1 Executive Security Assessment Report

1.1 Introduction

This report outlines the findings from a comprehensive security assessment conducted on the domain **flyiin.com**. The analysis was initiated on **April 16th** at **23:00** and concluded in **00h:11m:33s**. The assessment, identified by tracking ID **03e11dc65f8c**, was performed using a Basic scan type, focusing on identifying High and Medium-risk vulnerabilities. The evaluation adhered to OWASP and OSCP methodologies, ensuring a thorough examination of the web application and infrastructure.

1.2 Summary of Key Issues

The security assessment identified a total of **18 issues**: **1 High-risk**, **2 Medium-risk**, **1 Low-risk**, and **14 informational**. The most critical finding is the High-risk shared hosting environment, with one host (**flyiin.com**) sharing its IP with over **439,000 domains**, posing significant security risks due to potential cross-domain vulnerabilities. Medium-risk issues include an open HTTP port (**80**) lacking encryption, which could expose sensitive data, and an SSL certificate nearing expiration in **77 days**, requiring prompt renewal to maintain secure communications. The assessment also noted that all servers are located in the USA, with no High-risk geographic distribution detected. Immediate actions should focus on mitigating the High-risk shared hosting and addressing the Medium-risk vulnerabilities to enhance overall security posture.

1.3 Issues Table

Title	Risk
Shared Hosting Environment Analysis	High
Nmap Port Scan Results Analysis	Medium
SSL Certificate Expiration Analysis	Medium
SSL/TLS Protocols Security Assess.	Low

1.3.1 Shared Hosting Environment Analysis

Description:

The domain **flyiin.com** is hosted in a shared environment with over **439,000 domains** on the same IP address. This configuration poses a High risk due to potential cross-domain vulnerabilities that could be exploited by malicious actors.

Affected Assets:

- Hostname: **flyiin.com**

Recommendations:

Consider migrating to a dedicated hosting environment to minimize the risk of cross-domain vulnerabilities. - Implement strict access controls and continuous monitoring to detect any unauthorized activities.

1.3.2 Nmap Port Scan Results Analysis

Description:

An open HTTP port (**80**) was detected without encryption, which could lead to exposure of sensitive data if not properly managed. The lack of encryption on HTTP traffic is a Medium risk that requires attention.

Affected Assets:

- IP Address: **23.236.62.147** - Ports: **80/tcp** (http), **443/tcp** (ssl/https)

Recommendations:
- Ensure that HTTP traffic is redirected to HTTPS to secure data in transit. - Enable HTTP Strict Transport Security (HSTS) to enforce secure connections.

1.3.3 SSL Certificate Expiration Analysis

Description:
The SSL/TLS certificate for **flyiin.com** is set to expire in **77 days**, placing it in the "Warning" category. Timely renewal is essential to maintain secure communications and avoid service disruptions.

Affected Assets:
- Domain: **flyiin.com**

Recommendations:
- Initiate the renewal process for the SSL/TLS certificate well before expiration. - Consider implementing automated certificate management solutions to prevent future lapses.

1.4 General Recommendations

To enhance the overall security posture, it is recommended to prioritize addressing High and Medium-risk issues identified in this assessment. Transitioning to dedicated hosting, securing HTTP traffic, and ensuring timely SSL/TLS certificate renewals are critical steps. Continuous monitoring and adherence to security best practices will further safeguard against potential threats.