1 Executive Security Assessment Report

1.1 Overview

This security assessment was conducted on the domain **cccenduser.com**. The analysis commenced on **07-02** at **17:45** and concluded after a duration of **00h:10m:36s**. The assessment was executed as a Basic type scan. The evaluation focused on identifying High and Medium-risk vulnerabilities, utilizing methodologies aligned with OWASP and OSCP standards.

1.2 Summary of Key Findings

The security assessment identified **2** High-risk, **1** Medium-risk, and **16** informational issues. Critical findings include the detection of unencrypted HTTP traffic, affecting **4** URLs, which poses significant risks such as data interception and man-in-the-middle attacks, potentially compromising sensitive information. Additionally, a Denial of Service (DoS) vulnerability was found on port **443**, with a **97.97%** timeout rate, indicating a High risk of service disruption. The Medium-risk issue involves an open HTTP port (**80**) lacking encryption, necessitating immediate review for HTTPS implementation. These vulnerabilities highlight the need for enhanced encryption protocols and robust server monitoring to mitigate potential security breaches.

1.3 Issues Table

Title	Risk
Unencrypted HTTP Traffic Detected	High
Denial of Service (DoS) Vulnerability	High
Nmap Port Scan Results Analysis	Medium

1.4 Detailed Findings

1.4.1 Unencrypted HTTP Traffic Detected

Description:
Unencrypted HTTP traffic was detected across **4** URLs, exposing them to significant risks such as data interception and man-in-the-middle attacks. This lack of encryption compromises sensitive information, including login credentials, and fails to meet security compliance requirements.

Affected Assets:
-`http://cccenduser.com/../` -`http://cccenduser.com/./` -`http://99.83.176.46:80` -`http://cccenduser.com:80`

Recommendations:
Immediate implementation of HTTPS is recommended for all affected URLs to ensure data integrity and confidentiality. Enabling HTTP Strict Transport Security (HSTS) can further enhance security by enforcing secure connections.

1.4.2 Denial of Service (DoS) Vulnerability

Description:
A potential DoS vulnerability was identified on port **443** (HTTPS), with a **97.97%** timeout rate, indicating a High risk of service disruption. This could lead to significant downtime and affect service availability.

Affected Assets:
- Port **443** (HTTPS): High severity

Recommendations:
Enhance server monitoring and optimize server response to mitigate DoS risks. Implementing rate limiting and traffic analysis can help identify and prevent potential DoS attacks.

1.4.3 Nmap Port Scan Results Analysis

Description:
The scan revealed an open HTTP port (**80**) without encryption, posing a Medium risk due to potential data interception. This port is associated with the service version awselb/2.0.

Affected Assets:
- IP: **99.83.176.46** - Port: **80/tcp** - Service: **http** - Version: **awselb/2.0**

Recommendations:
Verify if there is a redirection to HTTPS or if HSTS is enabled for the affected port. Transitioning to HTTPS will secure data transmission and reduce the risk of interception.

1.5 General Recommendations

To address the identified vulnerabilities, it is crucial to implement comprehensive encryption protocols across all web services, ensuring that HTTPS is enforced site-wide. Regular monitoring and performance optimization should be conducted to detect and mitigate potential DoS attacks promptly. Additionally, conducting periodic security assessments will help maintain robust security postures and compliance with industry standards.