1 Executive Security Assessment Report

1.1 Introduction

This report presents the findings of a comprehensive security assessment conducted on the domain **registre.notebleue.pro**. The analysis was initiated on **July 23rd** at **11:45 AM** and completed in **00h:20m:49s**. The assessment was performed using a Basic scan methodology. The scope of the work included evaluating the web application and infrastructure security posture, focusing on identifying High and Medium-risk vulnerabilities.

1.2 Short Summary of Main Issues

The security assessment identified a total of **19** issues, categorized as **2** High-risk, **2** Medium-risk, **2** Low-risk, and **13** informational. Critical findings include vulnerabilities in SSL/TLS protocols, with TLS 1.0 and TLS 1.1 posing significant risks due to deprecated and exploitable weaknesses, and a High-risk Denial of Service (DoS) vulnerability with a **95.26%** timeout rate across key service ports, necessitating immediate mitigation to prevent service disruptions. Medium-risk issues such as the absence of a Web Application Firewall (WAF) and insecure open ports further elevate the risk of cyber-attacks. Addressing these vulnerabilities is crucial to safeguarding data integrity and ensuring uninterrupted service availability. Immediate actions include upgrading SSL/TLS protocols, implementing DoS protection, and enhancing WAF coverage to mitigate potential threats effectively.

1.3 Key Security Issues

Title	Risk
SSL/TLS Protocols Security Assessment	High
Denial of Service (DoS) Vulnerability	High
Absence of WAF	Medium
Nmap Port Scan Results Analysis	Medium
Shared Hosting Environment Analysis	Low
Services Vulnerable to Brute Force	Low

1.3.1 SSL/TLS Protocols Security Assessment

Description

The assessment revealed the presence of deprecated TLS protocols, specifically TLS 1.0 and TLS 1.1, which are vulnerable to known attacks such as BEAST and lack modern cryptographic algorithms. These protocols are considered insecure and pose a significant risk to data confidentiality and integrity.

Affected Assets:

- Endpoint with TLS 1.0: **registre.notebleue.pro** - Endpoint with TLS 1.1: **registre.notebleue.pro**

Recommendations:

Immediate upgrade to TLS 1.2 or higher is recommended, with a preference for TLS 1.3 to ensure optimal security and performance. Disabling support for deprecated protocols will mitigate the risk of exploitation.

1.3.2 Denial of Service (DoS) Vulnerability Assessment

Description:

The system is highly susceptible to DoS attacks, with a **95.26%** timeout rate observed across

HTTP and HTTPS services. This indicates a severe risk of service disruption, potentially impacting availability.

Affected Assets:

- HTTP Service: **registre.notebleue.pro:80** - HTTPS Service: **registre.notebleue.pro:443**

Recommendations:

Implement robust DoS protection mechanisms, such as rate limiting and traffic filtering, to reduce the likelihood of successful attacks. Regular monitoring and incident response planning are also advised.

1.3.3 Absence of WAF

Description:

The absence of a Web Application Firewall (WAF) exposes the application to various attack vectors, including injection attacks, due to a lack of filtering and monitoring capabilities.

Affected Assets:

- Host without WAF: **registre.notebleue.pro**

Recommendations:

Deploy a WAF to provide an additional layer of security by filtering malicious traffic and preventing unauthorized access attempts. Regularly update WAF rules to adapt to emerging threats.

1.3.4 Nmap Port Scan Results Analysis

Description:

The scan identified an open SMTP port (**25**) that is potentially insecure due to risks such as email spoofing and relay attacks.

Affected Assets:

- IP Address: **51.68.66.30** - Port: **25/tcp**

Recommendations:

Review the configuration of SMTP services to ensure secure communication practices are in place. Implement measures such as authentication requirements and encryption to mitigate associated risks.

1.4 General Recommendation

To enhance the overall security posture, it is recommended that all identified vulnerabilities be addressed promptly, prioritizing High-risk issues. Regular security assessments should be conducted to identify new vulnerabilities and ensure compliance with best practices. Additionally, implementing a comprehensive security strategy that includes continuous monitoring, incident response planning, and employee training will further strengthen defenses against potential threats.