments and continuous monitoring solutions. This proactive approach will help in identifying potential vulnerabilities early and mitigating risks effectively. Additionally, staying informed about emerging threats and adapting security strategies accordingly will be crucial in safeguarding the organization's digital assets.