1 Executive Security Assessment Report

1.1 Introduction

The security assessment was conducted on the domain **crossriver.caaweb.com**. The analysis commenced on **April 14th** at **01:00** and concluded in **00h:12m:11s**. The assessment was identified with the tracking ID **090a28dc871c** and was categorized as a **Basic** type scan. The evaluation focused on identifying potential vulnerabilities within the web application and associated 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, **1** Medium, **2** Low, 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 assessment revealed that while TLS **1.2** is in use, the absence of TLS **1.3** indicates room for improvement in encryption standards. The analysis also confirmed no shared hosting environments or high-density services, suggesting a well-segmented infrastructure. Immediate actions should focus on securing the HTTP service and considering upgrades to TLS **1.3** to enhance security posture.

1.3 Key Security Issues

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

1.4 Nmap Port Scan Results Analysis

Description

The analysis identified an open HTTP port (**80/tcp**) on IP address **107.162.182.73**, which lacks encryption. This poses a Medium risk as it could allow sensitive data to be intercepted if not properly redirected to HTTPS or if HTTP Strict Transport Security (HSTS) is not enabled.

Affected Assets

- IP: **107.162.182.73**
- Ports: **80/tcp** (http), **443/tcp** (ssl/https)

Recommendations

It is recommended to enforce HTTPS by redirecting HTTP traffic to HTTPS and enabling HSTS to ensure secure communication. Additionally, regular monitoring of open ports should be conducted to detect any unauthorized access attempts.

1.5 SSL/TLS Protocols Security Assessment

Description

The assessment revealed that TLS **1.2** is currently in use, which is acceptable; however, TLS **1.3** is not implemented. The absence of TLS **1.3** indicates a potential area for improvement in encryption standards, as it offers enhanced security and performance benefits.

Affected Assets

PUBLIC REPORT - DEMO SCAN - NO INTRUSIVE TESTING

- **1** endpoint using TLS **1.2**
- No endpoints using TLS **1.3**, TLS **1.1**, TLS **1.0**, or SSLv3

Recommendations

Upgrade to TLS **1.3** to leverage its improved security features and performance enhancements. Ensure that deprecated protocols such as SSLv3, TLS **1.0**, and TLS **1.1** remain disabled to prevent vulnerabilities like POODLE and BEAST attacks.

1.6 Login Form Detection Analysis

Description

A single login form was detected on the application, which is considered Low risk under normal circumstances. However, it is crucial to ensure that authentication interfaces are secure against common threats such as brute force attacks and credential stuffing.

Affected Assets

- URLs:
  - `http://crossriver.caaweb.com:80`
  - `https://crossriver.caaweb.com:443`

Recommendations

Implement strong authentication mechanisms such as multi-factor authentication (MFA) and rate limiting on login attempts to enhance security. Regularly review and update security measures to protect against evolving threats.

1.7 General Recommendations

To enhance the overall security posture, it is recommended to prioritize the implementation of HTTPS across all services and upgrade to TLS **1.3** where possible. Regular security audits should be conducted to identify and mitigate emerging threats promptly. Additionally, maintaining a robust incident response plan will ensure swift action in the event of a security breach.

PUBLIC REPORT - DEMO SCAN - NO INTRUSIVE TESTING