1 Executive Security Assessment Report

1.1 Introduction

This report presents the findings from a security assessment conducted on the domain **lululemon.co.jp**. The assessment was initiated on **September 21st** at **05:00** and completed in **26 minutes and 39 seconds**. The analysis was performed using a **Basic** scan type. The primary objective was to identify potential vulnerabilities within the web application and infrastructure, focusing on High and Medium-risk issues.

1.2 Summary of Findings

The security assessment identified a total of **18 issues**, categorized as **0 High-risk**, **3 Medium-risk**, **1 Low-risk**, and **14 informational**. Key Medium-risk findings include the detection of potentially insecure open ports (e.g., HTTP on port **80** and **8080**) and high service density on a single host, which increases the attack surface and potential for exploitation. The shared hosting environment analysis revealed one host with Medium interest due to shared domains, necessitating further scrutiny. Despite these concerns, the SSL/TLS protocols are robust, with **12 endpoints** supporting TLS 1.3, and no deprecated protocols detected. Immediate actions should focus on securing open ports and evaluating shared hosting configurations to mitigate potential vulnerabilities.

1.3 Issues Table

Title	Risk
Shared Hosting Environment Analysis	Medium
Nmap Port Scan Results Analysis	Medium
Service Density Analysis	Medium
SSL/TLS Protocols Security Assessment	Low

1.3.1 Shared Hosting Environment Analysis

Description:

The analysis identified that the domain **lululemon.co.jp** is hosted in a shared environment with **18 shared domains**, categorizing it under Medium Interest. Shared hosting can pose risks due to potential vulnerabilities in other hosted domains affecting the security posture of the primary domain.

Affected Assets:

- Hostname: **lululemon.co.jp**

Recommendations:

- Evaluate the necessity of shared hosting for critical applications. - Consider migrating to a dedicated hosting environment to reduce potential risks. - Implement strict access controls and monitoring to detect any unauthorized activities.

1.3.2 Nmap Port Scan Results Analysis

Description:

The scan detected **13 open ports** on IP address **104.18.9.22**, with ports **80** and **8080** highlighted as potentially insecure due to lack of encryption. These ports could be susceptible to data interception if not properly secured.

Affected Assets:

- IP Address: **104.18.9.22**

PUBLIC REPORT - DEMO SCAN - NO INTRUSIVE TESTING

Recommendations:
- Ensure HTTP traffic is redirected to HTTPS using secure protocols. - Implement HSTS (HTTP Strict Transport Security) to enforce secure connections. - Regularly review and close unnecessary open ports to minimize exposure.

1.3.3 Service Density Analysis

Description:
The host **104.18.9.22** was found to have a high service density with **13 services** running, increasing the attack surface. High service density can lead to increased risk of exploitation if any service is vulnerable.

Affected Assets:
- Host IP: **104.18.9.22**

Recommendations:
- Conduct regular vulnerability assessments on all running services. - Reduce service density by consolidating services where possible. - Implement network segmentation to isolate critical services from less secure areas.

1.3.4 SSL/TLS Protocols Security Assessment

Description:
The assessment confirmed that all endpoints support modern TLS protocols, with **12 endpoints** using TLS 1.3 and TLS 1.2, ensuring robust encryption standards are maintained.

Affected Assets:
- No vulnerable hosts detected.

Recommendations:
- Continue monitoring for updates in cryptographic standards and implement them as necessary. - Ensure all endpoints maintain support for TLS 1.3 to leverage improved security features.

1.4 General Recommendations

To enhance the overall security posture, it is recommended to prioritize securing open ports and evaluating shared hosting configurations. Regular security audits should be conducted to identify and mitigate emerging threats promptly. Additionally, maintaining up-to-date encryption standards will ensure data integrity and confidentiality across all communication channels.

PUBLIC REPORT - DEMO SCAN - NO INTRUSIVE TESTING