1 Executive Security Assessment Report

1.1 Introduction

This report presents the findings of a security assessment conducted on the domain **fvcbank-di.apps-uat.ilendx.tech**. The assessment was performed using a basic scan methodology, adhering to OWASP and OSCP standards. The analysis commenced on **05-09** at **15:00** and concluded in **00h:10m:07s**. The primary focus was on identifying High and Medium-risk vulnerabilities that could impact the security posture of the target domain.

1.2 Short Summary of Main Issues

The security assessment identified **3** Medium-risk, **1** Low-risk, and **14** informational issues. Notably, Medium-risk findings include insecure HTTP port (**80**) usage, which lacks encryption and could expose sensitive data, and sensitive subdomain naming that may reveal critical systems. Additionally, an API endpoint was confirmed in a non-production environment, potentially increasing exposure to unauthorized access. The SSL/TLS assessment showed reliance on TLS **1.2** without TLS **1.3**, indicating room for improvement in encryption standards. While no High-risk issues were found, addressing these Medium-risk vulnerabilities is crucial to enhance security posture and protect against potential breaches.

1.3 Key Security Issues

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

1.3.1 Nmap Port Scan Results Analysis

Description:

An analysis of open ports revealed the use of port **80** for HTTP services, which is unencrypted and poses a risk of exposing sensitive data during transmission. The presence of port **443** for HTTPS was noted, but it is crucial to ensure that all HTTP traffic is redirected to HTTPS or that HSTS is enabled.

Affected Assets:

- IP: **66.6.26.167** - Ports: **80/tcp**, **443/tcp**

Recommendations:

Implement HTTPS redirection for all HTTP traffic and enable HSTS to ensure secure data transmission. Regularly review and update SSL/TLS configurations to adhere to best practices.

1.3.2 Subdomain Naming Security Assessment

Description:

The subdomain **fvcbank-di.apps-uat.ilendx.tech** was identified as part of a development or staging environment. Such environments may contain unpatched vulnerabilities or debug information that could be exploited by attackers.

Affected Assets:

- Subdomain: **fvcbank-di.apps-uat.ilendx.tech**

Recommendations:
Restrict access to development and staging environments through IP whitelisting or VPN access. Regularly audit these environments for security vulnerabilities and ensure they do not expose sensitive information.

1.3.3 API Surface Analysis

Description:
The endpoint **fvcbank-di.apps-uat.ilendx.tech** was confirmed as an API with a high level of confidence. It is located in a non-production environment, which can increase the risk of unauthorized access if not properly secured.

Affected Assets:
- Endpoint: **fvcbank-di.apps-uat.ilendx.tech**

Recommendations:
Ensure that non-production APIs are secured with authentication mechanisms and are not exposed to the public internet. Implement logging and monitoring to detect unauthorized access attempts.

1.4 General Recommendation

To enhance the overall security posture, it is recommended to address the identified Medium-risk vulnerabilities promptly. This includes enforcing HTTPS across all services, securing non-production environments, and regularly updating SSL/TLS configurations to support modern encryption standards like TLS **1.3**. Continuous monitoring and periodic security assessments should be conducted to identify and mitigate emerging threats effectively.