1 Executive Security Assessment Report

1.1 Introduction

The following security assessment was conducted on the domain **ma.cbre.se**. The analysis was initiated on **03-11** at **07:45** and completed in a duration of **00h:12m:18s**. The assessment was identified with tracking ID **021d11bebf20** and employed a **Basic** type analysis. The evaluation involved scanning for vulnerabilities in web applications and infrastructure using methodologies aligned with OWASP and OSCP standards. This report focuses on High and Medium-risk issues identified during the scan.

1.2 Summary of Findings

The security assessment identified a total of **18 issues**, categorized as **2 High-risk**, **1 Medium-risk**, **1 Low-risk**, and **14 informational**. The most critical findings include the presence of unencrypted HTTP traffic, affecting **2 URLs**, which poses significant risks such as data interception and man-in-the-middle attacks. Additionally, a High-risk shared hosting environment was detected with over **405,607** shared domains, increasing the potential for cross-site vulnerabilities. The Medium-risk issue involves an open HTTP port (**80**) without encryption, necessitating immediate review for HTTPS implementation.

1.3 Issues Table

Title	Risk
Unencrypted HTTP Traffic Detected	High
Shared Hosting Environment Analysis	High
Nmap Port Scan Results Analysis	Medium
Denial of Service (DoS) Vulnerability	Low

1.4 Detailed Findings

1.4.1 Unencrypted HTTP Traffic Detected

Description:

The analysis revealed that two URLs are utilizing unencrypted HTTP traffic, exposing sensitive data to interception and man-in-the-middle attacks. The affected URLs are `http://ma.cbre.se/auto/dashboa` and `http://165.160.13.20:80`. This lack of encryption compromises data integrity and authenticity and does not meet modern security standards.

Affected Assets:

- URLs: `http://ma.cbre.se/auto/dashboard/*`, `http://165.160.13.20:80`

Recommendations:

Immediate action should be taken to implement HTTPS across all URLs to ensure data is encrypted in transit, thereby protecting against interception and ensuring compliance with security policies.

1.4.2 Shared Hosting Environment Analysis

Description:

The domain **ma.cbre.se** operates within a High-risk shared hosting environment, with over **405,607** shared domains. This setup increases the risk of cross-site vulnerabilities due to shared infrastructure, potentially leading to unauthorized access and data leakage.

Affected Assets:
- Hostname: ma.cbre.se

Recommendations:
Evaluate the current hosting arrangement to determine if a dedicated hosting solution is feasible. Implement strict access controls and monitoring to mitigate risks associated with shared hosting environments.

1.4.3 Nmap Port Scan Results Analysis

Description:
The scan identified an open HTTP port (**80**) on IP **165.160.13.20**, which is not encrypted. This configuration is vulnerable to eavesdropping and other security threats due to the lack of encryption.

Affected Assets:
- IP: **165.160.13.20** - Port: **80/tcp** - Service: **http**

Recommendations:
Ensure that HTTP traffic is redirected to HTTPS, and enable HTTP Strict Transport Security (HSTS) to enforce secure connections.

1.4.4 Denial of Service (DoS) Vulnerability Assessment

Description:
A Low-risk DoS vulnerability was identified with a timeout percentage of **0.65%** on service ports **80 (HTTP)** and **443 (HTTPS)**. This suggests isolated incidents that do not currently pose a significant threat.

Affected Assets:
- Service Ports: 80 (HTTP), 443 (HTTPS)

Recommendations:
Continue to monitor server performance during peak events and optimize server responses to prevent potential DoS attacks.

1.5 General Recommendations

To enhance the overall security posture, prioritize the implementation of HTTPS across all services, review hosting configurations for potential vulnerabilities, and maintain continuous monitoring and assessment to detect and address security issues proactively.