1 Executive Security Assessment Report

1.1 Introduction

This report presents the findings from a comprehensive security assessment conducted on the domain **net.s2stagehance.com**. The analysis was performed using OWASP and OSCP methodologies, focusing on web application and infrastructure security. The assessment was initiated on **March 19th** at **12:00** and concluded in **00h:11m:00s**. The tracking ID for this assessment is **130781c15164**, and it was categorized as a "Basic" type analysis. This report highlights the High and Medium-risk issues identified during the assessment, providing actionable recommendations to enhance security posture.

1.2 Summary of Key Issues

The security assessment identified a total of **19 issues**, categorized as **0 High-risk**, **4 Medium-risk**, **1 Low-risk**, and **14 informational**. Key Medium-risk findings include the absence of a Web Application Firewall (WAF) on **50%** of analyzed hosts, increasing vulnerability to cyber-attacks, and the presence of potentially insecure open ports, such as HTTP on port **80**, which lacks encryption. Additionally, SSL certificate expiration is approaching for two domains, with **63 days** remaining, necessitating timely renewal to avoid service disruptions. The analysis also highlighted sensitive subdomains that could expose critical systems. Immediate actions should focus on implementing WAF protection, securing open ports, and planning SSL certificate renewals to mitigate these risks effectively.

1.3 Issues Table

Title	Risk
Absence of WAF	Medium
Nmap Port Scan Results Analysis	Medium
Subdomain Naming Security Assessment	Medium
SSL Certificate Expiration Analysis	Medium

1.4 Detailed Findings

1.4.1 Absence of WAF

Description:
The analysis revealed that **1 out of 2 hosts** lacks a Web Application Firewall (WAF), resulting in a vulnerability rate of **50%**. This absence significantly increases the risk of successful cyber-attacks, particularly injection-based attacks, due to the lack of protective filtering mechanisms.

Affected Assets:
- Host: **www.net.s2stagehance.com**

Recommendations:
Implement a robust WAF solution to provide an additional layer of security by filtering and monitoring HTTP traffic between the web application and the Internet. This will help prevent common web exploits that can compromise application security.

1.4.2 Nmap Port Scan Results Analysis

Description:
The scan identified **4 open ports**, with port **80/tcp** running an HTTP service without encryption.

This lack of encryption poses a security risk as data transmitted over HTTP can be intercepted by attackers.

Affected Assets:

- IP: **151.101.66.52** with services running on ports **80/tcp** and **443/tcp**.

Recommendations:

Ensure that all HTTP traffic is redirected to HTTPS to secure data transmission. Implement HTTP Strict Transport Security (HSTS) to enforce secure connections.

1.4.3 Subdomain Naming Security Assessment

Description:

The assessment detected **2 sensitive subdomains**, indicating potential access to administrative interfaces or development environments. These subdomains may expose critical systems or sensitive data if not properly secured.

Affected Assets:

- Subdomains: **net.s2stagehance.com**, **www.net.s2stagehance.com**

Recommendations:

Restrict access to sensitive subdomains through IP whitelisting or VPN access. Regularly review and sanitize subdomain names to avoid exposing internal systems or development environments.

1.4.4 SSL Certificate Expiration Analysis

Description:

SSL certificates for two domains are set to expire in **63 days**, categorized under “Warning” status. Failure to renew these certificates in time could lead to service disruptions and loss of trust from users.

Affected Assets:

- Domains: **net.s2stagehance.com**, **www.net.s2stagehance.com**

Recommendations:

Plan for the timely renewal of SSL certificates to maintain secure communications and avoid service interruptions. Implement automated reminders for certificate renewals to ensure continuous compliance with security standards.

1.5 General Recommendations

To enhance the overall security posture, it is recommended to implement a comprehensive security strategy that includes regular vulnerability assessments, timely patch management, and continuous monitoring of network traffic. Additionally, employee training on cybersecurity best practices should be conducted to mitigate risks associated with human error.