1 Executive Security Assessment Report

1.1 Analysis Overview

The security assessment was conducted on the domain **derwent.in**. The analysis commenced on **September 5th** at **08:45** and concluded in **00h:09m:25s**. The assessment was categorized as a “Basic” type. The scope included evaluating the domain for potential vulnerabilities using OWASP and OSCP methodologies, focusing on High and Medium-risk issues.

1.2 Short Summary of Main Issues

The security assessment identified a total of **18** issues, categorized as **1** High-risk, **1** Medium-risk, and **16** informational. The most critical finding is the High-risk shared hosting environment, with one host (**derwent.in**) sharing its IP with over **262,000** domains, posing significant security risks due to potential cross-domain vulnerabilities. Additionally, a Medium-risk issue was detected with an open HTTP port (**80**) lacking encryption, which could expose sensitive data if not redirected to HTTPS. While no unusual port assignments or brute-force vulnerabilities were found, the focus should be on mitigating the High-risk shared hosting and ensuring secure configurations for exposed services. Immediate actions include reviewing shared hosting arrangements and enforcing HTTPS to protect data integrity and confidentiality.

1.3 Key Security Issues

Title	Risk
Shared Hosting Environment	High
Nmap Port Scan Results	Medium

1.3.1 Shared Hosting Environment Analysis

Description:
The assessment revealed that the domain **derwent.in** is part of a High-risk shared hosting environment. This host shares its IP address with over **262,000** other domains, significantly increasing the risk of cross-domain vulnerabilities. Such environments can lead to potential exposure of sensitive data and security breaches due to shared resources.

Affected Assets:
- Hostname: **derwent.in**

Recommendations:
- Evaluate the current hosting arrangement and consider migrating to a dedicated hosting environment to minimize exposure. - Implement strict access controls and monitoring to detect any unauthorized access or anomalies. - Regularly audit the hosting environment for any changes or new vulnerabilities.

1.3.2 Nmap Port Scan Results Analysis

Description:
The scan identified an open HTTP port (**80**) on IP address **3.33.139.32** running the service **awselb/2.0**. This port lacks encryption, posing a risk of data interception and exposure if not properly secured with HTTPS or HSTS.

Affected Assets:
- IP Address: **3.33.139.32** - Port: **80/tcp** - Service: **http** - Version: **awselb/2.0**

Recommendations:
- Implement HTTPS for all web traffic to ensure data is encrypted during transmission. - Enable

HTTP Strict Transport Security (HSTS) to enforce secure connections. - Regularly review and update SSL/TLS configurations to adhere to best practices.

1.4 General Recommendations

To enhance the overall security posture, it is recommended to prioritize addressing High and Medium-risk issues identified in this assessment. Transitioning to a more secure hosting environment and enforcing HTTPS will significantly reduce potential vulnerabilities. Continuous monitoring and regular security audits should be conducted to maintain robust security defenses against emerging threats.