1 Executive Security Assessment Report

1.1 Introduction

This report presents the findings from a security assessment conducted on the domain `pos-api-integration-` The assessment was initiated on May 19th at 21:45 and completed in a duration of **00h:10m:49s**. The analysis was performed using a Basic scan type, with the tracking ID `0d39ccdcd5e5`. The scope of the work included evaluating web application and infrastructure security using OWASP and OSCP methodologies.

1.2 Short Summary of Main Issues

The security assessment identified a total of **18 issues**, categorized as **0 High-risk**, **2 Medium-risk**, **2 Low-risk**, and **14 informational**. The most significant findings include Medium-risk vulnerabilities related to open HTTP ports (port **80**) that lack encryption, potentially exposing sensitive data, and sensitive subdomain names that could lead to unauthorized access to critical systems. The SSL/TLS protocols are generally secure, with **1 endpoint** supporting TLS 1.3 and **2 using TLS 1.2**, ensuring strong encryption standards. No shared hosting environments or brute-force susceptible services were detected, indicating a robust infrastructure. Immediate attention is recommended for the Medium-risk issues to mitigate potential security breaches.

1.3 Key Security Issues

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

1.3.1 Nmap Port Scan Results Analysis

Description:
The scan identified **4 open ports**, with port **80** (HTTP) being potentially insecure due to the lack of encryption. This could expose sensitive data if not redirected to HTTPS or if HSTS is not enabled.

Affected Assets:
- IPs: `176.100.165.240` and `146.75.105.91` - Services: HTTP and SSL/HTTPS

Recommendations:
- Implement HTTPS redirection for all HTTP traffic. - Enable HTTP Strict Transport Security (HSTS) to enforce secure connections. - Regularly monitor and update server configurations to adhere to best security practices.

1.3.2 Subdomain Naming Security Assessment

Description:
Two sensitive subdomains were detected, indicating potentially exposed API endpoints that could lead to unauthorized access to critical systems or data.

Affected Assets:
- Subdomains: -`pos-api-integration-radware.bentosandbox.com`-`www.pos-api-integration-radware.b`

Recommendations:
- Review and restrict access to sensitive subdomains. - Implement proper authentication and authorization mechanisms. - Regularly audit subdomain configurations for exposure risks.

1.3.3 SSL/TLS Protocols Security Assessment

Description:
The assessment confirmed that TLS 1.3 is supported by **1 endpoint**, while TLS 1.2 is used by **2 endpoints**. Deprecated protocols such as SSLv3, TLS 1.0, and TLS 1.1 were not found, indicating no current risk from these outdated protocols.

Affected Assets:

- Endpoints supporting TLS 1.3: **1** - Endpoints using TLS 1.2: **2**

Recommendations:

- Continue using TLS 1.3 where possible for enhanced security. - Ensure all endpoints are configured to disable deprecated protocols. - Regularly update cryptographic libraries and configurations.

1.3.4 API Surface Analysis

Description:
Potential API endpoints were identified with a high likelihood of being non-production environments, which may still pose security risks if not properly managed.

Affected Assets:

- Endpoints: -`pos-api-integration-radware.bentosandbox.com`-`www.pos-api-integration-radware.ben`

Recommendations:

- Secure non-production environments with appropriate access controls. - Regularly review API endpoints for exposure and vulnerabilities. - Implement logging and monitoring to detect unauthorized access attempts.

1.4 General Recommendation

It is recommended that the organization prioritize addressing the Medium-risk issues identified in this report to mitigate potential security breaches. Regular security assessments should be conducted to ensure ongoing protection against emerging threats. Additionally, implementing a comprehensive security policy that includes encryption, access control, and regular audits will enhance the overall security posture of the organization.