1 Executive Security Assessment Report

1.1 Introduction

The security assessment was conducted on the domain **healthleaders.com**. The analysis was initiated on **April 13th** at **21:00** and concluded in **00h:05m:21s**. The assessment type was classified as **Basic**. The scope of the work involved evaluating the web application and infrastructure security posture using OWASP and OSCP methodologies.

1.2 Summary of Findings

The recent security assessment reveals a low-risk profile with no high or medium-risk issues identified. The assessment found one low-risk issue related to shared hosting, with a single host categorized as low interest due to sharing its IP with **6** other domains. These findings suggest strong existing security measures, but further manual verification is recommended to ensure comprehensive coverage, especially given the potential for automated assessments to be blocked. Continued monitoring and analysis of shared hosting environments are advised to maintain security posture.

1.3 Key Security Issues

Title	Risk
Shared Hosting Environment	Low

1.3.1 Shared Hosting Environment Analysis

Description

The analysis focused on identifying shared hosting environments by evaluating the number of domains sharing the same IP address. The domain **healthleaders.com** was found to share its IP with **6** other domains, categorizing it as a low-interest host. This indicates a limited shared hosting environment, which generally poses minimal risk but should be monitored to prevent potential security implications from neighboring domains.

Affected Assets

- **Hostname:** healthleaders.com

Recommendations

- Regularly monitor the shared hosting environment to detect any changes in the number of shared domains.
- Implement network segmentation and isolation techniques to minimize potential risks from other domains sharing the same IP.
- Consider transitioning to a dedicated hosting environment if the number of shared domains increases significantly, which could elevate the risk profile.

1.4 General Recommendation

To maintain a robust security posture, it is recommended that continuous monitoring and periodic manual verification of security controls be performed. This ensures that any potential vulnerabilities are promptly identified and mitigated. Additionally, staying informed about the latest security threats and trends will aid in proactively defending against emerging risks.