1 Executive Security Assessment Report

1.1 Introduction

This security assessment was conducted on the domain **innography.idv.tw**. The analysis commenced on **March 23rd** at **19:00** and concluded after a duration of **12 minutes and 1 second**. The assessment was identified with tracking ID **04ee0316838f** and was performed using a Basic scan type. The evaluation focused on identifying High and Medium-risk vulnerabilities that could impact the security posture of the domain.

1.2 Summary of Findings

The security assessment identified **2** High-risk, **1** Medium-risk, and **15** informational issues. Critical findings include a Denial of Service (DoS) vulnerability on port **443**, with a **94%** timeout rate, posing a significant threat to service availability. Additionally, a High-risk shared hosting environment was detected, with over **262,000** domains sharing the same IP, increasing the risk of cross-domain vulnerabilities. A Medium-risk issue was found with HTTP services running on port **80** without encryption, necessitating verification of HTTPS redirection. Immediate actions should focus on mitigating the DoS vulnerability and securing the shared hosting environment to prevent potential disruptions and data breaches.

1.3 Key Security Issues

Title	Risk
Denial of Service (DoS)	High
Shared Hosting Environment	High
Nmap Port Scan Results	Medium

1.3.1 Denial of Service (DoS) Assessment

Description:

A Denial of Service (DoS) vulnerability was identified on port **443** (HTTPS), with an alarming timeout rate of **94.01%**. This indicates a significant risk to service availability, potentially allowing attackers to disrupt services by overwhelming the server with requests.

Affected Assets:

- Service Port: **443 (HTTPS)**

Recommendations:

- Implement robust rate limiting and traffic filtering mechanisms to mitigate potential DoS attacks. - Enhance server capacity and performance monitoring to quickly identify and respond to unusual traffic patterns. - Consider deploying a Web Application Firewall (WAF) to provide an additional layer of protection against DoS attacks.

1.3.2 Shared Hosting Environment Analysis

Description:

The domain is hosted in a shared environment with over **262,000** domains sharing the same IP address. This configuration poses a High risk due to potential cross-domain vulnerabilities, where an attack on one domain could affect others.

Affected Assets:

- Hostname: **innography.idv.tw**

Recommendations:

- Evaluate the feasibility of migrating to a dedicated hosting environment to reduce exposure to

cross-domain risks. - Regularly audit and monitor shared hosting configurations for any unauthorized changes or vulnerabilities. - Implement strict access controls and isolation measures to minimize the impact of potential security breaches.

1.3.3 Nmap Port Scan Results Analysis

Description:
Port **80** is running HTTP services without encryption, which is considered insecure. The absence of HTTPS or HSTS increases the risk of data interception and man-in-the-middle attacks.

Affected Assets:
- IP Address: **3.33.139.32** - Port: **80/tcp** - Service: **http** - Version: **awselb/2.0**

Recommendations:
- Ensure that all HTTP traffic is redirected to HTTPS to secure data in transit. - Enable HTTP Strict Transport Security (HSTS) to enforce secure connections. - Regularly update and patch web server software to protect against known vulnerabilities.

1.4 General Recommendations

To enhance the overall security posture, it is recommended to prioritize addressing High-risk vulnerabilities such as the DoS vulnerability and shared hosting risks. Implementing encryption for all web traffic and ensuring robust monitoring and response strategies will significantly reduce the likelihood of successful attacks. Regular security audits and adherence to best practices will further strengthen defenses against emerging threats.