1 Executive Security Assessment Report

1.1 Introduction

This security assessment was conducted on the domain **prd-ring-web-us.prd.rings.solutions**. The analysis commenced on **June 2nd** at **19:00** and concluded in **00h:09m:31s**. The assessment was identified with tracking ID **0617cad3b028** and was classified as a **Basic** type scan. The evaluation focused on identifying vulnerabilities within the web application and infrastructure, adhering to OWASP and OSCP methodologies. The primary objective was to uncover High and Medium-risk issues that could potentially impact the security posture of the client's assets.

1.2 Summary of Findings

The security assessment identified a total of **18** issues, categorized as **0** High-risk, **1** Medium-risk, **1** Low-risk, and **16** informational. The most significant finding is a Medium-risk issue related to open HTTP port **80**, which lacks encryption and poses potential security risks if not redirected to HTTPS or if HSTS is not enabled. This could expose sensitive data to interception, impacting data confidentiality. Additionally, the SSL/TLS assessment revealed that all endpoints use TLS **1.2**, with no support for the more secure TLS **1.3**, indicating a need for protocol upgrades. The analysis also confirmed no shared hosting environments, no High-risk geographic server locations, and no unusual port assignments, suggesting a generally secure infrastructure. Immediate actions should focus on securing the HTTP service and planning for TLS protocol enhancements to mitigate potential vulnerabilities.

1.3 Key Security Issues

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

1.3.1 Nmap Port Scan Results Analysis

Description

The assessment identified an open HTTP port (**80**) on IP address **18.205.127.192**. This port is associated with the HTTP service running on awselb/2.0, which lacks encryption. The absence of HTTPS redirection or HSTS configuration on this port poses a Medium risk as it could lead to potential data interception and compromise of data confidentiality.

Affected Assets

- IP Address: **18.205.127.192**
- Open Ports: **80/tcp** (http), **443/tcp** (ssl/https)

Recommendations

It is recommended to implement HTTPS redirection for all HTTP traffic to ensure data encryption in transit. Additionally, enabling HTTP Strict Transport Security (HSTS) will enforce secure connections and prevent downgrade attacks. Regularly review and update security configurations to align with best practices.

1.3.2 SSL/TLS Protocols Security Assessment

Description

The SSL/TLS assessment revealed that all endpoints are using TLS **1.2**, with no support for TLS **1.3**, which is considered the current best practice for enhanced security and performance.

While TLS **1.2** is acceptable, upgrading to TLS **1.3** would provide improved cryptographic algorithms and better protection against potential vulnerabilities.

Affected Assets

- **6** endpoints using TLS **1.2**
- No endpoints using TLS **1.3**, TLS **1.1**, TLS **1.0**, or SSLv3

Recommendations

It is advisable to plan for an upgrade to TLS **1.3** across all applicable endpoints to enhance security measures and future-proof the infrastructure against emerging threats. Ensure that deprecated protocols such as SSLv3, TLS **1.0**, and TLS **1.1** remain disabled to prevent exploitation of known vulnerabilities.

1.4 General Recommendations

To strengthen the overall security posture, it is crucial to prioritize the implementation of HTTPS with HSTS for all web services and transition to TLS **1.3** where feasible. Regular security audits and updates should be conducted to maintain compliance with industry standards and best practices. Continuous monitoring and incident response planning will further safeguard against potential threats and vulnerabilities.