1 Executive Security Assessment Report

1.1 Analysis Overview

The security assessment was conducted on the domain **0.watsons.com.ph**. The analysis commenced on **April 16th** at **17:45** and concluded in **00h:16m:27s**. The assessment was performed using a Basic scan type. The evaluation focused on identifying High and Medium-risk vulnerabilities within the web application and infrastructure, adhering to 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**, **1 Medium-risk**, **1 Low-risk**, and **16 informational**. The most significant finding is a Medium-risk issue related to an open HTTP port **80**, which lacks encryption and could expose sensitive data if not redirected to HTTPS. This vulnerability requires immediate attention to ensure data integrity and confidentiality. Additionally, the SSL/TLS protocols are secure, with all endpoints supporting TLS **1.2** and **1.3**, indicating strong encryption standards. No high-density service issues or shared hosting risks were detected, suggesting a well-managed infrastructure. It is recommended to address the HTTP port vulnerability and continue monitoring SSL certificate expiration to maintain a robust security posture.

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 analysis revealed that port **80** is open and running HTTP without encryption. This poses a risk as data transmitted over this port could be intercepted by malicious actors if not properly redirected to HTTPS or if HTTP Strict Transport Security (HSTS) is not enabled.

Affected Assets:
- **IP:** 104.93.21.107
- **Ports:** 80/tcp and 443/tcp

Recommendations:
- Implement a redirection from HTTP to HTTPS for all traffic to ensure data is encrypted during transmission. - Enable HSTS to enforce secure connections and prevent protocol downgrade attacks. - Regularly review and update security configurations to align with best practices.

1.3.2 SSL/TLS Protocols Security Assessment

Description:
The SSL/TLS assessment confirmed that all endpoints support TLS **1.2** and TLS **1.3**, which are considered secure protocols. No deprecated protocols such as SSLv3, TLS **1.0**, or TLS **1.1** were detected, indicating a strong encryption posture.

Affected Assets:
- **Endpoints with TLS 1.3: 2**
- **Endpoints with TLS 1.2: 2**

Recommendations:
- Continue monitoring for any updates in cryptographic standards and ensure compliance with the latest security protocols. - Schedule regular audits of SSL/TLS configurations to detect any potential weaknesses or misconfigurations. - Ensure that SSL certificates are valid and renewed before expiration to maintain trustworthiness.

1.4 General Recommendations

To maintain a strong security posture, it is crucial to address the identified Medium-risk issue promptly by enforcing HTTPS across all services. Regularly update security policies and configurations in line with emerging threats and best practices. Continuous monitoring and periodic security assessments are recommended to identify potential vulnerabilities early and mitigate risks effectively.