1 Executive Security Assessment Report

1.1 Analysis Overview

The security assessment was conducted on the domain **ipsearching.co.uk**. The analysis commenced on **March 26th** at **23:00** and concluded in **10 minutes and 24 seconds**. The assessment type was classified as “Basic”. The evaluation focused on identifying High and Medium-risk vulnerabilities that could impact the security posture of the domain.

1.2 Summary of Key Issues

The security assessment identified a total of **18** issues, with **2** High-risk, **1** Medium-risk, **1** Low-risk, and **14** informational findings. The most critical issues include a High-risk shared hosting environment with over **262,000** shared domains, posing significant exposure to potential attacks, and a Denial of Service (DoS) vulnerability on port **443** with a **95.89%** timeout rate, indicating severe service disruption risks. Additionally, a Medium-risk issue was found with HTTP services running on port **80** without encryption, necessitating immediate review for HTTPS redirection or HSTS implementation. These vulnerabilities require urgent attention to mitigate potential business impacts, such as data breaches and service outages. It is recommended to prioritize securing the shared hosting environment and addressing the DoS vulnerability to enhance overall security posture.

1.3 Key Security Issues

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

1.3.1 Shared Hosting Environment Analysis

Description The analysis revealed that the domain **ipsearching.co.uk** is hosted in a High-risk shared environment with over **262,264** domains sharing the same IP address. This configuration significantly increases the risk of cross-domain attacks and data leakage.

Affected Assets

- Hostname: **ipsearching.co.uk**

Recommendations It is recommended to migrate to a dedicated hosting environment to reduce exposure to potential attacks. Implementing strict access controls and monitoring for unusual activities can further enhance security.

1.3.2 Denial of Service (DoS) Assessment

Description A critical DoS vulnerability was identified on port **443**, with a timeout rate of **95.89%**, indicating a High risk of service disruption. This could lead to significant downtime and affect business operations.

Affected Assets

- Port: **443 (HTTPS)**

Recommendations Immediate action is required to optimize server performance and resilience against DoS attacks. Consider implementing rate limiting, traffic filtering, and load balancing to mitigate this risk.

1.3.3 Nmap Port Scan Results Analysis

Description The scan identified that port **80** is open and running HTTP without encryption. This poses a risk as data transmitted over this connection can be intercepted.

Affected Assets

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

Recommendations It is crucial to enforce HTTPS by redirecting HTTP traffic and enabling HTTP Strict Transport Security (HSTS) to ensure data integrity and confidentiality.

1.4 General Recommendations

To enhance the overall security posture, it is advised to prioritize addressing High-risk vulnerabilities, particularly those related to shared hosting environments and DoS vulnerabilities. Regular security audits, continuous monitoring, and adopting best practices for web application security are essential steps in maintaining a robust defense against potential threats.