1 Executive Security Assessment Report

1.1 Introduction

This report presents the findings from a security assessment conducted on the domain **platform.openai.com**. The assessment was initiated on **April 1st at 17:00** and completed in **12 minutes and 5 seconds**. The analysis was performed using a basic scanning methodology. The scope included a comprehensive evaluation of web application and infrastructure security, focusing on High and Medium-risk issues.

1.2 Summary of Findings

The security assessment identified a total of **18** issues, categorized as **0** High-risk, **3** Medium-risk, **2** Low-risk, and **13** informational. Key Medium-risk findings include the detection of potentially insecure ports (**80** and **8080**) that could expose the system to vulnerabilities and an SSL certificate nearing expiration in **80** days, which requires prompt renewal planning. The shared hosting environment was flagged as Medium interest due to **38** domains sharing the same IP, indicating potential exposure to shared infrastructure risks. Despite these concerns, the analysis showed no High-risk vulnerabilities, and all services are running on standard ports with no unusual assignments. Immediate actions should focus on addressing the Medium-risk issues to mitigate potential security threats and ensure continued compliance with security best practices.

1.3 Issues Table

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

1.4 Detailed Findings

1.4.1 Shared Hosting Environment Analysis

Description

The analysis identified a shared hosting environment for the domain **platform.openai.com**, with **38** domains sharing the same IP address. This configuration is categorized as Medium interest due to potential risks associated with shared infrastructure, such as cross-site contamination and resource contention.

Affected Assets:

- Hostname: **platform.openai.com**

Recommendations:

It is recommended to evaluate the necessity of shared hosting for critical applications. Consider migrating to a dedicated hosting environment to reduce exposure to shared infrastructure risks. Implement strict access controls and monitoring to detect any unauthorized activities.

1.4.2 Nmap Port Scan Results Analysis

Description:

The scan detected **4** open ports, with ports **80** and **8080** highlighted as potentially insecure.

Port **80** is associated with HTTP services lacking encryption, while port **8080** may expose web service vulnerabilities and proxy services.

Affected Assets:

- IP Address: **104.18.33.45** - Ports: **80/tcp, 443/tcp, 8080/tcp, 8443/tcp**

Recommendations:

Ensure that HTTP services on port **80** are redirected to HTTPS or have HSTS enabled to enforce secure connections. Review services running on port **8080** for vulnerabilities and consider restricting access to trusted sources only.

1.4.3 SSL Certificate Expiration Analysis

Description:

The SSL/TLS certificate for **platform.openai.com** is set to expire in **80** days, placing it in the "Warning" risk category. Timely renewal is necessary to maintain secure communications.

Affected Assets:

- Domain: **platform.openai.com**

Recommendations:

Initiate the renewal process for the SSL/TLS certificate well before expiration to avoid service disruptions. Implement automated monitoring for certificate expiration dates to ensure timely renewals in the future.

1.5 General Recommendations

To enhance overall security posture, it is advised to address Medium-risk issues promptly and continuously monitor for emerging threats. Regularly update software and systems, conduct periodic security assessments, and implement robust incident response plans to mitigate potential risks effectively.