1 Executive Security Assessment Report

1.1 Overview of the Security Assessment

The security assessment was conducted on the domain **agentphenix.billmatrix.com**. The analysis commenced on **April 3rd, 2025, at 04:00** and concluded in **00 hours, 12 minutes, and 25 seconds**. The assessment was categorized as a **Basic** type scan. The evaluation focused on identifying vulnerabilities within the web application and infrastructure using OWASP and OSCP methodologies.

1.2 Short Summary of Main Issues

The security assessment identified a total of **18 issues**, categorized as **0 High-risk**, **2 Medium-risk**, **1 Low-risk**, and **15 informational**. The most significant findings include medium-risk vulnerabilities related to open HTTP ports (port **80**) lacking encryption, which could expose sensitive data if not redirected to HTTPS, and a potential Denial of Service (DoS) vulnerability with a **0.09%** timeout rate on HTTPS (port **443**). These vulnerabilities could impact business continuity and data security. Additionally, the SSL/TLS assessment revealed that while TLS **1.2** is in use, there is no support for the more secure TLS **1.3** protocol. Actionable recommendations include enforcing HTTPS with HSTS, monitoring server performance for DoS resilience, and upgrading to TLS **1.3** to enhance security posture.

1.3 Key Security Issues

Title	Risk
Nmap Port Scan Results Analysis	Medium
Denial of Service (DoS) Vulnerability	Medium
SSL/TLS Protocols Security Assessment	Low

1.4 Nmap Port Scan Results Analysis

Description

The assessment identified that port **80** is open and running HTTP without encryption. This lack of encryption poses a risk as it can expose sensitive data if not properly redirected to HTTPS or if HTTP Strict Transport Security (HSTS) is not enabled.

Affected Assets

- **IP:** 107.162.176.32
- **Ports:** 80/tcp (HTTP), 443/tcp (SSL/HTTPS)

Recommendations

- Implement HTTPS redirection for all HTTP traffic.
- Enable HSTS to ensure all communications are encrypted.
- Regularly monitor and audit open ports to ensure compliance with security policies.

1.5 Denial of Service (DoS) Vulnerability Assessment

Description

A potential DoS vulnerability was identified with a **0.09%** timeout rate on HTTPS (port **443**). This indicates a possible isolated incident that could affect service availability.

Affected Assets

- **Port:** 80 (HTTP)

- **Port:** 443 (HTTPS)

Recommendations

- Monitor server performance during peak times to identify potential bottlenecks.
- Optimize server configurations to handle increased loads efficiently.
- Implement rate limiting and other DoS mitigation techniques to protect against service disruptions.

1.6 SSL/TLS Protocols Security Assessment

Description

The SSL/TLS assessment revealed that while TLS **1.2** is in use, there is no support for the more secure TLS **1.3** protocol. TLS **1.3** offers improved security and performance over its predecessors.

Affected Assets

- **Endpoints using TLS 1.2: 2**

Recommendations

- Upgrade to TLS **1.3** to enhance security and performance.
- Ensure all cryptographic protocols are up-to-date and configured according to best practices.
- Conduct regular audits of SSL/TLS configurations to maintain a robust security posture.

1.7 General Recommendation

To enhance the overall security posture, it is recommended to implement a comprehensive security strategy that includes regular vulnerability assessments, timely patch management, and continuous monitoring of network traffic. Adopting these measures will help mitigate risks, protect sensitive data, and ensure business continuity.