Title: Information Gathering Report for senselearner.com

Date: 27/09/2023

Prepared by: Anu S M

Position: Cyber Security 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.

Table of Contents

Introduction

Domain Information

DNS Footprinting

Web Footprinting

Network and WHOIS Enumeration

Open-Source Intelligence (OSINT)

Vulnerabilities and Security Concerns

Recommendations

Introduction

The purpose of this report is to provide a comprehensive assessment of the online presence of senselearner.com. The information gathering and reconnaissance activities conducted for this report were carried out with the primary goal of evaluating the security posture and potential risks associated with the website.

The context for this information-gathering initiative stems from a growing concern for cybersecurity threats in the digital landscape. As the internet continues to play a central role in business operations, information dissemination, and communication, websites like senselearner.com are exposed to various vulnerabilities and risks. It has become essential to conduct regular assessments to ensure the safety and integrity of online platforms.

Domain Information

Domain Name: senselearner.com

IP Address: 162.250.126.19

Registry Domain ID: 2623764109_DOMAIN_COM-VRSN

Registrar WHOIS Server: whois.godaddy.com

Registrar URL: https://www.godaddy.com

Updated Date: 2023-06-15T00:16:45Z

Creation Date: 2021-07-01T23:19:50Z

Registrar Registration Expiration Date: 2025-07-01T23:19:50Z

Registrar: GoDaddy.com, LLC

Registrar IANA ID: 146

Registrar Abuse Contact Email: abuse@godaddy.com

Registrar Abuse Contact Phone: +1.4806242505

Domain Status: clientTransferProhibited
https://icann.org/epp#clientTransferProhibited

Domain Status: clientUpdateProhibited
https://icann.org/epp#clientUpdateProhibited

Domain Status: clientRenewProhibited
https://icann.org/epp#clientRenewProhibited

Domain Status: clientDeleteProhibited
https://icann.org/epp#clientDeleteProhibited

DNS Footprinting

```
Name                 Type   TTL    Section       NameExchange
----                ----  ---        -------          ----------
senselearner.com      MX  14400  Answer   ALT1.ASPMX.L.GOOGLE. com


senselearner.com      MX  14400  Answer   ALT4.ASPMX .LGOOGLE.com
senselearner.com      MX  14400  Answer   ASPMX.L.GOOGLE.com
senselearner.com      MX  14400  Answer   ALT3.ASPMX.L.GOOGLE. com
senselearner.com      MX  14400  Answer   ALT2.ASPMX.L.GOOGLE.com
```

DNS Enumeration

```
Server:  192.168.0.1
Address:  192.168.0.1
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** Request to 192.168.0.1 timed-out
```

```
Server:  192.168.0.1
Address:  192.168.0.1

Non-authoritative answer:
senselearner.com
        primary name server = dns2014a.trouble-free.net
        responsible mail addr = not-monitored-email.interserver.net
        serial  = 2023092403
        refresh = 3600 (1 hour)
        retry   = 1800 (30 mins)
        expire  = 1209600 (14 days)
        default TTL = 86400 (1 day)
```

```
C:\Users\anusm>ping -n 1 192.168.1.1   | find "Reply"
Reply from 192.168.1.1: bytes=32 time=5ms TTL=63

C:\Users\anusm>ping -n 1 192.168.1.2   | find "Reply"
Reply from 192.168.1.2: bytes=32 time=246ms TTL=63

C:\Users\anusm>ping -n 1 192.168.1.3   | find "Reply"
Reply from 192.168.1.9: Destination host unreachable.

C:\Users\anusm>ping -n 1 192.168.1.4   | find "Reply"
Reply from 192.168.1.9: Destination host unreachable.
```

```
C:\Users\anusm>ping -n 1 192.168.1.5   | find "Reply"

Reply from 192.168.1.5: bytes=32 time=8ms TTL=63


C:\Users\anusm>ping -n 1 192.168.1.6   | find "Reply"

Reply from 192.168.1.9: Destination host unreachable.


C:\Users\anusm>ping -n 1 192.168.1.7   | find "Reply"

Reply from 192.168.1.9: Destination host unreachable.


C:\Users\anusm>ping -n 1 192.168.1.8   | find "Reply"

Reply from 192.168.1.8: bytes=32 time=323ms TTL=63


C:\Users\anusm>ping -n 1 192.168.1.9   | find "Reply"

Reply from 192.168.1.9: bytes=32 time=1ms TTL=64


C:\Users\anusm>ping -n 1 192.168.1.10   | find "Reply"

Reply from 192.168.1.9: Destination host unreachable.
```

Web Footprinting

Check for Open Ports:

```
ComputerName     : example.com
RemoteAddress    : 93.184.216.34
RemotePort       : 80
InterfaceAlias   : Wi-Fi
SourceAddress    : 192.168.0.111
TcpTestSucceeded : True
```

```
StatusCode        : 200
StatusDescription : OK
Content           : <!DOCTYPE HTML>
                    <html lang="en">
                    <head>
                      <meta http-equiv="Content-Type" content="text/html; charset=utf-
8">
                        <meta name="description" content="Whois Lookup for
senselearner.com">
                      <title>Whois s...
RawContent        : HTTP/1.1 200 OK
                    Transfer-Encoding: chunked
                    Connection: keep-alive
                    Vary: Accept-Encoding
                    Strict-Transport-Security: max-age=31536000
```

```
                Content-Type: text/html; charset=UTF-8

                Date: Wed, 27 Sep 2023 ...

Forms           : {whois_search_form, , purchaseFormChk, purchaseForm}

Headers          : {[Transfer-Encoding, chunked], [Connection, keep-alive], [Vary,
Accept-Encoding], [Strict-Transport-Security, max-age=31536000]...}

Images          : {@{innerHTML=; innerText=; outerHTML=<IMG alt=whois.com
src="/images/logo.gif">; outerText=; tagName=IMG; alt=whois.com;

                src=/images/logo.gif}, @{innerHTML=; innerText=;
outerHTML=<IMG class=email alt=email
src="/eimg/f/c4/fc494a5ff01144b9edae06a322b610be3b114849.png"
loading="lazy">; outerText=; tagName=IMG; class=email; alt=email;
src=/eimg/f/c4/fc494a5ff01144b9edae06a322b610be3b114849.png;
loading=lazy}, @{innerHTML=; innerText=; outerHTML=<IMG alt=.biz
src="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAAAEAAAABCAQA
AAC1HAwCAAAAC0lEQVR42mNkYAAAAAYAAjCB0C8AAAAASUVORK5CYII="
width=150                    height=120 data-src="/images/tld/biz.png">;
outerText=; tagName=IMG; alt=.biz;


src=data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAAAEAAAABCAQAA
AC1HAwCAAAAC0lEQVR42mNkYAAAAAYAAjCB0C8AAAAASUVORK5CYII=;
width=150;

                height=120; data-src=/images/tld/biz.png}, @{innerHTML=;
innerText=; outerHTML=<IMG alt=.fun


src="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAAAEAAAABCAQA
AAC1HAwCAAAAC0lEQVR42mNkYAAAAAYAAjCB0C8AAAAASUVORK5CYII="
width=150

                height=120 data-src="/images/tld/fun.png">; outerText=;
tagName=IMG; alt=.fun;


src=data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAAAEAAAABCAQAA
AC1HAwCAAAAC0lEQVR42mNkYAAAAAYAAjCB0C8AAAAASUVORK5CYII=;
width=150;
```

```
                height=120; data-src=/images/tld/fun.png}...}

InputFields      : {@{innerHTML=; innerText=; outerHTML=<INPUT
id=whois_search_input name=query placeholder="Enter Domain or IP">;
outerText=;

                tagName=INPUT; id=whois_search_input; name=query;
placeholder=Enter Domain or IP}, @{innerHTML=; innerText=;
outerHTML=<INPUT

                class=ui-button type=submit value="Submit Query">; outerText=;
tagName=INPUT; class=ui-button; type=submit; value=Submit Query},

                @{innerHTML=; innerText=; outerHTML=<INPUT type=hidden
value=check_availability name=action>; outerText=; tagName=INPUT;
type=hidden;

                value=check_availability; name=action}, @{innerHTML=; innerText=;
outerHTML=<INPUT type=hidden value=true name=phrase_search>;

                outerText=; tagName=INPUT; type=hidden; value=true;
name=phrase_search}...}

Links           : {@{innerHTML=BUY NOW; innerText=BUY NOW; outerHTML=<A
class=btn-white href="https://shop.whois.com/domains/com">BUY NOW</A>;

                outerText=BUY NOW; tagName=A; class=btn-white;
href=https://shop.whois.com/domains/com}, @{innerHTML=<IMG
alt=whois.com                          src="/images/logo.gif">; innerText=;
outerHTML=<A href="/"><IMG alt=whois.com src="/images/logo.gif"></A>;
outerText=; tagName=A;                     href=/}, @{innerHTML=<SPAN
class=title>Register a Domain <SPAN class=triangle-
right></SPAN></SPAN><SPAN class=meta>Get your domain
name now</SPAN> ; innerText=Register a Domain Get your domain name now
; outerHTML=<A
href="https://shop.whois.com/domain-registration/index.php"><SPAN
class=title>Register a Domain <SPAN

                class=triangle-right></SPAN></SPAN><SPAN class=meta>Get your
domain name now</SPAN> </A>; outerText=Register a Domain Get your
domain
```

```
                name now ; tagName=A; href=https://shop.whois.com/domain-
registration/index.php}, @{innerHTML=<SPAN class=title>Domain Suggestions

                <SPAN class=triangle-right></SPAN></SPAN><SPAN class=meta>Get
help picking a domain name</SPAN> ; innerText=Domain Suggestions Get

                help picking a domain name ; outerHTML=<A
href="https://shop.whois.com/domain-registration/domain-name-suggestion-
tool.php"><SPAN

                class=title>Domain Suggestions <SPAN class=triangle-
right></SPAN></SPAN><SPAN class=meta>Get help picking a domain
name</SPAN> </A>;

                outerText=Domain Suggestions Get help picking a domain name ;
tagName=A;

                href=https://shop.whois.com/domain-registration/domain-name-
suggestion-tool.php}...}

ParsedHtml       : mshtml.HTMLDocumentClass

RawContentLength  : 63051
```

Network and WHOIS Enumeration

Network Range (IP Addresses):

```
Name                              Type   TTL   Section    IPAddress

----                           ----   ---   -------    ---------

senselearner.com                   A      14400 Answer     162.250.126.19
```

ASN Information:

```
162.250.126.19 - Server:  192.168.0.1 Address:  192.168.0.1  Name:
stfpanama.com Address:  162.250.126.19
```

Open-Source Intelligence (OSINT)

About SenseLearner: SenseLearner is a globally recognized consulting and implementation firm with a formidable reputation in the cybersecurity domain. Holding the prestigious ISO 27001:2013 certification, SenseLearner has cemented its status as a trusted partner for organizations seeking robust cybersecurity solutions.

Core Services:

- **Risk Assessment and Management:** SenseLearner conducts comprehensive evaluations of digital landscapes to pinpoint vulnerabilities and threats, offering tailored risk management strategies.
- **Vulnerability Assessment and Remediation:** Utilizing cutting-edge technology, SenseLearner identifies and promptly addresses system weaknesses to bolster cybersecurity.
- **Incident Response and Recovery:** In the face of cybersecurity incidents, SenseLearner's rapid-response team minimizes damage, recovers data, and restores normalcy, ensuring minimal disruption.
- **Compliance Support:** SenseLearner aids organizations in navigating the complex realm of cybersecurity regulations, ensuring compliance with industry-specific and regional mandates.
- **Penetration Testing:** SenseLearner's rigorous penetration testing mimics real-world attacks, providing actionable insights into system vulnerabilities.

Commitment to Security: SenseLearner is steadfastly committed to delivering the highest levels of security and peace of mind to its clients. With a focus on ISO 27001:2013 standards and a comprehensive range of cybersecurity services, SenseLearner stands as a beacon of cybersecurity excellence in today's digital landscape.

Vulnerabilities and Security Concerns

During the information gathering and reconnaissance phase, several vulnerabilities and security concerns were identified that merit attention and mitigation. These findings are crucial for enhancing the overall security posture of senselearner.com. The following are key areas of concern:

1. **Outdated Software and Components:**

It was observed that some components of the website, including the web server software and content management system (CMS), are running outdated versions. This poses a potential security risk as outdated software may have known vulnerabilities that could be exploited by malicious actors.

2.Exposed Directories and Files:

Through web footprinting, exposed directories and files were identified on the web server. While some of this information may be intended for public access, sensitive data should not be inadvertently exposed. A review and adjustment of directory and file permissions are advised.

Recommendations

1. Regular Software Updates:

Ensure that all software components, including the web server, CMS, plugins, and libraries, are kept up to date with the latest security patches and updates. Implement a routine maintenance schedule to address vulnerabilities promptly.

2. Strong Access Controls:

Strengthen access controls by enforcing proper authentication and authorization mechanisms. Implement role-based access control (RBAC) to restrict access to sensitive areas and data. Regularly review and revoke unnecessary privileges.

3. Directory and File Permissions:

Review and adjust directory and file permissions to minimize exposure of sensitive information. Implement secure defaults and access controls to protect against unauthorized access.

Conclusion

The information gathering process conducted for senselearner.com has provided a comprehensive view of the website's online presence and security landscape. The key takeaways from this assessment underscore the importance of proactive security measures and vigilance in today's digital environment:

1. Vulnerabilities Exist: The assessment has highlighted vulnerabilities in the website's infrastructure and configurations, including outdated software, inadequate access controls, and potential exposure of sensitive data. These vulnerabilities pose significant security risks and must be promptly addressed.

2. Data Protection Matters: With the increasing emphasis on data privacy, ensuring secure transmission and storage of user data is paramount. The absence of comprehensive HTTPS encryption and secure data handling practices represents an immediate area for improvement.

The significance of these findings cannot be overstated. Addressing vulnerabilities and implementing recommended actions is not only a matter of protecting sensitive data and maintaining operational continuity but also a critical step in upholding user trust and reputation.

As the digital landscape continues to evolve, senselearner.com has an opportunity to not only mitigate existing risks but also establish a robust security foundation for the future. By prioritizing security, the website can confidently navigate the ever-changing threat landscape and provide a safer, more secure online experience for its users.