1 Executive Security Assessment Report

1.1 Introduction

This report presents the findings from a security assessment conducted on the domain **kyc-src.etoro.com**. The analysis was performed using a Basic scan methodology, adhering to OWASP and OSCP standards. The assessment commenced on **04-10** at **09:00** and concluded in **00h:16m:06s**. The primary focus was on identifying High and Medium-risk vulnerabilities that could impact the security posture of the domain.

1.2 Summary of Findings

The security assessment identified a total of **18 issues**, categorized as **0 High-risk**, **2 Medium-risk**, **2 Low-risk**, and **14 informational**. Key findings include Medium-risk vulnerabilities such as an open HTTP port 80, which lacks encryption, posing potential data interception risks, and an SSL certificate nearing expiration in **82 days**, which could impact secure communications if not renewed. Low-risk issues include the presence of login forms that require validation to prevent unauthorized access. Notably, **100%** of servers are located in the USA, with no High-risk geographic locations detected. The assessment emphasizes the need for immediate attention to Medium-risk vulnerabilities and proactive monitoring of SSL certificates to maintain secure operations.

1.3 Issues Table

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

1.3.1 Nmap Port Scan Results Analysis

Description:
The scan identified an open HTTP port 80 on IP **128.251.126.175**, which lacks encryption. This poses a risk of data interception and unauthorized access if not properly redirected to HTTPS or if HTTP Strict Transport Security (HSTS) is not enabled.

Affected Assets:
- IP: **128.251.126.175** - Ports: 80/tcp (http), 443/tcp (ssl/https)

Recommendations:
It is recommended to enforce HTTPS by redirecting HTTP traffic and enabling HSTS to ensure data integrity and confidentiality.

1.3.2 SSL Certificate Expiration Analysis

Description:
The SSL certificate for the domain **kyc-src.etoro.com** is set to expire in **82 days**, placing it in the “Warning” category. Failure to renew the certificate could disrupt secure communications.

Affected Assets:
- HTTPS-enabled subdomain: **kyc-src.etoro.com**

Recommendations:
Initiate the renewal process for the SSL certificate promptly to avoid any disruption in secure communications.

1.3.3 SSL/TLS Protocols Security Assessment

Description:
The assessment confirmed that TLS 1.3 is supported, which is ideal for security, while TLS 1.2 remains acceptable as a minimum standard. No deprecated protocols were detected, indicating a strong security posture.

Affected Assets:
- 1 endpoint with TLS 1.3 - 1 endpoint with TLS 1.2

Recommendations:
Continue monitoring for any updates in cryptographic standards and ensure that all endpoints are configured to support the latest protocols.

1.3.4 Login Form Detection Analysis

Description:
A login form was detected on the domain, which requires validation to prevent unauthorized access and ensure secure authentication processes.

Affected Assets:
- URLs: - `http://128.251.126.175/as/d/ccm/conversion` - `http://kyc-src.etoro.com:80`

Recommendations:
Implement robust authentication mechanisms, including input validation and secure transmission of credentials, to protect against unauthorized access.

1.4 General Recommendation

To maintain a robust security posture, it is crucial to address Medium-risk vulnerabilities promptly and ensure continuous monitoring of SSL certificates. Regular updates and adherence to best practices in encryption and authentication will further enhance the security of the domain.