REPORT

Title: Information Gathering Report for senselearner.com

Date: 22-Sept-2023

Prepared By: Sadiq Sonalkar

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:

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

Executive Summary:

The purpose of this Information Gathering Report is to collect, analyze, and present essential data and insights related to senselearner.com. This report aims to provide a comprehensive understanding on information gathering through various sources.

Introduction:

I Sadiq Sonalkar, intern at senselearner.com. This is my second week into internship and we were tasked to make a report on information gathering on senselearner.com

Domain Information:

- **Domain Name:** senselearner.com

- **IP Address:** 162.250.126.19

- **Registrar:** godaddy.com

- **Registration Date:** 2021-07-01

- **Expiry Date:** 2025-07-01

- **Status:** Active

Domain Information

Domain:	senselearner.com
Registrar:	GoDaddy.com, LLC
Registered On:	2021-07-02
Expires On:	2025-07-01
Updated On:	2023-06-15
Status:	clientDeleteProhibited
	clientRenewProhibited
	clientTransferProhibited
	clientUpdateProhibited
Name Servers:	dns2014a.trouble-free.net
	dns2014b.trouble-free.net

Site	http://senselearner.com ⧉	Domain	senselearner.com
Netblock Owner	Interserver, Inc	Nameserver	dns2014a.trouble-free.net
Hosting company	InterServer Hosting	Domain registrar	godaddy.com
Hosting country	🇺🇸 US ⧉	Nameserver organisation	whois.tucows.com
IPv4 address	162.250.126.19 (VirusTotal) ⧉	Organisation	unknown
IPv4 autonomous systems	AS19318 ⧉	DNS admin	not-monitored-email@interserver.net
IPv6 address	Not Present	Top Level Domain	Commercial entities (.com)
IPv6 autonomous systems	Not Present	DNS Security Extensions	unknown
Reverse DNS	stfpanama.com		

dns:senselearner.com

🔄 dns

Type	Domain Name	IP Address	TTL	Status	Time (ms)	Auth	Parent	Local
NS	dns2014a.trouble-free.net	162.250.126.18 Unknown (AS19318)	24 hrs	✅		✅	✅	✅
NS	dns2014b.trouble-free.net	162.250.126.19 Unknown (AS19318)	24 hrs	✅		✅	✅	✅

Pinging the IP Address to confirm whether its active or not

```
C:\Users\Sadiq>ping 162.250.126.19

Pinging 162.250.126.19 with 32 bytes of data:
Reply from 162.250.126.19: bytes=32 time=210ms TTL=46
Reply from 162.250.126.19: bytes=32 time=213ms TTL=46
Reply from 162.250.126.19: bytes=32 time=216ms TTL=46
Reply from 162.250.126.19: bytes=32 time=187ms TTL=46

Ping statistics for 162.250.126.19:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 187ms, Maximum = 216ms, Average = 206ms
```

Its Active.

DNS Footprinting:

List of DNS Records:
A record:

	a:senselearner.com	Find Problems			🔄 a

Type	Domain Name	IP Address	TTL
A	senselearner.com	162.250.126.19 Unknown (AS19318)	4 hrs

	Test	Result
✅	DNS Record Published	DNS Record found

dns check   mx lookup   dmarc lookup   spf lookup   dns propagation

Reported by **dns2014b.trouble-free.net** on 9/24/2023 at **4:45:53 AM (UTC -5)**, just for you.   Transcript

DNS record:

dns:senselearner.com [Find Problems]   [⟳ dns]

Type	Domain Name	IP Address	TTL	Status	Time (ms)	Auth	Parent	Local
NS	dns2014a.trouble-free.net	162.250.126.18 Unknown (AS19318)	24 hrs	✅	10	✅	✅	✅
NS	dns2014b.trouble-free.net	162.250.126.19 Unknown (AS19318)	24 hrs	✅	10	✅	✅	✅

	Result	
⚠️	Name Servers are on the Same Subnet `162.250.126`	ℹ️ More Info

MX record:

mx:senselearner.com [Find Problems] [Solve Email Delivery Problems]   [⟳ mx]

Pref	Hostname	IP Address	TTL		
1	ASPMX.L.GOOGLE.com	172.253.63.26 Unknown (AS15169)	4 hrs	Blacklist Check	SMTP Test
1	ASPMX.L.GOOGLE.com	2607:f8b0:4004:c09::1a	4 hrs	Blacklist Check	
5	ALT1.ASPMX.L.GOOGLE.com	74.125.193.27 Unknown (AS15169)	4 hrs	Blacklist Check	SMTP Test
5	ALT1.ASPMX.L.GOOGLE.com	2a00:1450:400b:c01::1a	4 hrs	Blacklist Check	
5	ALT2.ASPMX.L.GOOGLE.com	64.233.184.26 Unknown (AS15169)	4 hrs	Blacklist Check	SMTP Test
5	ALT2.ASPMX.L.GOOGLE.com	2a00:1450:400c:c0b::1a	4 hrs	Blacklist Check	
10	ALT3.ASPMX.L.GOOGLE.com	142.250.27.27 Unknown (AS15169)	4 hrs	Blacklist Check	SMTP Test
10	ALT3.ASPMX.L.GOOGLE.com	2a00:1450:4025:401::1b	4 hrs	Blacklist Check	
10	ALT4.ASPMX.L.GOOGLE.com	142.250.153.27 Unknown (AS15169)	4 hrs	Blacklist Check	SMTP Test
10	ALT4.ASPMX.L.GOOGLE.com	2a00:1450:4013:c16::1a	4 hrs	Blacklist Check	

DMARC record:

dmarc:senselearner.com [Find Problems] [Solve Email Delivery Problems]   [⟳ dmarc]

	Test	Result	
❌	DMARC Record Published	No DMARC Record found	ℹ️ More Info

dns lookup   dns check   mx lookup   spf lookup   dns propagation

Reported by dns2014a.trouble-free.net on 9/24/2023 at **4:50:36 AM (UTC -5)**, just for you.   Transcript

SPF record:

```
v=spf1 +a +mx +ip4:162.250.126.18 include:relay.is.cc ~all
```

Prefix	Type	Value	PrefixDesc	Description
	v	spf1		The SPF record version
+	a		Pass	Match if IP has a DNS 'A' record in given domain.
+	mx		Pass	Match if IP is one of the MX hosts for given domain name.
+	ip4	162.250.126.18	Pass	Match if IP is in the given range.
+	include	relay.is.cc	Pass	The specified domain is searched for an 'allow'.
~	all		SoftFail	Always matches. It goes at the end of your record.

dns2014a.trouble-free.net (SOA)

Type	Domain Name	TTL	Record
TXT	senselearner.com	24 hrs	`google-site-verification=21dWAeLOTAQNSrIU2i9Yz1B0tIKGG9XWbI5XunkOx10`
TXT	senselearner.com	4 hrs	`v=spf1 +a +mx +ip4:162.250.126.18 include:relay.is.cc ~all`

dns2014b.trouble-free.net (Matches SOA)

Type	Domain Name	TTL	Record
TXT	senselearner.com	24 hrs	`google-site-verification=21dWAeLOTAQNSrIU2i9Yz1B0tIKGG9XWbI5XunkOx10`
TXT	senselearner.com	4 hrs	`v=spf1 +a +mx +ip4:162.250.126.18 include:relay.is.cc ~all`

dns lookup   dns check   mx lookup   dmarc lookup

Cname record:

	Test	Result	
❌	DNS Record Published	DNS Record not found	ⓘ More Info

dns lookup   dns check   mx lookup   dmarc lookup   dns propagation

Reported by **dns2014b.trouble-free.net** on 9/24/2023 at **4:51:38 AM (UTC -5)**, just for you.   Transcript

Name server record:

NS ⊕

Type	Domain Name	TTL	Canonical Name
NS	senselearner.com	4248	dns2014a.trouble-free.net. (162.250.126.18 ☑ | Check IP Blacklist) Owner: InterServer Inc 🇺🇸	WHOIS	AS19318
NS	senselearner.com	4248	dns2014b.trouble-free.net. (162.250.126.19 ☑ | Check IP Blacklist) Owner: InterServer Inc 🇺🇸	WHOIS	AS19318

SOA and TXT record:

SOA ⊕

Type	Domain Name	TTL	Primary NS	Responsible Email
SOA	senselearner.com	8205	dns2014a.trouble-free.net.	not-monitored-email.interserver.net.

TXT ⊕

Type	Domain Name	TTL	Record
TXT	senselearner.com	11296	v=spf1 +a +mx +ip4:162.250.126.18 include:relay.is.cc ~all
TXT	senselearner.com	18496	google-site-verification =21dWAeLOTAQNSrIU2 i9YzIB0tIKGG9XWbI5Xu nkOx10

Subdomains: Enumerate any subdomains discovered.

Total results for senselearner.com — 7 subdomains scanned on 24 Sep 2023 10:00:19 AM. Scan ID: 6846864766632

No	Subdomain	IP	Provider
1	cpanel.senselearner.com	162.250.126.19	Interserver, Inc Secaucus, United States
2	cpcontacts.senselearner.com	162.250.126.19	Interserver, Inc Secaucus, United States
3	senselearner.com	162.250.126.19	Interserver, Inc Secaucus, United States
4	webmail.senselearner.com	162.250.126.19	Interserver, Inc Secaucus, United States
5	webdisk.senselearner.com	162.250.126.19	Interserver, Inc Secaucus, United States
6	cpcalendars.senselearner.com	162.250.126.19	Interserver, Inc Secaucus, United States
7	crm.senselearner.com	103.118.16.154	Neerja Softwares Pvt Ltd Jaipur, India

Web Footprinting:

Web Server Information:
Tracing route to senselearner.com


```
Microsoft Windows [Version 10.0.22621.2283]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Sadiq>Tracert senselearner.com

Tracing route to senselearner.com [162.250.126.19]
over a maximum of 30 hops:

  1     2 ms    <1 ms     1 ms  192.168.1.1
  2     4 ms     4 ms     1 ms  103.250.36.225
  3     5 ms     1 ms     1 ms  103.250.39.33
  4     5 ms     5 ms     2 ms  103.184.155.253
  5     5 ms     2 ms     2 ms  103.228.155.165
  6     9 ms     *        *     125.19.50.17
  7   194 ms   194 ms   195 ms  116.119.57.19
  8   281 ms   304 ms   305 ms  eqix-ny2.interserver.com [198.32.118.45]
  9   315 ms   304 ms   307 ms  64.20.32.213
 10     *      342 ms   332 ms  switch26.as19318.net [64.20.32.138]
 11   242 ms   304 ms   304 ms  switch34n.trouble-free.net [173.225.96.227]
 12   307 ms   305 ms   304 ms  stfpanama.com [162.250.126.19]

Trace complete.
```

Webserver Software:

Check Website Webserver

Enter Url or IP:

| 162.250.126.19 | | Find it |

162.250.126.19

| Webserver Software: | LiteSpeed |

Domains hosted in same web server as senselearner.com:

you get signal

Reverse IP Domain Check

Remote Address [senselearner.com] [Check]

Found **39** domains hosted on the same web server as senselearner.com (162.250.126.19).

american-seo.com	bitch9.tk
blogcharge.com	careerscoop.in
cloudfunda.tk	creativedezinesolutions.com
dutchessderm.com	escolta.shop
impa.gov.eg	itempiamoslubos.org
kingadz.com	kuotabelajar.xyz
loudtechie.com	mangumstarnews.net
maroccoupon.com	martialartscorner.com
mobile-legend.me	mq.gl
netfliix.gq	no-kr.com
number.xmohamed.com	peraquamspa.com
saradhicfe.com	scfe.net.in
senselearner.com	terrydrakebasketball.com
tradex-investment.com	transitiontalks.org
vairuokautomobili.lt	viit.edu.in
wordsmithkaur.com	www.axcontrol.com
www.boholwebwp.com	www.openroadac.com
www.senselearner.com	www.travellersblogs.com
www.trsrentelco.com	x-grips.com
xmohamed.com	

History of Senselearner.com:

	013	2014	2015	2016	2017	2018	2019	2020	2021	2022	**2023**
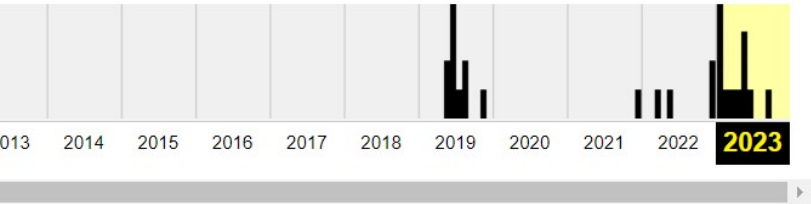
Multipurpose Internet Mail Extensions Count:

Quick search on MIME-types...   << < 1 2 > >>

Captures

	Captures	URLs	New URLs
text/html	592	260	228
text/css	99	97	97
application/javascript	94	89	89
image/png	92	86	86
application/json	55	43	43
image/jpeg	47	43	43
image/svg+xml	25	23	23
font/ttf	4	4	4
image/gif	3	3	3
application/xml	3	2	1
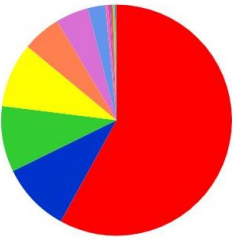
Explore senselearner.com URLs

URL's of senselearner.com:

861 URLs have been captured for this URL prefix.

Filter results by URL or MIME Type (i.e. '.txt')

URL ↑	MIME Type	From	To	Captures	Duplicates	Uniques
http://senselearner.com/bundles/jqueryval3656?v=hEGG8cMxk9p0ncdRUOJ-CniKN7NezhnPnWlvn6REucZo1	unk	Mar 12, 2022	Mar 12, 2022	1	0	1
http://senselearner.com/bundles/lib83ce?v=ZajcXlX04vV7hjQq2qUW43-f5AylM45iszlT1Q4XTA01	unk	Mar 23, 2022	Mar 23, 2022	1	0	1
http://senselearner.com/bundles/modernizr8fce?v=wBEWDufH_8Md-Pbioxomf90vm6lJN2Pyy9u9zHtWsPo1	unk	Feb 17, 2022	Feb 17, 2022	1	0	1
http://senselearner.com/cgi-sys/suspendedpage.cgi	text/html	Sep 22, 2022	Sep 22, 2022	1	0	1
http://senselearner.com/Content/ajax-loader.gif	image/gif	May 14, 2022	May 14, 2022	1	0	1
http://senselearner.com/Content/css02ca.css?v=XeliJGeqedMLOD288CCYPjd2cJxhlk8J2uDB8o9_Mts1	text/css	Apr 21, 2022	Apr 21, 2022	1	0	1
http://senselearner.com/Content/fonts/Montserrat-Bold.ttf	font/ttf	Apr 29, 2022	Apr 29, 2022	1	0	1
http://senselearner.com/Content/fonts/Montserrat-Medium.ttf	font/ttf	Apr 29, 2022	Apr 29, 2022	1	0	1
http://senselearner.com/Content/fonts/Montserrat-Regular.ttf	font/ttf	Apr 29, 2022	Apr 29, 2022	1	0	1
http://senselearner.com/Content/fonts/slick.woff	font/woff	Apr 29, 2022	Apr 29, 2022	1	0	1
http://senselearner.com/Content/images/02.jpg	image/jpeg	May 14, 2022	May 14, 2022	1	0	1
http://senselearner.com/Content/images/03.jpg	image/jpeg	May 14, 2022	May 14, 2022	1	0	1
http://senselearner.com/Content/images/Application Security.png	image/png	Mar 22, 2022	Mar 22, 2022	1	0	1
http://senselearner.com/Content/images/caret.png	image/png	Apr 8, 2022	Apr 8, 2022	1	0	1
http://senselearner.com/Content/Images/CompaniesSlider/01.jpg	image/jpeg	Jun 27, 2022	Jun 27, 2022	1	0	1
http://senselearner.com/Content/Images/CompaniesSlider/02.jpg	image/jpeg	Feb 17, 2022	Feb 17, 2022	1	0	1
http://senselearner.com/Content/Images/CompaniesSlider/03.jpg	image/jpeg	May 11, 2022	May 11, 2022	1	0	1
http://senselearner.com/Content/Images/CompaniesSlider/05.jpg	image/jpeg	May 11, 2022	May 11, 2022	1	0	1

Technologies in Use:

Senselearner.com was built with using:

SENSELEARNER.COM

Analytics and Tracking
View Global Trends

G Google Analytics
Google Analytics Usage Statistics · Download List of All Websites using Google Analytics
Google Analytics offers a host of compelling features and benefits for everyone from senior executives and advertising and marketing professionals to site owners and content developers.
Application Performance · Audience Measurement · Visitor Count Tracking

G Google Analytics 4
Google Analytics 4 Usage Statistics · Download List of All Websites using Google Analytics 4
Google Analytics 4 formerly known as App + Web is a new version of Google Analytics that was released in October 2020.

G Global Site Tag
Global Site Tag Usage Statistics · Download List of All Websites using Global Site Tag
Google's primary tag for Google Measurement/Conversion Tracking, Adwords and DoubleClick.

Widgets
View Global Trends

Chaty Premio
Chaty Premio Usage Statistics · Download List of All Websites using Chaty Premio
Wordpress and Shopify chat program.
Live Chat

G Google Font API
Google Font API Usage Statistics · Download List of All Websites using Google Font API
Fonts

Wordpress Plugins
Wordpress Plugins Usage Statistics · Download List of All Websites using Wordpress Plugins
Plugins are tools to extend the functionality of WordPress. The website uses various plugins from WordPress to provide additional functionality. Some of them may be listed here.

Contact Form 7
Contact Form 7 Usage Statistics · Download List of All Websites using Contact Form 7
Specifically designed for wordpress blogs. Contact Form 7 can manage multiple contact forms, plus you can customize the form and the mail contents flexibly with simple markup.
Feedback Forms and Surveys

Slider Revolution
Slider Revolution Usage Statistics · Download List of All Websites using Slider Revolution
A response sliding image plugin.
WordPress Plugins

Font Awesome
Font Awesome Usage Statistics · Download List of All Websites using Font Awesome
Iconic font and CSS toolkit.
Fonts

G Google Tag Manager
Google Tag Manager Usage Statistics · Download List of All Websites using Google Tag Manager
Tag management that lets you add and update website tags without changes to underlying website code.
Tag Management

Yoast Plugins
Yoast Plugins Usage Statistics · Download List of All Websites using Yoast Plugins
SEO based plugins from Yoast.
WordPress Plugins

Yoast Plugins Usage Statistics · Download List of All Websites using Yoast Plugins
SEO based plugins from Yoast.
WordPress Plugins

Yoast WordPress SEO Plugin
Yoast WordPress SEO Plugin Usage Statistics · Download List of All Websites using Yoast WordPress SEO Plugin
Functionality that helps you optimize your pages content, images titles, meta descriptions and more.

US Privacy User Signal Mechanism
US Privacy User Signal Mechanism Usage Statistics · Download List of All Websites using US Privacy User Signal Mechanism
The US Privacy API (USP API) is a lightweight API used to communicate signals represented in the US Privacy String.
Privacy Compliance

Twemoji
Twemoji Usage Statistics · Download List of All Websites using Twemoji
Twitter Emoji for Everyone

Blog Designer Pack
Blog Designer Pack Usage Statistics · Download List of All Websites using Blog Designer Pack
Display blog posts on your Wordpress website with 6 blog layouts.
WordPress Plugins

Testimonial Builder
Testimonial Builder Usage Statistics · Download List of All Websites using Testimonial Builder
Quotes and testimonial management plugin for wordpress.
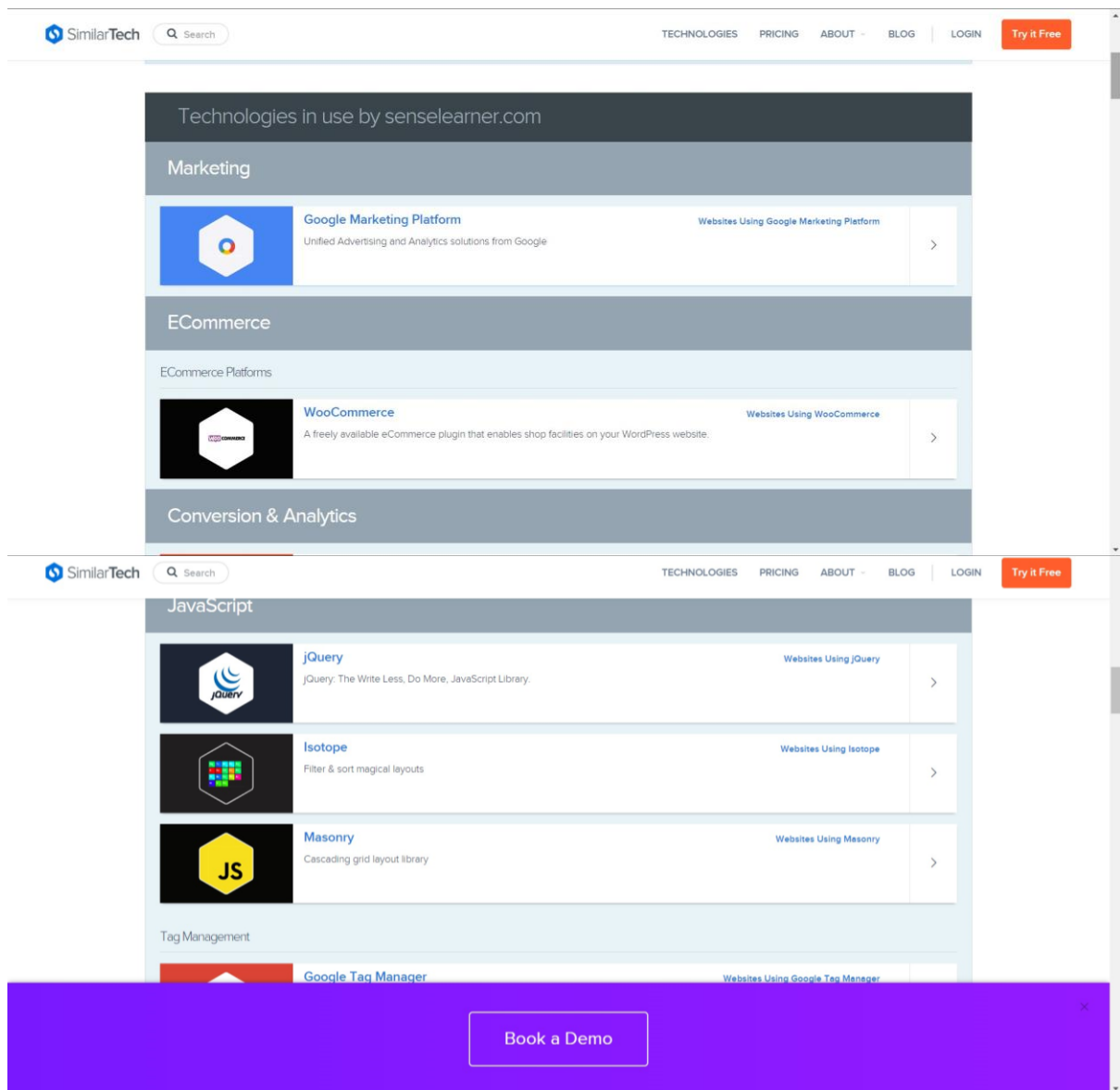WordPress Plugins

WP Custom Cursors
WP Custom Cursors Usage Statistics · Download List of All Websites using WP Custom Cursors
Enables integration of custom cursors.
WordPress Plugins

CrUX Dataset
CrUX Dataset Usage Statistics · Download List of All Websites using CrUX Dataset

---

Profile Details
Change Layout

Last technology detected on 18th September 2023. We know of 76 technologies on this page and 65 technologies removed from senselearner.com since 2nd April 2019. Link to this page.

Get a notification when senselearner.com adds new technologies.

Create Notification

Recent Lookups

goingoffscript.com	perfectketo.com
discogalerie.com	cygniamaintenance.com
twpl.com	nutraco.com
ujmd.edu.sv	sandellcontractors.co.uk
xboxliveshop.nl	sharek961.org
rbw-cgi.it	marketsfloor.com
jardins.lu	zeygos.com
livehealthystate.org	innteva.com
younginklings.org	vitalindia.org
elrecibidor.com	homespiremortgage.com
lencse.hu	casalugano.ch
ceezer.earth	brascri.ch
afamconcept.com	sop.se
ecossolar.mx	crescendam.fr
benjaminurson.com	slideshuttle.com
tenk.se	1234.sk
investeamrealty.com	pmcaddy.com
piguslesiai.lt	websmart.site
gatewaysurveyors.co.uk	fb.com
roematec.com	goldlawgroup.com
iowasigncompany.com	themedicube.co.kr
tcmortgageservices.com	craftbeertemple.com
legionbox.com	futurescholar.com
stencoconstruction.com	resolutionlawng.com
endisputes.com	centralgrower.com
werent.co	watsonburns.com
sevenandtwelve.com	1hao.mobi
beautifulcode.co	greenerfootprints.com
mariani.com	sonicbee.nl
dateaha.com	senselearner.com

Get senselearner.com profile as an XML, JSON, CSV or XLSX via the Domain API.

Suggest a Technology

Can't find the technology you are looking for? Send us a suggestion, we will try and add it to our database.

URL pages crawling:

Metadata: Include metadata from web pages, if available.

```
{
  "title": "Cyber Security Services Company in India",
  "description": "Senselearner is a leading cyber security company serving clients in India. Hire the best cyber security service & s
  "images": [
    "https://senselearner.com/wp-content/uploads/2018/04/slider-1-bg.jpg"
  ],
  "duration": 1075,
  "domain": "senselearner.com",
  "url": "https://senselearner.com/"
}
```

Network and WHOIS Enumeration:

Network Range:

SuperTool Beta7

| senselearner.com | DNS Check ▾ |

dns:senselearner.com [Find Problems] ⟳ dns

Type	Domain Name	IP Address	TTL	Status	Time (ms)	Auth	Parent	Local
NS	dns2014a.trouble-free.net	162.250.126.18 Unknown (AS19318)	24 hrs	✅		✅	✅	✅
NS	dns2014b.trouble-free.net	162.250.126.19 Unknown (AS19318)	24 hrs	✅	21	✅	✅	✅

	Result	
⚠️	Name Servers are on the Same Subnet 162.250.126	ℹ️ More Info

WHOIS Records:

senselearner.com

Updated 2 hours ago ⟳

Domain Information

Domain:	senselearner.com
Registrar:	GoDaddy.com, LLC
Registered On:	2021-07-02
Expires On:	2025-07-01
Updated On:	2023-06-15
Status:	clientDeleteProhibited clientRenewProhibited clientTransferProhibited clientUpdateProhibited
Name Servers:	dns2014a.trouble-free.net dns2014b.trouble-free.net

Registrant Contact

Name:	Registration Private
Organization:	Domains By Proxy, LLC
Street:	DomainsByProxy.com 2155 E Warner Rd
City:	Tempe
State:	Arizona
Postal Code:	85284
Country:	US
Phone:	+1.4806242599
Fax:	+1.4806242598
Email:	Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=senselearner.com

Administrative Contact

Name:	Registration Private
Organization:	Domains By Proxy, LLC
Street:	DomainsByProxy.com 2155 E Warner Rd
City:	Tempe
State:	Arizona
Postal Code:	85284
Country:	US
Phone:	+1.4806242599
Fax:	+1.4806242598
Email:	Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=senselearner.com

Technical Contact

Name:	Registration Private
Organization:	Domains By Proxy, LLC
Street:	DomainsByProxy.com 2155 E Warner Rd
City:	Tempe
State:	Arizona
Postal Code:	85284
Country:	US
Phone:	+1.4806242599
Fax:	+1.4806242598
Email:	Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=senselearner.com

ASN Information:

asn:162.250.126.19

↻ asn

Total amount of IPs for this ASN: **2,048**

As Number	As Name	CIDR Range	Monitor
19318	Unknown	162.250.120.0/21	

Name Servers	DNS2014A.TROUBLE-FREE.NET (has 144,979 domains) DNS2014B.TROUBLE-FREE.NET (has 144,979 domains)
IP Address	162.250.126.19 - 1,071 other sites hosted on this server
IP Location	- New Jersey - Secaucus - Interserver Inc
ASN	AS19318 IS-AS-1, US (registered Dec 09, 2005)

Open-Source Intelligence (OSINT):

SpiderFoot Reconnaisance:
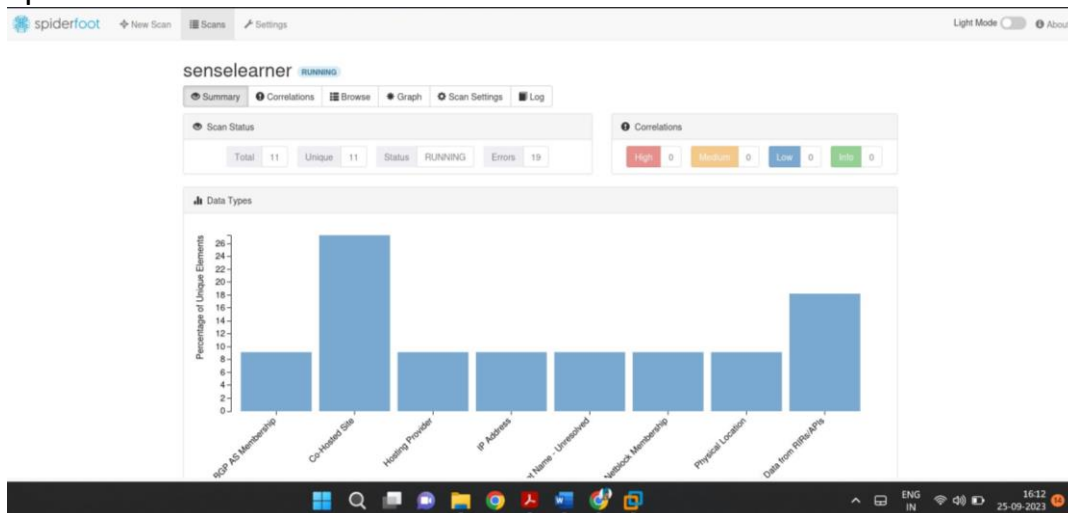
Shodan.io:
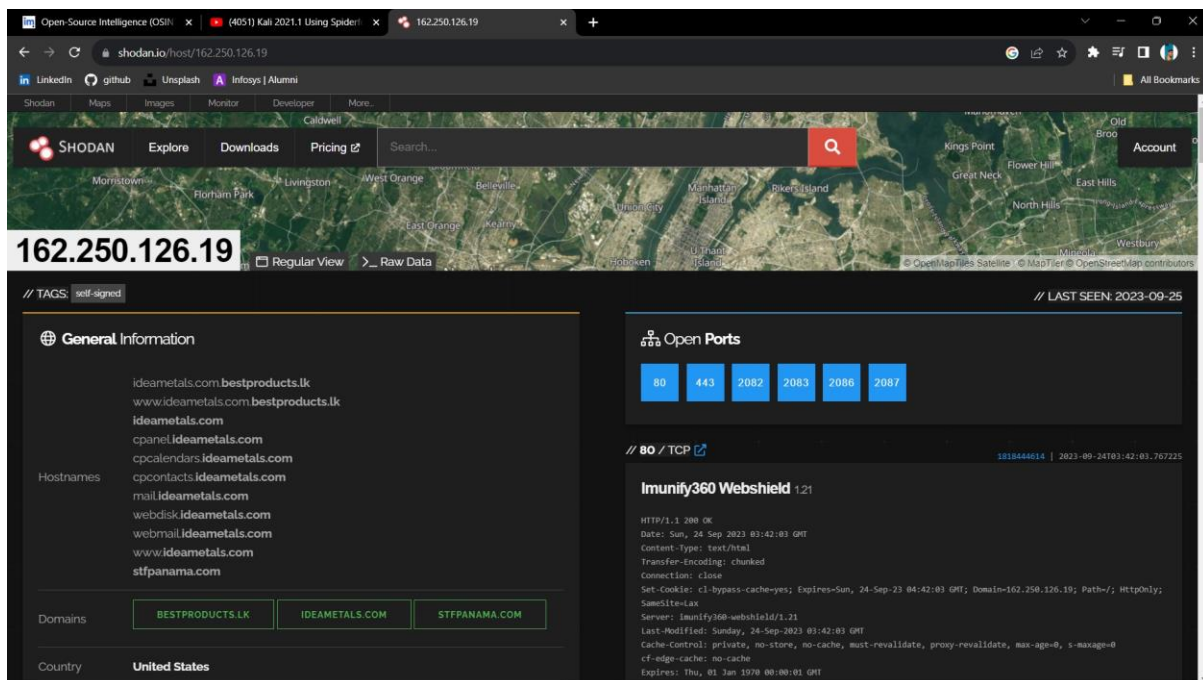
LinkedIn:
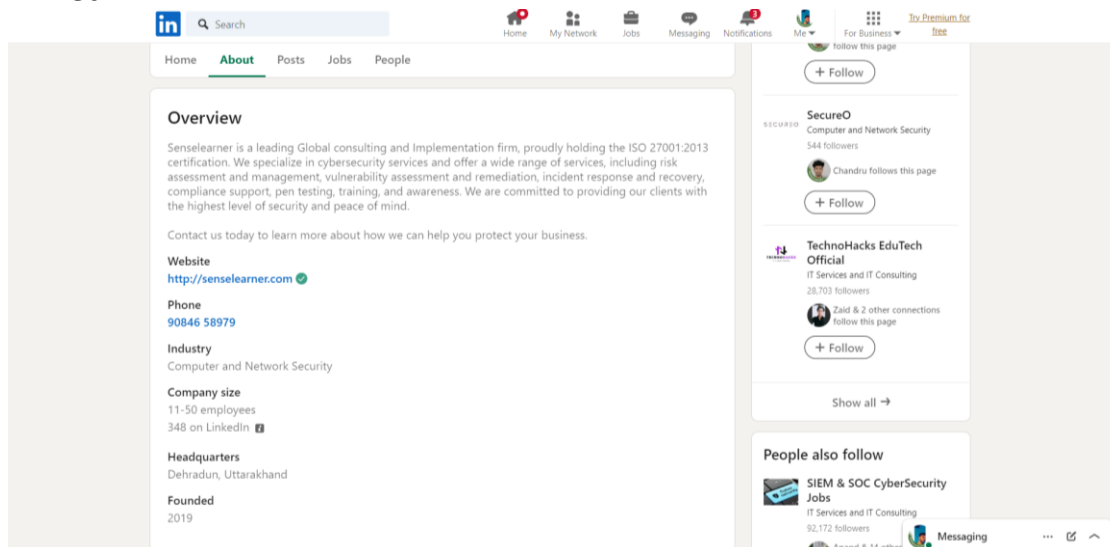
Facebook:
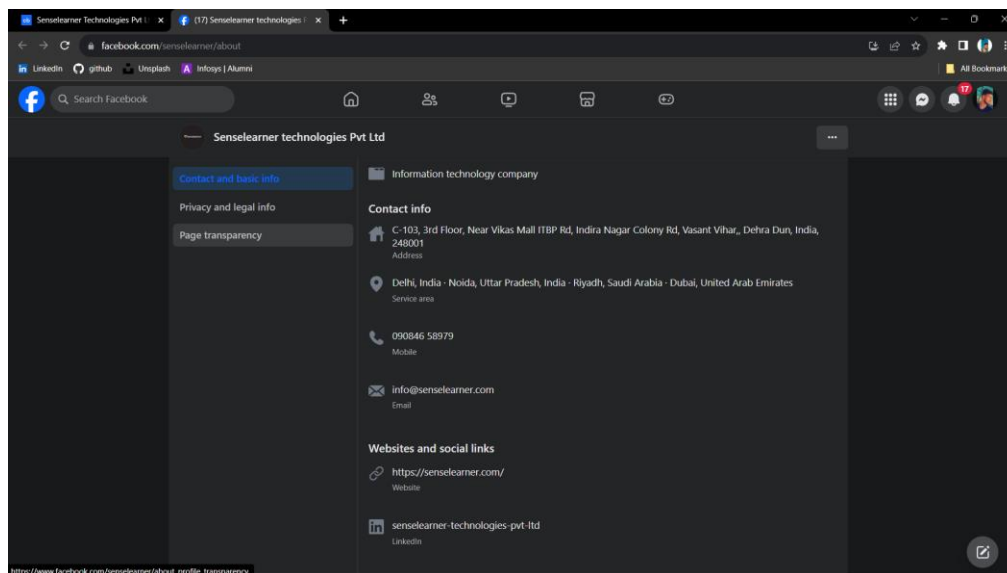
Directors:

About Senselearner Technologies Private Limited

Senselearner Technologies Private Limited is a Unlisted Private Company. It was incorporated on 07 August, 2019.
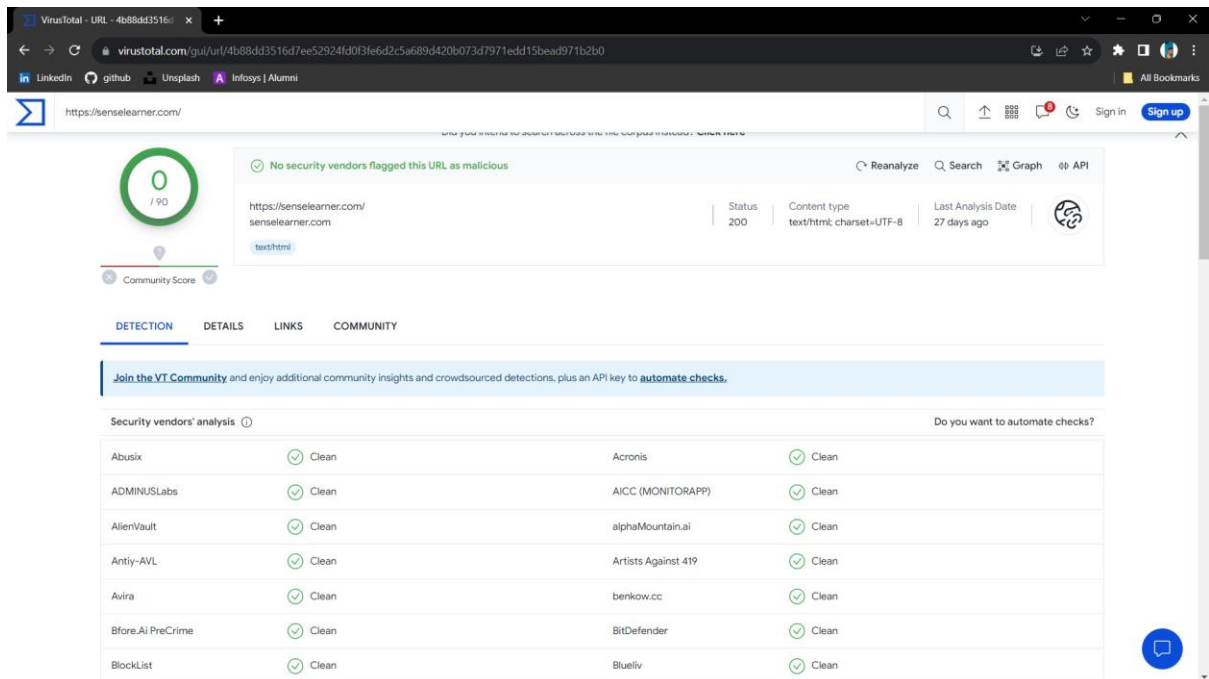
It is a Company limited by Shares having its registered office at C/O. Gulam Rasool, 7, Jagat Farm, Amrit Puram Chowk, Near Pari Chowk, Greater Noida, Noida Gautam Buddha Nagar Uttar Pradesh - 201301 India. It is further classified as a Non-govt company.

The CIN number of Senselearner Technologies Private Limited is U72900UP2019PTC119946.

Senselearner Technologies Private Limited has 2 appointed directors/decision makers Pawan Sikarbar and Gulam Rasool.

CIN:	U72900UP2019PTC119946	**Industry:**	Computer Related Services
Type:	Unlisted Private Company	**Founded:**	07 August, 2019
Revenue:	Undisclosed	**Authorized Capital:**	Less than $10,000
Paid-up Capital:	Less than $10,000	**Category:**	Company limited by Shares
Sub-Category:	Non-govt company	**Address:**	C/O. Gulam Rasool, 7, Jagat Farm, Amrit Puram Chowk, Near Pari Chowk, Greater Noida, Noida Gautam Buddha Nagar Uttar Pradesh - 201301 India
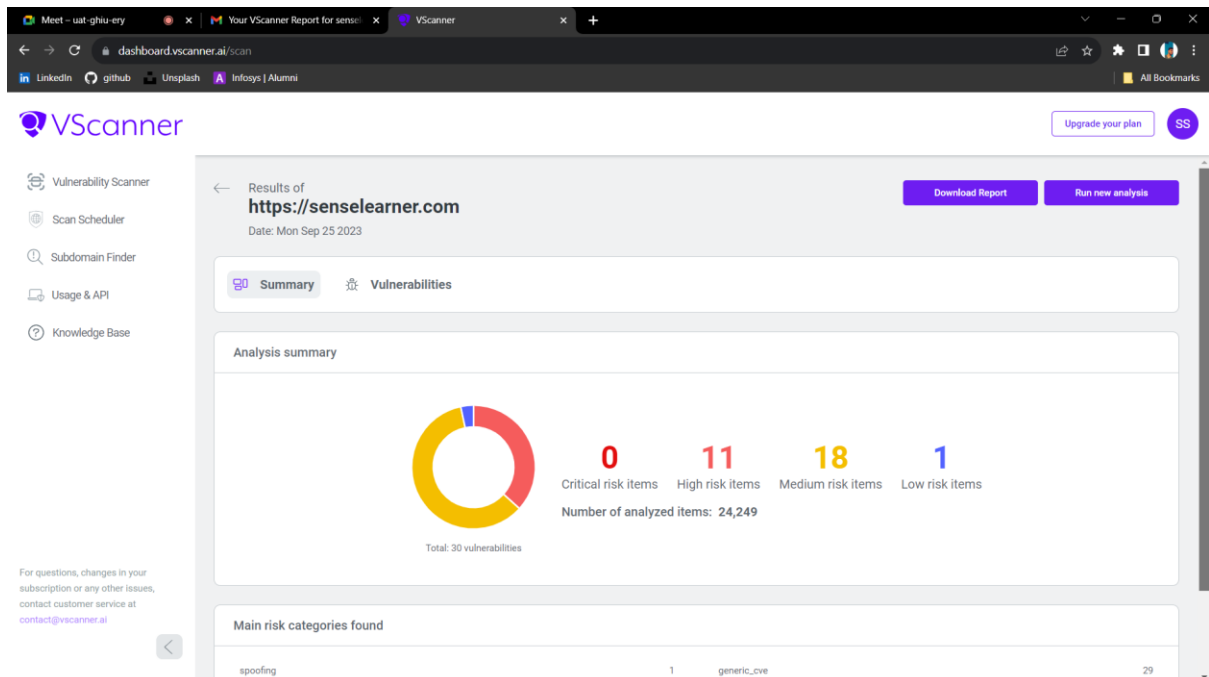
Vulnerabilities and Security Concerns:

VirusTotal:

VScanner:

Following are the vulnerabilities:

1. The domain http://senselearner.com may be vulnerable to email spoofing - Medium Risk
2. openbsd.openssh.protocol2.0.OpenSSH@7.4 - Medium Risk
3. woocommerce@2.7.0 - Medium Risk
4. woocommerce@2.1.4 - Medium Risk

Recommendations:

The solution for vulnerabilities:

1. The domain http://senselearner.com may be vulnerable to email spoofing = Set up DMARC, DKIM, and SPF for email security. DMARC requires creating a record in your domain's DNS, detailing report address and message failure policy. DKIM involves generating a public/private key pair, publishing the public key in DNS as a TXT record, and configuring your email server to sign messages with the private key. SPF requires creating a DNS record that lists authorized email servers for your domain. Setup can vary with different

email server software and hosting providers; check your specific setup's documentation.

2. **openbsd.openssh.protocol2.0.OpenSSH@7.4** = Update the software to the latest version

3. **woocommerce@2.7.0** = Update the software to the latest version

4. **woocommerce@2.1.4** = Update the software to the latest version

Conclusion:

In conclusion, the reconnaissance report has provided valuable insights and data on senselearner.com. These findings collectively contribute to a better understanding and will be instrumental in guiding future actions and decision-making. It is crucial to highlight that while the reconnaissance mission has yielded important information, further investigation and analysis may be required to gain a comprehensive view.

References:

https://who.is/whois/senselearner.com
https://mxtoolbox.com/SuperTool.aspx?action=a%3asenselearner.com&run=toolpage
https://www.whois.com/whois/senselearner.com
https://sitereport.netcraft.com/?url=http://senselearner.com
https://www.hackingarticles.in/beginner-guide-website-footprinting/
https://builtwith.com/senselearner.com
https://mxtoolbox.com/SuperTool.aspx?action=a%3asenselearner.com&run=toolpage
https://whois.domaintools.com/senselearner.com
https://mxtoolbox.com/SuperTool.aspx?action=asn%3asenselearner.com&run=toolpage
https://pentest-tools.com/website-vulnerability-scanning/discover-hidden-directories-and-files
https://nanonets.com/website-scraper
https://www.lantechsoft.com/web-data-extractor.html
https://web.archive.org/web/*/senselearner.com*
https://iplocation.io/website-server-software/162.250.126.19