



1 Executive Security Assessment Report

1.1 Introduction

This report presents the findings from a security assessment conducted on the domain **mynycb.caaweb.com**. The evaluation was performed using a Basic scan type, initiated on **05-07 at 09:45** and completed in **00h:09m:25s**. The scope of the analysis included a comprehensive review of the web application and its infrastructure, focusing on identifying potential vulnerabilities using OWASP and OSCP methodologies.

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 critical finding is the Medium-risk issue related to the Nmap port scan, which detected an open HTTP port (**80**) without encryption, potentially exposing sensitive data if not redirected to HTTPS. This vulnerability could lead to data interception, impacting business confidentiality and integrity. Additionally, the SSL/TLS analysis revealed the use of TLS **1.2**, which is acceptable but lacks the enhanced security of TLS **1.3**. The assessment also noted a Low-risk issue with login form detection indicating potential exposure to unauthorized access. It is crucial to address these vulnerabilities by enforcing HTTPS and considering an upgrade to TLS **1.3** to enhance security posture.

1.3 Issues Table

Title	Risk
Nmap Port Scan Results Analysis	Medium
SSL/TLS Protocols Security Assess.	Low
Login Form Detection Analysis	Low

1.4 Detailed Findings

1.4.1 Nmap Port Scan Results Analysis

Description:

The Nmap port scan revealed **2 open ports** on the IP address **66.22.56.177**. Port **80/tcp** is running HTTP without encryption, posing a risk unless mitigated by redirection to HTTPS or HSTS. This lack of encryption can lead to data interception, compromising confidentiality and integrity.

Affected Assets:

- IP: **66.22.56.177** with open ports **80/tcp** and **443/tcp**.

Recommendations:

Implement HTTPS redirection for all HTTP traffic. - Enable HTTP Strict Transport Security (HSTS) to enforce secure connections. - Regularly monitor and audit open ports to ensure compliance with security policies.

1.4.2 SSL/TLS Protocols Security Assessment

Description:

The SSL/TLS analysis identified that the endpoint is using TLS **1.2**, which is currently acceptable but does not offer the enhanced security features of TLS **1.3**. No endpoints were found using deprecated or vulnerable protocols such as SSLv3, TLS **1.0**, or TLS **1.1**.

Affected Assets:

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



Recommendations:

- Upgrade to TLS 1.3 to leverage improved security and performance. - Ensure all cryptographic settings are aligned with current best practices.

1.4.3 Login Form Detection Analysis

Description:

The assessment detected **1 login form** across the application, which includes username fields but lacks advanced security measures such as multi-factor authentication (MFA). This could potentially expose the application to unauthorized access attempts.

Affected Assets:

- URLs: - <https://mynycb.caaweb.com:443> - <http://mynycb.caaweb.com:80>

Recommendations:

- Implement multi-factor authentication (MFA) for all login interfaces. - Conduct regular security reviews of authentication mechanisms. - Ensure secure transmission of credentials over HTTPS.

1.5 General Recommendations

To enhance the overall security posture, it is recommended to enforce HTTPS across all services, upgrade cryptographic protocols to TLS 1.3 where possible, and implement multi-factor authentication for critical access points. Regular security audits and monitoring should be conducted to identify and mitigate emerging threats promptly.

PUBLIC REPORT - DEMO SCAN - NO INTRUSIVE TESTING