1 Executive Security Assessment Report

1.1 Introduction

This report presents the findings from a security assessment conducted on the domain **cbb.caaweb.com**. The assessment was initiated on **April 18th** at **01:46** and concluded in a duration of **00h:12m:32s**. The analysis was performed using a Basic scan methodology. The primary focus was on identifying High and Medium-risk vulnerabilities within the web application and infrastructure, following 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 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. This could expose sensitive data to interception, impacting data confidentiality. Additionally, the SSL/TLS analysis revealed that while TLS **1.2** is in use, there is no support for the more secure TLS **1.3**, and the SSL certificate is set to expire in **172** days, requiring monitoring. The assessment also confirmed no shared hosting environments or brute-force vulnerable services, indicating a generally secure infrastructure. Immediate actions should focus on securing the HTTP service and planning for SSL certificate renewal.

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 assessment identified an open HTTP port (port **80**) on IP **107.162.168.164** that lacks encryption. This poses a Medium risk as it may allow sensitive data to be intercepted by unauthorized parties if not properly redirected to HTTPS or if HSTS is not enabled.

Affected Assets:

- IP: **107.162.168.164** - Ports: **80/tcp** (http), **443/tcp** (ssl/https)

Recommendations:

It is recommended to enforce HTTPS redirection for all HTTP traffic and enable HTTP Strict Transport Security (HSTS) to ensure data confidentiality and integrity.

1.3.2 SSL/TLS Protocols Security Assessment

Description:

The SSL/TLS analysis revealed that the domain supports TLS **1.2** but lacks support for the more secure TLS **1.3** protocol. While TLS **1.2** is currently acceptable, adopting TLS **1.3** would enhance security and performance.

Affected Assets:

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

Recommendations:

Upgrade the server configuration to support TLS **1.3** to align with current best practices for security and performance improvements.

1.3.3 SSL Certificate Expiration Analysis

Description:
The SSL certificate for the domain **cbb.caaweb.com** is set to expire in **172** days, placing it in the “Monitor” category. This indicates that while immediate action is not required, the certificate should be monitored for timely renewal.

Affected Assets:
- HTTPS-enabled subdomain: **cbb.caaweb.com**

Recommendations:
Implement a monitoring process to track SSL certificate expiration dates and ensure timely renewal to maintain secure communications.

1.4 General Recommendations

To enhance the security posture of the domain **cbb.caaweb.com**, it is recommended to prioritize the implementation of HTTPS redirection and HSTS for all HTTP services, upgrade to TLS **1.3**, and establish a robust SSL certificate monitoring and renewal process. These actions will mitigate identified risks and align with industry best practices for web application security.