1 Executive Security Assessment Report

1.1 Analysis Overview

The security assessment was conducted on the domain **smslistener.billmatrix.com**. The evaluation commenced on **April 3rd** at **02:45** and concluded after a duration of **00h:12m:44s**. The assessment was executed using a Basic scan type. The primary objective was to identify vulnerabilities within the web application and infrastructure, following OWASP and OSCP methodologies.

1.2 Short Summary of Main Issues

The security assessment identified a total of **18** issues, with **0** high-risk, **1** medium-risk, **1** low-risk, and **16** informational findings. The most significant issue is a medium-risk finding related to an open HTTP port (**80**) without encryption, which could expose sensitive data if not redirected to HTTPS. Additionally, the use of TLS **1.2**, while currently acceptable, lacks the enhanced security features of TLS **1.3**.

1.3 Key Security Issues

Title	Risk
Nmap Port Scan Results Analysis	Medium
SSL/TLS Protocols Security Assessment	Low

1.3.1 Nmap Port Scan Results Analysis

Description:

The assessment identified an open HTTP port (**80**) on the IP address **107.162.158.45**. This port is associated with an HTTP service that lacks encryption, posing a risk of data exposure if not properly managed. The absence of encryption on HTTP traffic can lead to interception and unauthorized access to sensitive information.

Affected Assets:

- **IP Address:** 107.162.158.45
- **Ports:** 80/tcp (http), 443/tcp (ssl/https)

Recommendations:

It is recommended to implement a redirection from HTTP to HTTPS to ensure all data in transit is encrypted. Additionally, enabling HTTP Strict Transport Security (HSTS) will help enforce secure connections and mitigate potential risks associated with unencrypted traffic.

1.3.2 SSL/TLS Protocols Security Assessment

Description:

The analysis revealed that the endpoint is utilizing TLS **1.2**, which is currently considered an acceptable minimum standard for secure communications. However, it lacks the advanced security features and performance improvements offered by TLS **1.3**.

Affected Assets:

- **Endpoint:** 1 endpoint using TLS 1.2

Recommendations:

To enhance security posture, it is advisable to upgrade to TLS **1.3**, which provides improved cryptographic algorithms and better performance. This upgrade will ensure compliance with current best practices for secure communications.

1.4 General Recommendations

To improve the overall security posture, it is crucial to address the medium-risk issue by enforcing HTTPS across all services and upgrading to TLS **1.3** where possible. Regular security assessments should be conducted to identify and mitigate emerging threats promptly. Implementing these recommendations will help safeguard sensitive data and maintain the integrity and confidentiality of communications within the network infrastructure.