1 Executive Security Assessment Report

1.1 Introduction

The security assessment was conducted on the domain **tmgo365.no**. The analysis commenced on **April 9th** at **01:00** and concluded in **00h:09m:39s**. The assessment was identified with tracking ID **05560ef66790** and was categorized as a **Basic** type scan. The evaluation focused on identifying High and Medium-risk vulnerabilities using OWASP and OSCP methodologies, ensuring a comprehensive review of the web application and infrastructure security posture.

1.2 Summary of Key Issues

The security assessment identified **3** High-risk, **1** Medium-risk, and **15** informational issues. Critical findings include the presence of unencrypted HTTP traffic affecting **4** URLs, posing risks of data interception and non-compliance with security standards. Additionally, a Denial of Service (DoS) vulnerability was detected on port **443**, with a **97.78%** timeout rate, indicating a High risk of service disruption. The shared hosting environment analysis revealed a host with over **51,000** shared domains, increasing exposure to potential security threats. Immediate actions include enforcing HTTPS across all web applications and addressing the DoS vulnerability to ensure service resilience.

1.3 Issues Table

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

1.3.1 Shared Hosting Environment Analysis

Description The analysis identified a High-risk shared hosting environment with **51,197** shared domains on the host **tmgo365.no**. This configuration significantly increases the attack surface, potentially allowing attackers to exploit vulnerabilities in one domain to compromise others.

Affected Assets

- Hostname: **tmgo365.no**

Recommendations It is recommended to evaluate the necessity of such extensive domain sharing and consider isolating critical services or domains into dedicated hosting environments to reduce exposure and potential attack vectors.

1.3.2 Unencrypted HTTP Traffic Detected

Description The assessment detected unencrypted HTTP traffic across **4** URLs, which exposes data to interception and eavesdropping risks. The lack of HTTPS compromises data integrity and authenticity, failing to meet security compliance requirements.

Affected Assets

- URLs:
  - `http://a44fc39dcd01d2028.awsglobalaccelerator.com/?#`
  - `http://99.83.176.46:80`
  - `http://a44fc39dcd01d2028.awsglobalaccelerator.com:80`
  - `http://tmgo365.no:80`

Recommendations Immediate implementation of HTTPS across all web applications is advised. Ensure that HTTP Strict Transport Security (HSTS) is enabled to enforce secure connections and prevent downgrade attacks.

1.3.3 Denial of Service (DoS) Vulnerability Assessment

Description A DoS vulnerability was identified on port **443** (HTTPS), with a **97.78%** timeout rate from **135** responses monitored. This indicates a severe risk of service disruption, potentially impacting availability.

Affected Assets

- Ports analyzed: **80** (HTTP) and **443** (HTTPS)

Recommendations Enhance server capacity and optimize configurations to handle peak loads effectively. Implement rate limiting and anomaly detection mechanisms to mitigate potential DoS attacks.

1.3.4 Nmap Port Scan Results Analysis

Description The scan revealed an open port **80** running HTTP service without encryption, which is vulnerable to data interception and man-in-the-middle attacks.

Affected Assets

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

Recommendations Ensure that all HTTP services are redirected to HTTPS, and enable HSTS to enforce secure communication protocols.

1.4 General Recommendation

To enhance the overall security posture, it is crucial to prioritize the remediation of High-risk vulnerabilities identified in this assessment. Implementing robust encryption protocols, optimizing server configurations, and reducing shared hosting dependencies will significantly mitigate potential threats. Regular security assessments should be conducted to ensure ongoing protection against emerging vulnerabilities.