1 Executive Security Assessment Report

1.1 Introduction

The security assessment was conducted on the domain **ab.wc3.com** using a Basic scan type. The analysis commenced on **April 20th at 11:45** and concluded in **00h:12m:05s**. The scope of the work included a comprehensive evaluation of the domain's web application and infrastructure security posture, employing methodologies aligned with OWASP and OSCP standards. The focus was on identifying High and Medium-risk issues to ensure the protection of sensitive data and maintain the integrity of business operations.

1.2 Summary of Findings

The security assessment identified a total of **18** issues, categorized as **0** High-risk, **1** Medium-risk, **2** Low-risk, and **15** informational. The most significant finding is a Medium-risk issue related to an open HTTP port **80**, which lacks encryption and poses potential security risks if not redirected to HTTPS or secured with HSTS. This could expose sensitive data to interception, impacting business confidentiality and integrity. Additionally, SSL/TLS analysis revealed that while TLS **1.2** is in use, the absence of TLS **1.3** indicates room for improvement in encryption standards. The SSL certificate for the domain is set to expire in **124** days, requiring monitoring to avoid service disruptions. Overall, the assessment suggests a need for enhanced encryption practices and proactive certificate management to mitigate potential vulnerabilities.

1.3 Key Security Issues

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

1.3.1 Nmap Port Scan Results Analysis

Description:
The analysis identified an open HTTP port (**80**) on IP **107.162.168.81** that lacks encryption, posing a Medium risk. Without encryption, data transmitted over this port can be intercepted by unauthorized parties, potentially leading to data breaches and compromising business confidentiality.

Affected Assets:
- IP: **107.162.168.81** - Ports: **80/tcp** (http), **443/tcp** (ssl/https?)

Recommendations:
It is recommended to implement a redirection from HTTP to HTTPS and enable HTTP Strict Transport Security (HSTS) to enforce secure connections. This will ensure that all communications are encrypted, thereby protecting sensitive data from interception.

1.3.2 SSL/TLS Protocols Security Assessment

Description:
The assessment revealed that TLS **1.2** is currently in use, which is acceptable but does not include support for TLS **1.3**, the current best practice for enhanced security and performance. While no deprecated protocols were found, the absence of TLS **1.3** indicates an opportunity for improvement.

Affected Assets:

- **1** endpoint using TLS **1.2**

Recommendations:

Upgrade to TLS **1.3** to leverage its improved security features and performance benefits. This will provide stronger encryption and better protect against potential vulnerabilities associated with older protocols.

1.3.3 SSL Certificate Expiration Analysis

Description:

The SSL/TLS certificate for the domain **ab.wc3.com** is set to expire in **124** days, placing it in a "Monitor" status. Although not immediately critical, failure to renew the certificate in a timely manner could lead to service disruptions and loss of trust from users.

Affected Assets:

- Domain: **ab.wc3.com**

Recommendations:

Implement a monitoring system to track certificate expiration dates and ensure timely renewal processes are in place. This proactive approach will prevent service interruptions and maintain user trust.

1.4 General Recommendations

To enhance the overall security posture, it is advised to prioritize the implementation of HTTPS across all services, upgrade to TLS **1.3** where possible, and establish a robust certificate management process. Regular security assessments should be conducted to identify and address emerging vulnerabilities promptly.