1 Executive Security Assessment Report

1.1 Overview

The security assessment was conducted on the domain **trademarkgo365.no**. The analysis commenced on **April 25th at 20:45** and concluded in **00h:09m:06s**. The assessment utilized a Basic scan type and focused on identifying High and Medium-risk vulnerabilities, employing methodologies aligned with OWASP and OSCP standards.

1.2 Summary of Key Findings

The security assessment identified a total of **19 issues**, categorized as **2 High-risk**, **1 Medium-risk**, and **16 informational**. The most critical findings include the detection of unencrypted HTTP traffic across **4 URLs**, posing significant risks of data interception and man-in-the-middle attacks, and a High-risk shared hosting environment with over **51,000 shared domains** on a single host, potentially exposing sensitive data. Additionally, a Medium-risk issue was identified with open HTTP port **80**, lacking encryption, which could lead to data breaches. Immediate actions should focus on implementing HTTPS to secure data transmission and reviewing shared hosting configurations to mitigate exposure. These vulnerabilities highlight the need for enhanced security measures to protect sensitive information and maintain compliance with security standards.

1.3 Key Security Issues

Title	Risk
Shared Hosting Environment	High
Unencrypted HTTP Traffic	High
Nmap Port Scan Results	Medium

1.3.1 Shared Hosting Environment Analysis

Description:
The analysis revealed that the domain **trademarkgo365.no** is hosted in a High-risk shared environment with over **51,000 shared domains**. This configuration increases the risk of data leakage and unauthorized access due to shared infrastructure vulnerabilities.

Affected Assets:
- Hostname: **trademarkgo365.no**

Recommendations:
- Evaluate the current hosting environment and consider migrating to a dedicated or virtual private server to reduce exposure. - Implement strict access controls and monitoring to detect any unauthorized activities. - Regularly audit the hosting environment for potential security vulnerabilities.

1.3.2 Unencrypted HTTP Traffic Detected

Description:
A total of **4 URLs** were identified using unencrypted HTTP protocol, which exposes data to interception and man-in-the-middle attacks. The lack of HTTPS alternatives compromises data integrity and confidentiality.

Affected Assets:
- URLs: `-http://trademarkgo365.no/./-http://99.83.176.46:80-http://a44fc39dcd01d2028.awsgloba`
`-http://trademarkgo365.no:80`

Recommendations:
- Implement HTTPS across all web applications to ensure encrypted data transmission. - Utilize SSL/TLS certificates from a trusted certificate authority. - Enable HTTP Strict Transport Security (HSTS) to enforce secure connections.

1.3.3 Nmap Port Scan Results Analysis

Description:
The scan identified an open HTTP port **80** on IP **99.83.176.46**, which lacks encryption, posing a risk of data interception and unauthorized access.

Affected Assets:
- IP: **99.83.176.46** - Port: **80/tcp** - Service: **http** - Version: **awselb/2.0**

Recommendations:
- Redirect HTTP traffic to HTTPS to ensure secure communication. - Regularly update and patch services to mitigate known vulnerabilities. - Conduct periodic security assessments to identify and address emerging threats.

1.4 General Recommendations

To enhance the security posture of the domain **trademarkgo36[illegible]**, it is recommended to prioritize the implementation of HTTPS across all services, review hosting configurations for potential risks, and establish continuous monitoring and auditing processes. These actions will help safeguard sensitive information, ensure compliance with security standards, and mitigate the risk of data breaches.