1 Executive Security Assessment Report

1.1 Introduction

This report presents the findings from a comprehensive security assessment conducted on the domain **monosem.in**. The analysis was initiated on **June 18th** at **15:45** and completed in a duration of **00h:13m:26s**. The assessment was performed using a Basic scan type, with tracking ID **05a99d3f678c**. The primary objective was to identify 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 findings. The most critical vulnerabilities include a Denial of Service (DoS) risk, with an alarming **93.26%** timeout rate on HTTP and **86.63%** on HTTPS, necessitating immediate action to enhance server resilience and implement specific DoS protections. Additionally, a High-risk shared hosting environment was detected, with one host sharing its IP with over **9,495** domains, potentially increasing exposure to security threats.

1.3 Issues Table

Title	Risk
Shared Hosting Environment	High
Denial of Service (DoS) Assessment	High

1.4 Detailed Findings

1.4.1 Shared Hosting Environment Analysis

Description

The analysis revealed that the domain **monosem.in** is hosted in a shared environment with its IP address being shared by over **9,495** domains. This high level of shared hosting increases the risk of cross-contamination and potential exposure to security threats due to the actions of other domains sharing the same server resources.

Affected Assets

- Hostname: **monosem.in**

Recommendations

- Transition to a dedicated hosting environment to minimize risks associated with shared hosting.
- Implement strict access controls and monitoring to detect any unauthorized activities.
- Regularly audit server configurations and update security patches promptly.

1.4.2 Denial of Service (DoS) Assessment

Description

The assessment identified significant vulnerabilities related to Denial of Service (DoS) attacks on service ports **80 (HTTP)** and **443 (HTTPS)**. The analysis recorded a total of **395** responses, with **355** timeouts, resulting in an overall timeout percentage of **89.87%**. Specifically, port 80 experienced a **93.26%** timeout rate, while port 443 had an **86.63%** timeout rate. These findings indicate a High risk of service disruption due to potential DoS attacks.

Affected Assets

- Service Ports: **80 (HTTP)**, **443 (HTTPS)**

Recommendations

- Implement robust DoS protection mechanisms, such as rate limiting and traffic filtering.
- Configure firewalls to limit the number of simultaneous connections from individual IP addresses.
- Enhance server performance monitoring to quickly identify and respond to unusual traffic patterns.
- Optimize server response configurations to reduce vulnerability to DoS attacks.

1.5 General Recommendations

To strengthen the security posture of **monosem.in**, it is recommended to prioritize addressing the High-risk vulnerabilities identified in this assessment. Transitioning to dedicated hosting and implementing comprehensive DoS protection measures are critical steps. Additionally, continuous monitoring and regular security audits should be conducted to ensure ongoing protection against emerging threats.