1 Executive Security Assessment Report

1.1 Introduction

This report presents the findings from a comprehensive security assessment conducted on the domain **shopify.plus**. The assessment was initiated on **April 17th at 22:45** and completed in **00h:10m:31s**. The analysis was performed using a basic scan type. The scope of the work included evaluating the web application and infrastructure security, focusing on identifying High and Medium-risk vulnerabilities.

1.2 Summary of Key Issues

The security assessment identified a total of **18** issues, categorized as **1** High-risk, **2** Medium-risk, **2** Low-risk, and **13** informational. The most critical finding is the High-risk shared hosting environment with over **1000** domains on a single IP, posing significant exposure to potential attacks. Medium-risk issues include insecure open ports (HTTP on port **80** and **8080**) and an SSL certificate nearing expiration in **44** days, necessitating prompt renewal to avoid service disruptions. While the SSL/TLS protocols are generally secure, with TLS 1.**3** supported, the presence of login forms and open ports requires ongoing monitoring to mitigate brute force and other attacks. Immediate actions should focus on addressing the High-risk shared hosting and ensuring SSL certificate renewal to maintain operational security.

1.3 Key Security Issues

Title	Risk
Shared Hosting Environment Analysis	High
Nmap Port Scan Results Analysis	Medium
SSL Certificate Expiration Analysis	Medium
SSL/TLS Protocols Security Assess.	Low
Login Form Detection Analysis	Low

1.3.1 Shared Hosting Environment Analysis

Description:

The assessment revealed that the domain **shopify.plus** is hosted in a shared environment with over **1046** domains on a single IP. This configuration significantly increases the risk of cross-contamination attacks, where vulnerabilities in one domain could potentially affect others.

Affected Assets:

- Hostname: **shopify.plus**

Recommendations:

- Consider migrating to a dedicated hosting environment to reduce exposure to shared infrastructure risks. - Implement strict access controls and continuous monitoring to detect and respond to any unauthorized activities promptly.

1.3.2 Nmap Port Scan Results Analysis

Description:

The scan identified **4** open ports, with ports **80** and **8080** flagged as potentially insecure due to lack of encryption. These ports are commonly associated with web service vulnerabilities and proxy services.

Affected Assets:
- IP Address: **185.146.173.20** - Ports: **80/tcp, 443/tcp, 8080/tcp, 8443/tcp**

Recommendations:
- Ensure that HTTP traffic is redirected to HTTPS to enforce encryption. - Regularly update and patch web services to mitigate known vulnerabilities. - Consider disabling unnecessary open ports or implementing firewall rules to restrict access.

1.3.3 SSL Certificate Expiration Analysis

Description:
The SSL certificate for **shopify.plus** is set to expire in **44** days, which could lead to service disruptions if not renewed promptly.

Affected Assets:
- Domain: **shopify.plus**

Recommendations:
- Initiate the renewal process for the SSL certificate immediately to avoid any service interruptions. - Implement automated alerts for certificate expiration to ensure timely renewals in the future.

1.4 General Recommendations

To enhance the overall security posture, it is recommended to prioritize addressing High-risk issues such as shared hosting vulnerabilities and SSL certificate management. Additionally, regular security assessments should be conducted to identify and mitigate emerging threats promptly. Implementing a robust incident response plan and continuous monitoring will further strengthen defenses against potential attacks.