1 Executive Security Assessment Report

1.1 Introduction

The security assessment was conducted on the domain `pathward.apps-uat.ilendx.tech` using a Basic scan methodology. The analysis was initiated on May 14th at 13:45 and completed in **00h:09m:03s**. The tracking ID for this assessment is `0daedbe0490b`. The scope of the work included a comprehensive evaluation of the domain's web application and infrastructure, focusing on identifying High and Medium-risk vulnerabilities. The assessment adhered to OWASP and OSCP methodologies to ensure thoroughness and accuracy.

1.2 Summary of Findings

The security assessment identified **0** High-risk, **2** Medium-risk, **1** Low-risk, and **15** informational issues. Notably, Medium-risk vulnerabilities include open HTTP port **80**, which lacks encryption and could expose sensitive data, and a potentially sensitive subdomain indicating a development environment that may harbor unpatched vulnerabilities. The SSL/TLS assessment showed no support for the latest TLS **1.3**, with only TLS **1.2** being used, which is currently acceptable but not optimal. All analyzed hosts are on dedicated infrastructure, with no shared hosting risks detected. Immediate attention is recommended for securing HTTP services and reviewing the security of development environments to mitigate potential exposure.

1.3 Issues Table

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

1.4 Detailed Findings

1.4.1 Nmap Port Scan Results Analysis

Description:
The analysis identified **2** open ports on the IP address **66.6.26.169**. Port **80/tcp** is running HTTP without encryption, which poses a risk if not redirected to HTTPS or if HSTS is not enabled. This lack of encryption can lead to exposure of sensitive data during transmission.

Affected Assets:
- IP: **66.6.26.169** with open ports **80/tcp** and **443/tcp**.

Recommendations:
- Implement HTTPS with a valid SSL/TLS certificate for all HTTP services. - Ensure HTTP Strict Transport Security (HSTS) is enabled to enforce secure connections. - Regularly review and update SSL/TLS configurations to support the latest protocols.

1.4.2 Subdomain Naming Security Assessment

Description:
A potentially sensitive subdomain, `pathward.apps-uat.ilendx.tech`, was identified as part of a development or staging environment. Such environments may contain unpatched vulnerabilities or debug information, increasing the risk of unauthorized access or data leakage.

Affected Assets:
- Subdomain: `pathward.apps-uat.ilendx.tech`

Recommendations:
- Restrict access to development and staging environments using IP whitelisting or VPNs. - Regularly audit these environments for outdated software and apply necessary patches. - Avoid using descriptive subdomain names that reveal the environment's purpose.

1.5 General Recommendation

To enhance the overall security posture, it is recommended to prioritize the implementation of encryption across all services, particularly those exposed to the internet. Regular security audits should be conducted to identify and mitigate emerging threats promptly. Additionally, consider adopting a robust patch management strategy to ensure all systems remain up-to-date with the latest security fixes.