1 Executive Security Assessment Report

1.1 Introduction

The security assessment was conducted on the domain **precision.apps-qa.ilendx.tech**. The analysis was initiated on **May 30th at 14:00** and concluded in **00h:10m:10s**. The assessment was identified with the tracking ID **0c45107e9eb4** and executed using a Basic scan type. The evaluation focused on identifying High and Medium-risk vulnerabilities within the web application and its infrastructure, following OWASP and OSCP methodologies.

1.2 Summary of Key Issues

The security assessment identified **1** High-risk, **2** Medium-risk, **1** Low-risk, and **14** informational issues. The most critical finding is a Denial of Service (DoS) vulnerability on port **443**, with a **4.69%** timeout rate, posing a High risk of service disruption. Medium-risk issues include insecure HTTP port **80**, lacking encryption, and a sensitive subdomain indicating potential exposure of development environments. The SSL/TLS assessment revealed no support for TLS **1.3**, suggesting an opportunity to enhance encryption standards. Immediate actions include addressing the DoS vulnerability, securing HTTP communications, and reviewing subdomain security to mitigate potential threats.

1.3 Issues Table

Title	Risk
Denial of Service (DoS) Vulnerability	High
Nmap Port Scan Results Analysis	Medium
Subdomain Naming Security Assessment	Medium
SSL/TLS Protocols Security Assessment	Low

1.4 Detailed Findings

1.4.1 Denial of Service (DoS) Vulnerability

Description:

A Denial of Service vulnerability was detected on port **443**, with a **4.69%** timeout rate among **341** responses, indicating a High risk of service disruption. This vulnerability could be exploited to render the service unavailable to legitimate users.

Affected Assets:

- Ports Analyzed: **80** (HTTP), **443** (HTTPS)

Recommendations:

- Implement rate limiting and traffic filtering to mitigate potential DoS attacks. - Optimize server performance and monitor for unusual traffic patterns. - Consider deploying Web Application Firewalls (WAF) to protect against such attacks.

1.4.2 Nmap Port Scan Results Analysis

Description:

Port **80** is running HTTP without encryption, which poses a risk unless redirected to HTTPS or secured with HSTS. This lack of encryption can lead to data interception and unauthorized access.

Affected Assets:

- IP: **66.22.56.179** - Ports: **80/tcp** (http), **443/tcp** (ssl/https)

Recommendations:
- Redirect all HTTP traffic to HTTPS. - Implement HSTS to enforce secure connections. - Regularly update and patch web server software to mitigate vulnerabilities.

1.4.3 Subdomain Naming Security Assessment

Description:
The subdomain **precision.apps-qa.ilendx.tech** is associated with development/staging environments, which may contain unpatched vulnerabilities or debug information. These endpoints could provide access to critical systems and sensitive data.

Affected Assets:
- Subdomain: **precision.apps-qa.ilendx.tech**

Recommendations:
- Restrict access to development/staging environments using IP whitelisting or VPN. - Regularly audit and sanitize development environments to remove sensitive data. - Implement strong authentication mechanisms for accessing these environments.

1.5 General Recommendations

To enhance the overall security posture, it is recommended to address the identified vulnerabilities promptly. Prioritize the remediation of High-risk issues such as the DoS vulnerability on port **443**. Additionally, improve encryption standards by supporting TLS **1.3** and secure all communications by enforcing HTTPS with HSTS. Regular security audits and monitoring should be conducted to ensure ongoing protection against emerging threats.