1 Executive Security Assessment Report

1.1 Introduction

This report presents the findings from a comprehensive security assessment conducted on the domain **deposits.digitalcommerce.truist.com**. The assessment was performed using OWASP and OSCP methodologies, focusing on web application and infrastructure security. The analysis was initiated on **April 12th at 06:45** and concluded in **00h:09m:47s**. The scope included a basic scan of the domain to identify potential vulnerabilities.

1.2 Summary of Key Findings

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**) on Amazon CloudFront, which lacks encryption and requires verification for HTTPS redirection or HSTS implementation. This poses a potential risk for data interception. Additionally, SSL/TLS analysis revealed that all endpoints support modern TLS **1.3**, with no deprecated protocols detected, ensuring strong encryption standards. The SSL certificate for the domain is set to expire in **91** days, necessitating monitoring for timely renewal. Overall, the assessment indicates a robust security posture with minor areas for improvement, particularly in ensuring secure communication channels.

1.3 Issues Table

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

1.4 Detailed Findings

1.4.1 Nmap Port Scan Results Analysis

Description:
The analysis identified an open HTTP port (**80**) on Amazon CloudFront that lacks encryption. This configuration can expose data to interception risks if not properly redirected to HTTPS or secured with HSTS.

Affected Assets:
- **IP:** 18.160.172.84
- **Ports:** 80/tcp, 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 confirmed that all endpoints support modern TLS **1.3**, with no deprecated protocols detected. This ensures strong encryption standards across the domain.

Affected Assets:
- **4** endpoints using TLS **1.3**. - **4** endpoints using TLS **1.2**.

Recommendations:
- Continue supporting TLS **1.3** as the primary protocol for enhanced security. - Ensure regular updates and patches are applied to maintain protocol integrity. - Monitor for any future deprecations or vulnerabilities in TLS protocols.

1.4.3 SSL Certificate Expiration Analysis

Description:
The SSL/TLS certificate for the domain is set to expire in **91** days, categorized under “Monitor” status. Timely renewal is essential to maintain secure communications.

Affected Assets:
- **Domain:** deposits.digitalcommerce.truist.com

Recommendations:
- Schedule a renewal process for the SSL certificate well before the expiration date. - Implement automated alerts to notify relevant personnel of upcoming expirations. - Consider longer validity periods for certificates where applicable, balancing security and operational needs.

1.5 General Recommendations

To enhance the overall security posture, it is recommended to implement a continuous monitoring strategy that includes regular vulnerability assessments and penetration testing. This proactive approach will help identify and mitigate potential risks before they can be exploited. Additionally, maintaining up-to-date security policies and ensuring all systems are patched against known vulnerabilities will further strengthen defenses against cyber threats.