**Report Format**

**Senselearner**

**Title**: Information Gathering Report for senselearner.com

**Date**: September 20, 2023

**Prepared by**: Jeff Tsui

**Position**: Cybersecurity Intern

**Objective**:

The objective of this report is to present the findings of the information gathering and reconnaissance activities conducted on senselearner.com in a legal and ethical manner. The information collected is intended for security assessment and risk analysis.

**Executive Summary:**

The comprehensive assessment of senselearner.com has furnished crucial insights into its digital footprint and associated security considerations. In our analysis of domain information, we unveiled essential details, including the domain's creation date, registrar (Godaddy), and active status, forming the bedrock of our understanding of its online presence. Notably, DNS Footprinting did not yield specific findings within the provided information.

Within the domain of web footprinting, we identified that the web server operates on LiteSpeed software and employs PHP/7.4.33. This discovery raises security concerns due to the end-of-life status of PHP 7.4, effective as of November 2022. However, despite this finding, no directory, file structure, or additional technologies in use were disclosed.

Network and WHOIS enumeration did not provide specific details pertaining to network range or IP addresses. In contrast, our open-source intelligence (OSINT) endeavors proved fruitful, enabling us to extract valuable information, including the IP address, DNS records, registrar, and registrar status through Domain Dossier and Domaintools. Additionally, the use of Shodan unveiled a multitude of hostnames and domains previously concealed from Kali Linux tools.

Significantly, our primary security concern centers on the outdated PHP version, underscoring the imperative need for swift updates to mitigate potential vulnerabilities. In light of these findings, this assessment underscores the paramount importance of continuous monitoring and proactive security measures to uphold the integrity and resilience of digital assets in an ever-evolving cybersecurity landscape.

**Table of Contents**:

* Executive Summary
* Introduction
* Domain Information
* DNS Footprinting
* Web Footprinting
* Network and WHOIS Enumeration
* Open-Source Intelligence (OSINT)
* Vulnerabilities and Security Concerns
* Recommendations
* Conclusion

**Introduction**:

In today's digital-centric landscape, safeguarding sensitive data and securing online assets is of utmost importance. As technology evolves, so do the tactics employed by cyber adversaries aiming to exploit digital weaknesses. To counter these rising threats, businesses and organizations emphasize the essential role of conducting comprehensive Footprinting and Reconnaissance activities in their cybersecurity strategies. This report details the rigorous evaluation of senselearner.com, conducted in strict adherence to legal and ethical standards, with a primary focus on strengthening security and performing a thorough risk analysis.

**Domain Information**:

* **Domain Name**: senselearner.com
* **IP Address**: [162.250.126.19]
* **Registrar**: [Godaddy]
* **Registration Date**: [2021-07-02]
* **Expiry Date**: [2025-07-02]
* **Status**: [Active]

**DNS Footprinting**:

Summarize the findings from DNS Footprinting, including:

A computer screen shot of a computer

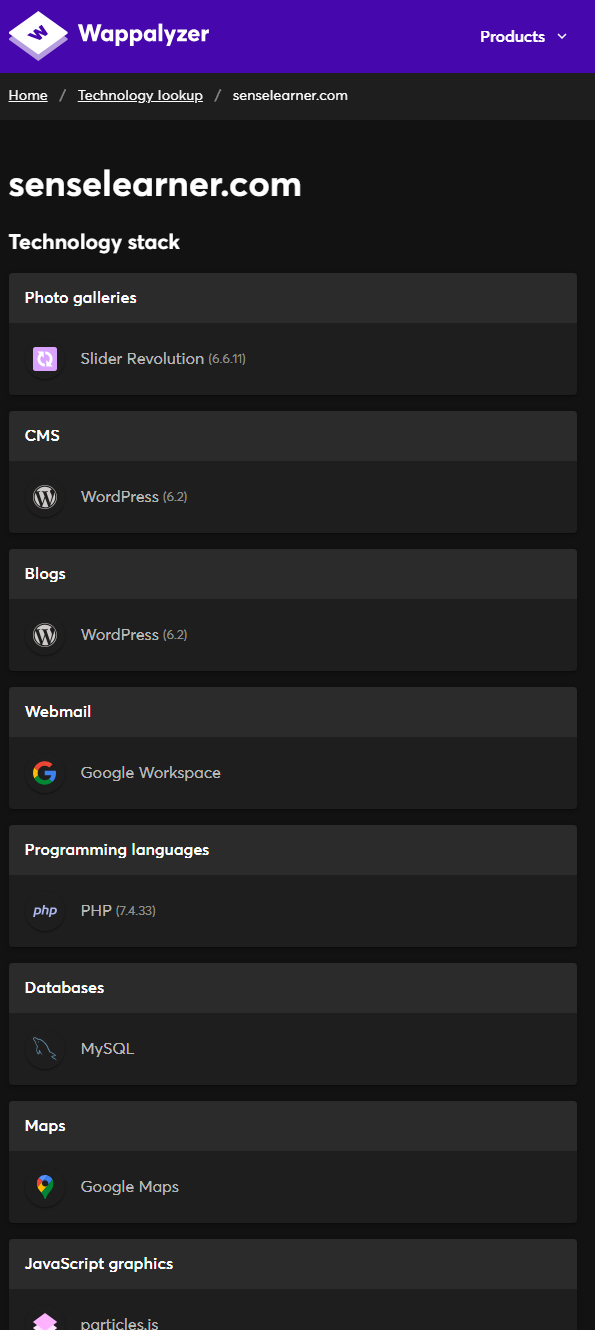
Description automatically generated

**Web Footprinting**:

Detail the results of web Footprinting, such as:

* Web Server Information: Identify the web server software and version.
  + Server: LiteSpeed
  + A screenshot of a computer

    Description automatically generatedX-Powered-By: PHP/7.4.33



* Directory and File Structure: Document any directories or files discovered.
  + No way to hack into any hidden directory or files.
* Technologies in Use: List content management systems (CMS), frameworks, or scripting languages used.
* Metadata: Include metadata from web pages, if available.

A screenshot of a computer program

Description automatically generated

**Network and WHOIS Enumeration**:

Discuss network and WHOIS enumeration results:

* A computer screen shot of a computer

  Description automatically generatedNetwork Range: Note the network range and IP addresses.
* WHOIS Records: Include details from WHOIS records, such as the registrant's contact information.

A screen shot of a computer

Description automatically generated

* ASN Information: If applicable, mention Autonomous System Number (ASN) data.

A screenshot of a computer

Description automatically generated

**Open-Source Intelligence (OSINT)**:

From using OSINT, I can find its IP address along with all DNS records by using the Domain Dossier. Can also use the Domaintools to find the registrar and registrar status. By using Shodan, I also found a lot of Hostnames and Domains that I couldn’t find using Kali Linux.

**Vulnerabilities and Security Concerns**:

The only vulnerability that I found is the X-Powered-by: PHP/7.4.33

* The end-of-life date for PHP 7.4 was November 28, 2022.

**Recommendations**:

Provide recommendations for addressing any identified vulnerabilities or concerns. These recommendations may include:

* Download a newer version of PHP

**Conclusion**:

In conclusion, the comprehensive assessment of senselearner.com has revealed valuable insights into its digital footprint. In the domain information analysis, we uncovered vital details such as the domain's creation date, its registrar (GoDaddy), and its active status, providing a foundational understanding of its online presence. DNS Footprinting did not yield any specific findings in the provided information. In the realm of web Footprinting, we identified that the web server employs LiteSpeed software and operates with PHP/7.4.33, potentially raising security concerns due to PHP 7.4 reaching its end-of-life in November 2022. Despite these observations, no directory, file structure, or additional technologies in use were disclosed. Network and WHOIS enumeration offered no specific details regarding network range or IP addresses. Our open-source intelligence (OSINT) efforts allowed us to uncover the IP address, DNS records, registrar, and registrar status through Domain Dossier and Domaintools. Additionally, Shodan revealed a host of hostnames and domains not initially accessible through Kali Linux tools. Notably, the primary security concern lies in the outdated PHP version, highlighting the need for prompt updates to mitigate potential vulnerabilities. This assessment underscores the importance of continuous monitoring and proactive security measures in maintaining the integrity and resilience of digital assets in an ever-evolving cybersecurity landscape.

**Appendices**:

Walkthrough can be found on: <https://github.com/jefftsui1/Cybersecurity-Home-Labs/blob/main/Senselearner-Internship/Week-2/Footprinting%20and%20Reconnaissance%20Report%20Walkthrough.md>

**References**:

* Hackertarget.com
* Kali Linux
  + Dig command, Whois command, ping command
* Osintframework.com
* Shodan.com
* Wappalyzer.com