1 Executive Security Assessment Report

1.1 Introduction

This security assessment was conducted on the domain **googlebrowser.no**. The analysis commenced on **March 31st** at **00:00** and concluded in **00h:09m:21s**. The assessment utilized a basic scan type, focusing on identifying High and Medium-risk vulnerabilities using OWASP and OSCP methodologies to ensure comprehensive coverage of potential security threats.

1.2 Short Summary of Main Issues

The security assessment identified a total of **18 issues**, categorized as **2 High-risk**, **2 Medium-risk**, and **14 informational**. The most critical findings include a Denial of Service (DoS) vulnerability on port 443, with a **96.97%** timeout rate, posing a significant risk to service availability. Additionally, a High-risk shared hosting environment was detected with over **262,000** domains sharing the same IP, potentially exposing sensitive data. Medium-risk issues include insecure HTTP port exposure and sensitive subdomain endpoints. Immediate actions should focus on mitigating the DoS vulnerability and securing the shared hosting environment to prevent potential data breaches and service disruptions.

1.3 Key Security Issues

Title	Risk
Denial of Service (DoS) Assessment	High
Shared Hosting Environment Analysis	High
Nmap Port Scan Results Analysis	Medium
Subdomain Naming Security Assessment	Medium

1.3.1 Denial of Service (DoS) Assessment

Description:
A significant Denial of Service (DoS) vulnerability was identified on port 443 (HTTPS), with a **96.97%** timeout rate. This indicates a severe risk to service availability, potentially allowing attackers to disrupt access to critical services.

Affected Assets:
- Port: **443 (HTTPS)**

Recommendations:
- Implement rate limiting and traffic filtering to mitigate potential DoS attacks. - Optimize server configurations to handle high traffic loads efficiently. - Regularly monitor server performance and establish alerts for unusual activity patterns.

1.3.2 Shared Hosting Environment Analysis

Description:
The domain **googlebrowser.no** is hosted in a High-risk shared environment with over **262,000** domains sharing the same IP address. This configuration increases the risk of data leakage and unauthorized access due to the shared nature of the hosting environment.

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

Recommendations:
- Consider migrating to a dedicated hosting environment to reduce exposure. - Implement

strict access controls and monitoring to detect unauthorized access attempts. - Regularly audit hosted applications for vulnerabilities that could be exploited in a shared environment.

1.3.3 Nmap Port Scan Results Analysis

Description:
Port 80 (HTTP) was identified as potentially insecure due to the lack of encryption, posing a risk if not redirected to HTTPS or if HTTP Strict Transport Security (HSTS) is not enabled.
Affected Assets:
- IP Address: **3.33.139.32** - Port: **80/tcp** - Service: **http**
Recommendations:
- Ensure all HTTP traffic is redirected to HTTPS. - Enable HSTS to enforce secure connections.
- Regularly review web server configurations for compliance with security best practices.

1.3.4 Subdomain Naming Security Assessment

Description:
A sensitive subdomain was identified, which may provide access to critical systems and sensitive data. The subdomain could expose development or staging environments that may contain unpatched vulnerabilities or debug information.
Affected Assets:
- Subdomain: **googlebrowser.no**
Recommendations:
- Conduct regular audits of subdomains to identify and secure sensitive endpoints. - Implement access controls and authentication mechanisms for sensitive subdomains. - Monitor subdomain activity for signs of unauthorized access or data exfiltration.

1.4 General Recommendation

To enhance overall security posture, it is recommended to implement a comprehensive security monitoring strategy that includes regular vulnerability assessments, real-time threat detection, and incident response planning. Additionally, adopting a proactive approach to patch management and configuration reviews will help mitigate potential risks and ensure compliance with industry standards.