1 Executive Security Assessment Report

1.1 Analysis Overview

The security assessment was conducted on the domain `cpwrfcu-di.apps-uat.ilendx.tech` using a Basic scan type. The analysis commenced on March 19 at **15:45** and concluded in **8** minutes and **50** seconds. The tracking ID for this assessment is `076e1182caa4`. The evaluation focused on identifying High and Medium-risk vulnerabilities within the web application and infrastructure, following OWASP and OSCP methodologies.

1.2 Summary of Findings

The security assessment identified a total of **18 issues**, categorized as **0 High-risk**, **4 Medium-risk**, **1 Low-risk**, and **13 informational**. Key Medium-risk findings include the exposure of potentially insecure HTTP ports and sensitive subdomains, which could lead to unauthorized access or data exposure. Additionally, the SSL certificate for one domain is nearing expiration within **49** days, necessitating prompt renewal to maintain secure communications. The analysis also revealed that all services are running on standard ports, and no brute-force vulnerable services were detected, indicating a generally secure configuration. Immediate attention to Medium-risk issues and proactive management of SSL certificates are recommended to mitigate potential security threats.

1.3 Issues Table

Title	Risk
Nmap Port Scan Results Analysis	Medium
Subdomain Naming Security Assessment	Medium
API Surface Analysis	Medium
SSL Certificate Expiration Analysis	Medium
SSL/TLS Protocols Security Assessment	Low

1.3.1 Nmap Port Scan Results Analysis

Description

The assessment identified **2** open ports on IP **66.6.26.167**: port **80/tcp** (HTTP) and port **443/tcp** (SSL/HTTPS). Port **80** is flagged as potentially insecure due to the lack of encryption, which requires verification for HTTPS redirection or HSTS implementation.

Affected Assets

- IP: **66.6.26.167** - Ports: **80/tcp** (http), **443/tcp** (ssl/https)

Recommendations

Ensure that HTTP traffic is redirected to HTTPS and that HSTS is enabled to enforce secure connections. Regularly review open ports and services for potential vulnerabilities.

1.3.2 Subdomain Naming Security Assessment

Description

A sensitive subdomain, `cpwrfcu-di.apps-uat.ilendx.tech`, was identified as a development/staging environment. Such environments may expose administrative interfaces or internal systems, increasing the risk of unauthorized access or data exposure.

Affected Assets

- Subdomain: `cpwrfcu-di.apps-uat.ilendx.tech`

Recommendations

Restrict access to development and staging environments through IP whitelisting or VPN access. Regularly audit subdomains for sensitive information exposure and apply security patches promptly.

1.3.3 API Surface Analysis

Description

The endpoint `cpwrfcu-di.apps-uat.ilendx.tech` was confirmed as an API with **99%** confidence based on response validation. It is identified as being in a non-production environment, which serves as an additional risk indicator.

Affected Assets

- Endpoint: `cpwrfcu-di.apps-uat.ilendx.tech`

Recommendations

Implement strict access controls and authentication mechanisms for APIs, especially in non-production environments. Regularly test APIs for security vulnerabilities and ensure sensitive data is not exposed.

1.3.4 SSL Certificate Expiration Analysis

Description

The SSL certificate for the domain `cpwrfcu-di.apps-uat.ilendx.tech` is set to expire in **49** days, placing it in a warning status. Timely renewal is necessary to maintain secure communications.

Affected Assets

- Domain: `cpwrfcu-di.apps-uat.ilendx.tech`

Recommendations

Schedule the renewal of the SSL certificate well before expiration to avoid service disruptions. Implement automated monitoring for certificate expiration dates to ensure timely renewals.

1.4 General Recommendations

To enhance overall security posture, it is recommended to implement a comprehensive vulnerability management program that includes regular security assessments, timely patch management, and continuous monitoring of network traffic and system logs. Additionally, ensure that all sensitive environments are adequately protected with strong authentication mechanisms and access controls.