1 Executive Security Assessment Report

1.1 Introduction

The security assessment was conducted on the domain **api.pagerduty.com**. The analysis commenced on **07-12** at **10:00** and concluded after **00h:11m:38s**. The assessment utilized a basic scan type, focusing on identifying potential vulnerabilities within the web application and infrastructure. The evaluation adhered to OWASP and OSCP methodologies to ensure comprehensive coverage of security risks.

1.2 Summary of Findings

The security assessment identified a total of **19** issues, categorized as **0** high-risk, **4** medium-risk, **2** low-risk, and **13** informational. Key medium-risk findings include the absence of Web Application Firewall (WAF) protection on **50%** of analyzed hosts, increasing vulnerability to cyber-attacks, and the detection of insecure HTTP ports that lack encryption, potentially exposing sensitive data. Additionally, shared hosting environments were identified, with two hosts categorized as medium interest due to shared domains, which could lead to resource contention and security risks. The subdomain naming assessment revealed potentially sensitive endpoints that could be exploited if not properly secured. Immediate actions should focus on implementing WAF protection, securing HTTP ports, and reviewing shared hosting configurations to mitigate these vulnerabilities.

1.3 Issues Table

Title	Risk
Absence of WAF	Medium
Nmap Port Scan Results Analysis	Medium
Shared Hosting Environment Analysis	Medium
Subdomain Naming Security Assessment	Medium

1.4 Detailed Findings

1.4.1 Absence of WAF

Description:
The analysis revealed that **1** out of **2** hosts lacked Web Application Firewall (WAF) protection, resulting in a **50.00%** vulnerability rate. This absence significantly increases the risk of successful cyber-attacks, particularly injection-based attacks, which could lead to unauthorized data access, data breaches, and potential system compromise.

Affected Assets:
- Host: `www.api.pagerduty.com`

Recommendations:
Implement a robust Web Application Firewall (WAF) to provide an additional layer of security against common web-based attacks. Regularly update and configure the WAF rules to adapt to emerging threats.

1.4.2 Nmap Port Scan Results Analysis

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

poses a risk as data transmitted over HTTP can be intercepted by attackers unless there is a redirection to HTTPS or HSTS is enabled.

Affected Assets:

- IP Address: `44.237.102.140` - Ports: `80/tcp`, `443/tcp`

Recommendations:

Ensure all HTTP traffic is redirected to HTTPS and consider enabling HTTP Strict Transport Security (HSTS) to enforce secure connections. Regularly review and close unnecessary open ports to minimize exposure.

1.4.3 Shared Hosting Environment Analysis

Description:

The analysis identified that both `api.pagerduty.com` and `www.api.pagerduty.com` are hosted in shared environments with a medium interest level due to the number of shared domains (**55** and **49** respectively). Shared hosting can lead to resource contention and increased security risks if one of the co-hosted domains is compromised.

Affected Assets:

- Hostnames: `api.pagerduty.com`, `www.api.pagerduty.com`

Recommendations:

Consider migrating critical services to dedicated hosting environments to reduce the risk associated with shared resources. Implement strict access controls and monitoring to detect any unauthorized activities.

1.4.4 Subdomain Naming Security Assessment

Description:

The subdomain assessment detected **2** sensitive subdomains, `api.pagerduty.com` and `www.api.pagerduty.c` which could indicate potential access points to critical systems and sensitive data. These endpoints may expose development or staging environments with unpatched vulnerabilities or debug information.

Affected Assets:

- Subdomains: `api.pagerduty.com`, `www.api.pagerduty.com`

Recommendations:

Conduct a thorough review of subdomain configurations and ensure that sensitive endpoints are adequately secured. Implement access controls and monitor for unauthorized access attempts.

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 can help mitigate human-related risks.