1 Executive Security Assessment Report

1.1 Introduction

The security assessment was conducted on the domain `fnblecenter-cs.apps-uat.ilendx.tech`. The analysis commenced on July 30th at 10:45 and concluded in **00h:20m:02s**. This basic security scan aimed to identify potential vulnerabilities within the web application and infrastructure, utilizing methodologies aligned with OWASP and OSCP standards.

1.2 Short Summary of Main Issues

The security assessment identified a total of **19 issues**, categorized as **0 High**, **3 Medium**, **1 Low**, and **15 informational**. The most critical findings include the absence of a Web Application Firewall (WAF) on **100%** of analyzed hosts, significantly increasing the risk of cyber-attacks, particularly injection-based attacks. Additionally, the Nmap port scan revealed the use of HTTP on port 80 without encryption, which requires immediate attention to ensure secure data transmission. The subdomain naming security assessment highlighted potentially sensitive endpoints, such as development environments, which could expose critical systems to unauthorized access. While SSL/TLS protocols are generally secure with TLS 1.2 in use, the lack of TLS 1.3 support suggests room for improvement. Addressing these vulnerabilities is crucial to enhancing the organization's security posture and protecting sensitive data.

1.3 Key Security Issues

Title	Risk
Absence of WAF	Medium
Nmap Port Scan Results Analysis	Medium
Subdomain Naming Security Assessment	Medium
SSL/TLS Protocols Security Assessment	Low

1.3.1 Absence of WAF

Description:

The absence of a Web Application Firewall (WAF) was detected on all analyzed hosts, resulting in a **100% vulnerability rate**. This significantly elevates the risk of successful cyber-attacks, particularly those involving injection-based attacks. Without WAF protection, unauthorized data access, data breaches, and potential system compromise are more likely.

Affected Assets:

- Host: `fnblecenter-cs.apps-uat.ilendx.tech`

Recommendations:

Implement a robust Web Application Firewall to monitor and filter HTTP traffic between the web application and the internet. This will help mitigate risks associated with injection attacks and unauthorized access attempts.

1.3.2 Nmap Port Scan Results Analysis

Description:

The Nmap port scan identified **2 open ports**, with port 80 (HTTP) flagged as potentially insecure due to the lack of encryption. This poses a risk as data transmitted over HTTP can be intercepted by attackers.

Affected Assets:

- IP: `66.6.26.168`

Recommendations:
Ensure that HTTP traffic is redirected to HTTPS and consider enabling HTTP Strict Transport Security (HSTS) to enforce secure connections. This will protect data integrity and confidentiality during transmission.

1.3.3 Subdomain Naming Security Assessment

Description:
A sensitive subdomain categorized under "Development/Staging" was identified, posing a Medium risk level. Such environments may expose critical systems and sensitive data due to potential unpatched vulnerabilities or debug information.

Affected Assets:
- Subdomain: `fnblecenter-cs.apps-uat.ilendx.tech`

Recommendations:
Restrict access to development and staging environments through IP whitelisting or VPN access. Regularly audit these environments for vulnerabilities and ensure they are patched promptly.

1.3.4 SSL/TLS Protocols Security Assessment

Description:
The assessment found that TLS 1.2 is in use, which is currently acceptable; however, there is no support for TLS 1.3, which offers improved security and performance.

Affected Assets:
- Endpoint using TLS 1.2

Recommendations:
Upgrade to TLS 1.3 where possible to enhance security and performance. Ensure all cryptographic protocols are up-to-date and configured according to best practices.

1.4 General Recommendations

To enhance the overall security posture, it is recommended to implement a comprehensive security strategy that includes regular vulnerability assessments, timely patch management, and continuous monitoring of network traffic. Additionally, adopting advanced encryption protocols and securing all endpoints will further protect against potential threats.