1 Executive Security Assessment Report

1.1 Introduction

The security assessment was conducted on the domain **css.transunion.com** using a Basic scan type. The analysis commenced on **May 13th** at **18:00** and concluded in **00h:09m:56s**. The tracking ID for this assessment is **0455d0d9775d**. The evaluation focused on identifying potential vulnerabilities within the web application and infrastructure, following OWASP and OSCP methodologies. This report highlights the critical findings and provides actionable recommendations to enhance the security posture of the assessed domain.

1.2 Summary of Findings

The security assessment identified a total of **18 issues**, categorized as **0 High**, **3 Medium**, **1 Low**, and **14 informational**. Key medium-risk findings include the detection of potentially insecure ports (HTTP on port **80** and **8080**) which could expose the organization to unencrypted data transmission risks, and SSL certificate expiration within **38 days**, necessitating prompt renewal to avoid service disruptions. Additionally, three login forms were detected, indicating a medium interest level that requires further security validation to prevent unauthorized access. The assessment also confirmed that all services are running on standard ports, and no shared hosting environments or brute-force susceptible services were found, reflecting a generally secure infrastructure. Immediate attention to the medium-risk issues is recommended to mitigate potential vulnerabilities.

1.3 Issues Table

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

1.4 Detailed Findings

1.4.1 Nmap Port Scan Results Analysis

Description:
The scan identified **4 open ports** on the IP address **172.83.72.32**, with services running on ports **80/tcp, 443/tcp, 8080/tcp, and 8443/tcp**. Ports **80** and **8080** are flagged for potential security risks due to lack of encryption and possible web service vulnerabilities.
Affected Assets:
- IP Address: **172.83.72.32** - Services running on ports: **80/tcp, 443/tcp, 8080/tcp, 8443/tcp**
Recommendations:
- Implement HTTPS redirection for services running on port **80**. - Ensure HSTS is enabled to enforce secure connections. - Regularly update and patch web services to mitigate vulnerabilities associated with proxy services on port **8080**.

1.4.2 SSL Certificate Expiration Analysis

Description:
The SSL certificate for the domain **css.transunion.com** is set to expire in **38 days**, placing it in the "Warning" category. This necessitates planning for renewal to prevent service disruptions.

Affected Assets:

- Domain: **css.transunion.com**

Recommendations:

- Initiate the renewal process for the SSL certificate immediately to ensure continuity of secure communications. - Implement monitoring tools to alert administrators of upcoming certificate expirations.

1.4.3 Login Form Detection Analysis

Description:
A total of **3 login forms** were detected across various URLs, indicating a medium interest level that requires further security validation to prevent unauthorized access.

Affected Assets:

- URLs: - `http://css.transunion.com:8080` - `http://css.transunion.com:80` - `http://172.83.72.32:80` - `http://172.83.72.32:8080` - `http://css.transunion.com/cdn-cgi/l/email-protection#`

Recommendations:

- Conduct thorough security assessments of all login forms to ensure they are protected against common vulnerabilities such as SQL injection and cross-site scripting (XSS). - Implement multi-factor authentication (MFA) to enhance login security. - Ensure all login forms transmit data over HTTPS to protect user credentials.

1.5 General Recommendation

To maintain a robust security posture, it is crucial to address the identified medium-risk issues promptly. Regular security assessments should be conducted to identify new vulnerabilities and ensure compliance with best practices. Additionally, implementing continuous monitoring solutions will help detect and respond to potential threats in real-time, further safeguarding the organization's digital assets.