1 Executive Security Assessment Report

1.1 Introduction

The security assessment was conducted on the domain **ramu27.omnipaytest.com**. The analysis commenced on **March 17th** at **19:45** and concluded in **00h:11m:33s**. The assessment was categorized as a “Basic” type scan. The evaluation focused on identifying potential vulnerabilities within the web application and its infrastructure, adhering to OWASP and OSCP methodologies.

1.2 Summary of Findings

The security assessment identified a total of **18** issues, categorized as **0** High, **2** Medium, **2** Low, and **14** informational. The most significant findings include the presence of a shared hosting environment and sensitive subdomain naming, both rated as Medium. These issues could expose the organization to potential security breaches if not addressed, as shared hosting can lead to resource contention and sensitive subdomains may reveal critical system interfaces. Additionally, the SSL/TLS protocol analysis showed reliance on TLS 1.2 without TLS 1.3, indicating room for improvement in encryption standards. While no High-risk vulnerabilities were found, it is crucial to address the Medium-risk issues to mitigate potential threats. The assessment also confirmed that all services are running on standard ports, and no brute-force susceptible services were detected, reflecting a generally secure configuration.

1.3 Key Security Issues

Title	Risk
Shared Hosting Environment Analysis	Medium
Subdomain Naming Security Assessment	Medium
SSL/TLS Protocols Security Assessment	Low
Login Form Detection Analysis	Low

1.3.1 Shared Hosting Environment Analysis

Description:
The analysis identified that the domain **ramu27.omnipaytest.com** is hosted in a shared environment with **35** shared domains, categorized as medium interest. Shared hosting environments can lead to resource contention and potential security risks if one of the shared domains is compromised.

Affected Assets:
- Hostname: **ramu27.omnipaytest.com**

Recommendations:
Consider migrating to a dedicated hosting environment to minimize security risks associated with shared hosting. - Implement strict access controls and monitoring to detect any unauthorized activities promptly.

1.3.2 Subdomain Naming Security Assessment

Description:
A sensitive subdomain, **ramu27.omnipaytest.com**, associated with development/staging environments was detected. Such environments may contain unpatched vulnerabilities or debug information, potentially exposing administrative and monitoring interfaces.

PUBLIC REPORT - DEMO SCAN - NO INTRUSIVE TESTING

Affected Assets:
- Subdomain: **ramu27.omnipaytest.com**

Recommendations:
- Restrict access to development and staging environments using VPNs or IP whitelisting. - Regularly audit and sanitize subdomains to ensure no sensitive information is exposed.

1.3.3 SSL/TLS Protocols Security Assessment

Description:
The SSL/TLS protocol analysis revealed that the domain is using TLS 1.2, which is currently acceptable but lacks support for TLS 1.3, the current best practice for enhanced security and performance.

Affected Assets:
- **1** endpoint using TLS 1.2.

Recommendations:
- Upgrade to TLS 1.3 to benefit from improved security features and performance enhancements. - Regularly review and update cryptographic protocols to align with industry standards.

1.3.4 Login Form Detection Analysis

Description:
A login form was detected on the domain, which requires security validation to ensure it is not susceptible to common web application attacks such as SQL injection or cross-site scripting.

Affected Assets:
- URL: `https://ramu27.omnipaytest.com:443`

Recommendations:
- Implement input validation and sanitization to prevent injection attacks. - Use HTTPS to encrypt data in transit and protect user credentials.

1.4 General Recommendations

To enhance the overall security posture, it is recommended to address all Medium-risk issues promptly and consider implementing a continuous monitoring strategy. Regular security assessments should be conducted to identify and mitigate emerging threats, ensuring compliance with best practices and industry standards.

PUBLIC REPORT - DEMO SCAN - NO INTRUSIVE TESTING