



1 Security Assessment Report

Domain Analyzed: cbre.com.qa

Tracking ID: 1f05007820da

Type of Analysis: Basic Security Assessment

Initiation Date and Time: 04-10 14:45

Duration: 00h:09m:18s

This security assessment was conducted using OWASP and OSCP methodologies to evaluate the security posture of the domain cbre.com.qa. The analysis focused on identifying High and Medium-risk vulnerabilities that could impact the organization's infrastructure and web applications.

1.1 Short Summary of Main Issues

The assessment identified **3 Medium-risk** issues, including insecure HTTP ports, sensitive subdomains, and a shared hosting environment with **29 shared domains**. These findings highlight potential exposure to unauthorized access and data leakage risks. Immediate remediation is advised to enhance security controls.

1.2 Executive Summary

Title	Risk
Shared Hosting Environment Analysis	Medium
Nmap Port Scan Results Analysis	Medium
Subdomain Naming Security Assessment	Medium
SSL/TLS Protocols Security Assessment	Low
SSL Certificate Expiration Analysis	Low

Shared Hosting Environment Analysis Description:

The domain cbre.com.qa is hosted in a shared environment with **29 other domains**, categorized as Medium interest. Shared hosting can lead to security risks due to potential cross-site contamination and resource sharing vulnerabilities.

Affected Assets:

- Hostname: **cbre.com.qa**

Recommendations:

- Consider migrating to a dedicated hosting environment to isolate critical systems. - Implement strict access controls and monitoring to detect unauthorized activities.

Nmap Port Scan Results Analysis Description:

An open HTTP port (**80/tcp**) was detected on IP **20.10.162.75**, which lacks encryption, posing a risk of data interception. The presence of HTTPS on port **443/tcp** is noted, but it is crucial to ensure proper redirection from HTTP to HTTPS.

Affected Assets:

- IP: **20.10.162.75** - Ports: **80/tcp, 443/tcp**

Recommendations:

- Enforce HTTPS by redirecting all HTTP traffic to HTTPS. - Enable HTTP Strict Transport Security (HSTS) to prevent protocol downgrade attacks.



Subdomain Naming Security Assessment Description:

A sensitive subdomain associated with development or staging environments was identified, which may expose unpatched vulnerabilities or sensitive information.

Affected Assets:

- Subdomain: **cbre.com.qa**

Recommendations:

- Restrict access to development and staging environments. - Regularly audit subdomains for exposure of sensitive information.

1.3 General Recommendations

To mitigate the identified risks, it is recommended to prioritize securing HTTP services, review access controls for sensitive subdomains, and consider isolating shared hosting environments. Continuous monitoring and timely updates of security configurations will further strengthen the security posture of the domain cbre.com.qa.

PUBLIC REPORT - DEMO SCAN - NO INTRUSIVE TESTING