1 Executive Security Assessment Report

1.1 Introduction

This security assessment was conducted on the domain **precisionindexing.net** using our certified and qualified web application and infrastructure penetration testing tool. The analysis was performed in accordance with OWASP and OSCP methodologies. The assessment commenced on **03-11** at **11:45** and was completed in **00h:05m:22s**. The scope of the work involved a basic scan to identify potential vulnerabilities that could impact the security posture of the domain.

1.2 Summary of Findings

The security assessment identified a total of **18 issues**, categorized as follows: **1 High-risk**, **2 Medium-risk**, **1 Low-risk**, and **14 informational**. The most critical finding is a High-risk Denial of Service (DoS) vulnerability, with a **95.77% timeout rate** on HTTP port 80, necessitating immediate action to enhance server resilience and implement specific DoS protections. Additionally, the absence of a Web Application Firewall (WAF) on **100%** of analyzed hosts poses a Medium risk, increasing susceptibility to injection attacks. Another Medium-risk issue is the shared hosting environment, with one host sharing its IP with **65 other domains**, potentially impacting service integrity.

1.3 Key Security Issues

Title	Risk
Denial of Service (DoS) Vulnerability	High
Absence of WAF	Medium
Shared Hosting Environment Analysis	Medium
All Ports Filtered - Possible Security Controls	Low

1.3.1 Denial of Service (DoS) Vulnerability

Description:
A high severity DoS vulnerability was identified, characterized by a significant timeout rate on HTTP port 80. The analysis revealed an overall timeout percentage of **95.77%**, indicating a critical need for enhanced security configurations.

Affected Assets:
- **precisionindexing.net:80**

Recommendations:
Immediate implementation of DoS mitigation strategies is recommended, including rate limiting, traffic analysis, and deployment of anti-DoS technologies to prevent service disruptions.

1.3.2 Absence of WAF

Description:
The absence of a Web Application Firewall (WAF) was noted across all analyzed hosts, resulting in a **100% vulnerability rate**. This lack of protection increases the risk of successful cyber-attacks, particularly those involving injection-based methods.

Affected Assets:
- Host: **precisionindexing.net**

Recommendations:
Deploy a robust WAF to filter and monitor HTTP requests, providing an additional layer of defense against common web application attacks such as SQL injection and cross-site scripting (XSS).

1.3.3 Shared Hosting Environment Analysis

Description:
The domain is hosted in a shared environment with **65 other domains**, which may lead to security risks due to shared resources and potential cross-domain attacks.

Affected Assets:
- Hostname: **precisionindexing.net**

Recommendations:
Consider migrating to a dedicated hosting environment to minimize risks associated with shared hosting, ensuring better isolation and control over the hosting infrastructure.

1.3.4 All Ports Filtered - Possible Security Controls

Description:
All scanned ports were found to be filtered, indicating strong perimeter security controls such as firewalls and intrusion prevention systems.

Affected Assets:
- Network perimeter (all scanned ports)

Recommendations:
Maintain current security configurations while conducting regular audits to ensure that these controls remain effective against evolving threats.

1.4 General Recommendations

It is crucial to address the identified vulnerabilities promptly to enhance the security posture of the domain. Implementing comprehensive security measures such as deploying a WAF, improving DoS protections, and considering dedicated hosting solutions are recommended steps to mitigate risks and protect against unauthorized access and service disruptions. Regular security assessments should also be conducted to identify and remediate potential vulnerabilities proactively.