1 Executive Security Assessment Report

1.1 Analysis Overview

The security assessment was conducted on the domain **cov-cbre.be**. The analysis commenced on **April 25th** at **17:00** and concluded in **00h:13m:34s**. The scope of the work included a basic security scan focusing on identifying High and Medium-risk vulnerabilities within the web application and infrastructure.

1.2 Summary of Findings

The security assessment identified a total of **20** issues, categorized as **2** High-risk, **2** Medium-risk, and **16** informational. The most critical findings include the detection of unencrypted HTTP traffic affecting **2,330** URLs, posing significant risks of data interception and man-in-the-middle attacks, and a High-risk shared hosting environment with over **405,607** shared domains, which could lead to potential security breaches. Additionally, the absence of a Web Application Firewall (WAF) on **100%** of analyzed hosts increases vulnerability to cyber-attacks. Medium-risk issues also include insecure open ports, such as HTTP on port **80**, which lacks encryption. Immediate action is recommended to implement HTTPS and deploy a WAF to mitigate these risks and enhance security posture.

1.3 Key Security Issues

Title	Risk
Unencrypted HTTP Traffic Detected	High
Shared Hosting Environment Analysis	High
Absence of WAF	Medium
Nmap Port Scan Results Analysis	Medium

1.3.1 Unencrypted HTTP Traffic Detected

Description A total of 2,330 URLs were found using unencrypted HTTP protocol without any HTTPS alternatives. This exposes the application to significant risks such as data interception, eavesdropping, man-in-the-middle attacks, and compromise of sensitive information.

Affected Assets

- All identified URLs are using unencrypted HTTP protocol.

Recommendations

- Implement HTTPS across all URLs to ensure data encryption in transit.
- Enable HTTP Strict Transport Security (HSTS) to enforce secure connections.
- Regularly audit and update SSL/TLS configurations to adhere to best practices.

1.3.2 Shared Hosting Environment Analysis

Description The domain **cov-www.cbre.be** is hosted in a shared environment with over **405,607** shared domains, indicating a High-risk level due to potential exposure and security concerns.

Affected Assets

- Hostname: cov-www.cbre.be

Recommendations

- Consider migrating to a dedicated hosting environment to reduce exposure.
- Implement strict access controls and monitoring to detect unauthorized activities.
- Regularly review hosting configurations for compliance with security standards.

1.3.3 Absence of WAF

Description The absence of a Web Application Firewall (WAF) was noted on **100%** of analyzed hosts, significantly increasing the risk of successful cyber-attacks, particularly injection-based attacks.

Affected Assets

- Host: cov-www.cbre.be

Recommendations

- Deploy a Web Application Firewall (WAF) to filter and monitor HTTP traffic.
- Regularly update WAF rulesets to protect against emerging threats.
- Conduct periodic security assessments to ensure the effectiveness of WAF implementations.

1.3.4 Nmap Port Scan Results Analysis

Description Port **80** was identified as open and associated with HTTP service, which lacks encryption. This poses a risk due to the potential for data interception.

Affected Assets

- IP: (165.160.13.20)
- Port: 80/tcp

Recommendations

- Redirect HTTP traffic on port **80** to HTTPS.
- Implement HSTS to enforce secure connections.
- Regularly scan for open ports and ensure secure configurations.

1.4 General Recommendations

To enhance the overall security posture, it is recommended to implement comprehensive encryption strategies, including the deployment of HTTPS and HSTS across all web services. Additionally, transitioning from shared hosting environments to dedicated or cloud-based solutions can significantly reduce exposure risks. Deploying a Web Application Firewall (WAF) will provide an additional layer of defense against web-based attacks. Regular security assessments and audits should be conducted to ensure ongoing compliance with security best practices and standards.