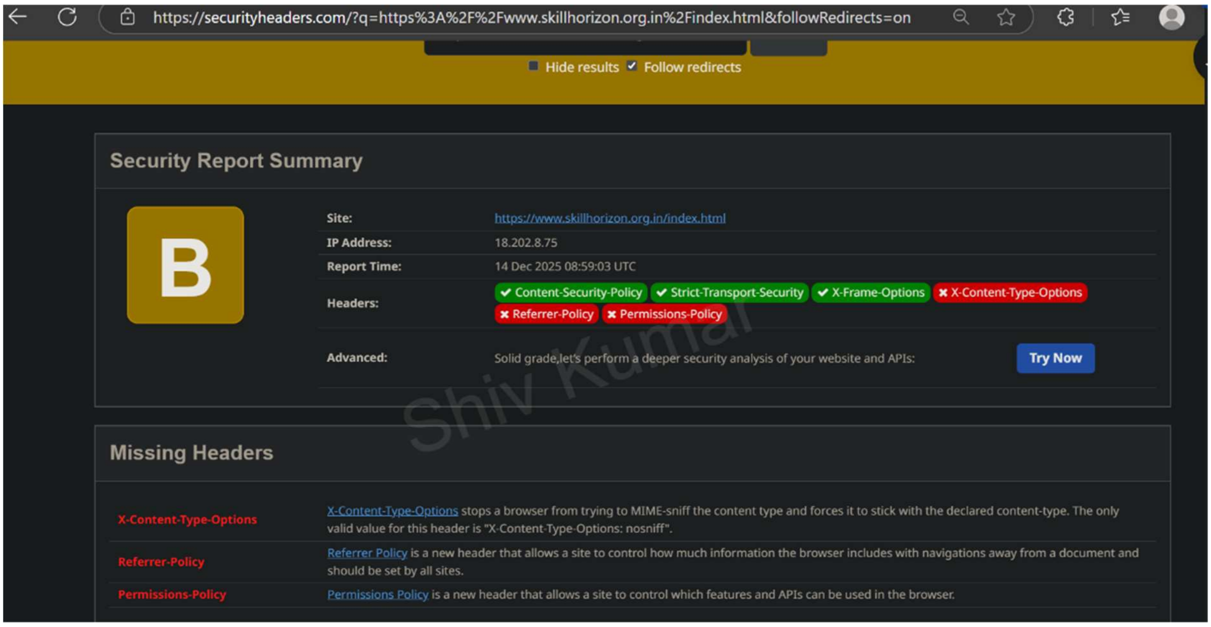
Assessment 7 VAPT : Vulnerability Assessment & Penetration Testing Red teaming Static analysis

Using Domain skillhorizon.com

1. **Security headers** Content-security-policy X-content-type-options Strict-Transport-security X-frame-options X-Xss-protection Cache-control



https://securityheaders.com/?q=https%3A%2F%2Fwww.skillhorizon.org.in%2Findex.html&followRedirects=on

■ Hide results ☑ Follow redirects

Security Report Summary

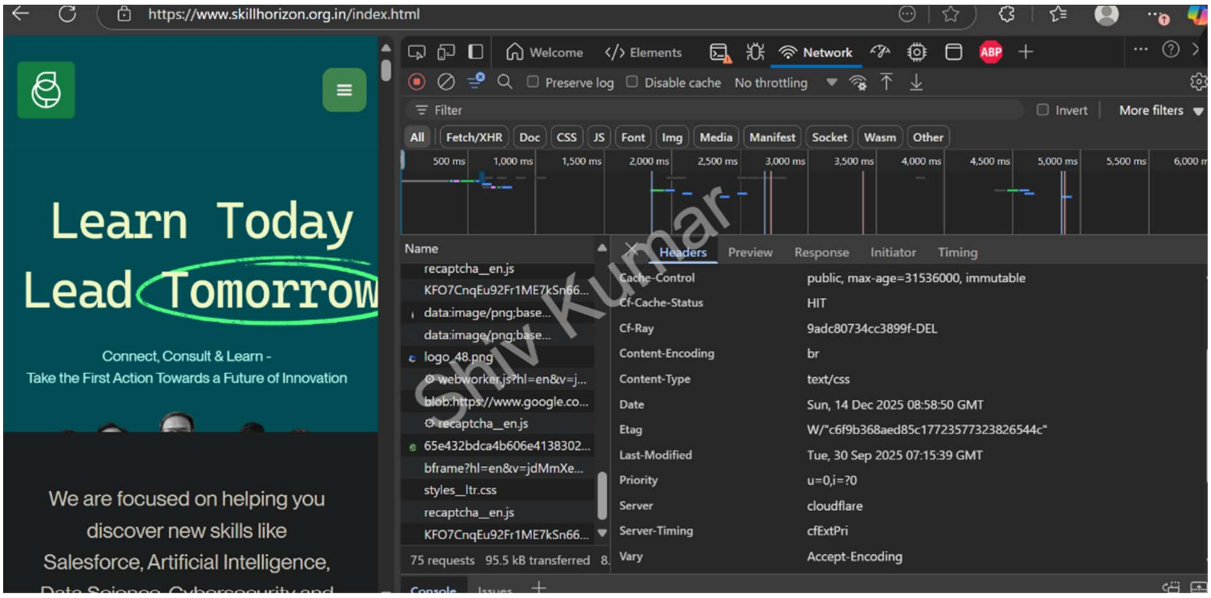
B

Site:	https://www.skillhorizon.org.in/index.html
IP Address:	18.202.8.75
Report Time:	14 Dec 2025 08:59:03 UTC
Headers:	✓ Content-Security-Policy ✓ Strict-Transport-Security ✓ X-Frame-Options ✗ X-Content-Type-Options ✗ Referrer-Policy ✗ Permissions-Policy
Advanced:	Solid grade,let's perform a deeper security analysis of your website and APIs: Try Now

Missing Headers

X-Content-Type-Options	X-Content-Type-Options stops a browser from trying to MIME-sniff the content type and forces it to stick with the declared content-type. The only valid value for this header is "X-Content-Type-Options: nosniff".
Referrer-Policy	Referrer Policy is a new header that allows a site to control how much information the browser includes with navigations away from a document and should be set by all sites.
Permissions-Policy	Permissions Policy is a new header that allows a site to control which features and APIs can be used in the browser.

2. **SSL Cert Testing Ssllabs.com**
   Only cache-control security header is present
   -Missing one’s list having below names
   Content security policy
   X-content-type-options
   Strict-Transport-security
   X-frame-options
   X-Xss-protection
   Cache-control



https://www.skillhorizon.org.in/index.html

Learn Today
Lead Tomorrow

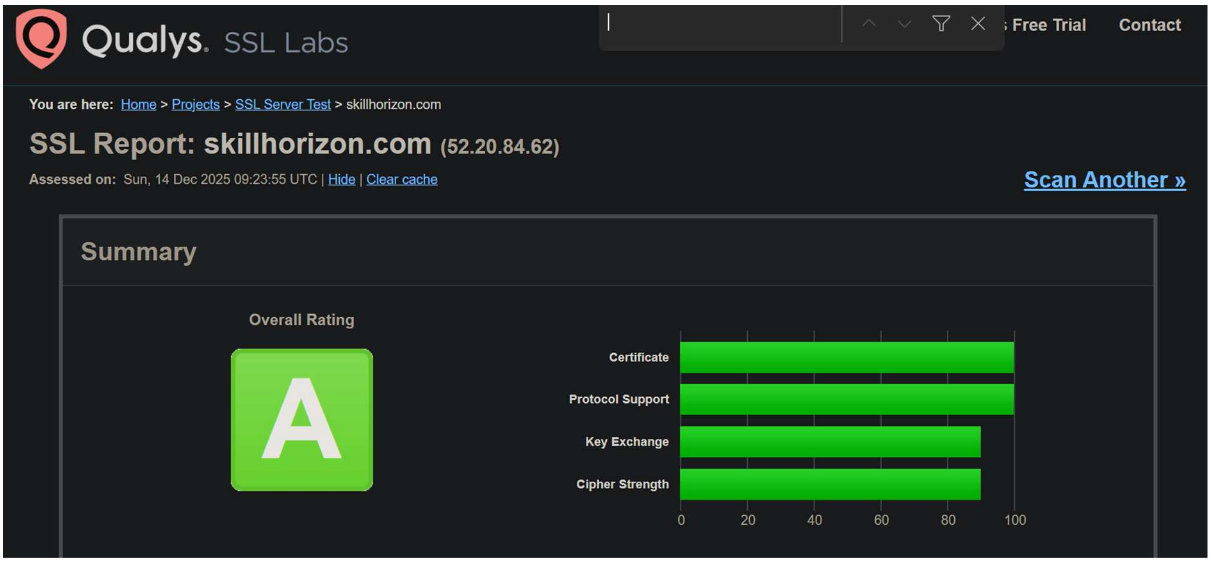
Connect, Consult & Learn -
Take the First Action Towards a Future of Innovation

We are focused on helping you discover new skills like Salesforce, Artificial Intelligence, Data Science, Cybersecurity and

Name
recaptcha__en.js
KFO7CnqEu92Fr1ME7kSn66...
data:image/png;base...
data:image/png;base...
logo_48.png
webworker.js?hl=en&v=j...
blob:https://www.google.co...
recaptcha__en.js
65e432bdca4b606e4138302...
bframe?hl=en&v=jdMmXe...
styles__ltr.css
recaptcha__en.js
KFO7CnqEu92Fr1ME7kSn66...
75 requests 95.5 kB transferred 8.

Cache-Control	public, max-age=31536000, immutable
Cf-Cache-Status	HIT
Cf-Ray	9adc80734cc3899f-DEL
Content-Encoding	br
Content-Type	text/css
Date	Sun, 14 Dec 2025 08:58:50 GMT
Etag	W/"c6f9b368aed85c17723577323826544c"
Last-Modified	Tue, 30 Sep 2025 07:15:39 GMT
Priority	u=0,i=?0
Server	cloudflare
Server-Timing	cfExtPri
Vary	Accept-Encoding

Using SSl labs



You are here: Home > Projects > SSL Server Test > skillhorizon.com

SSL Report: skillhorizon.com (52.20.84.62)

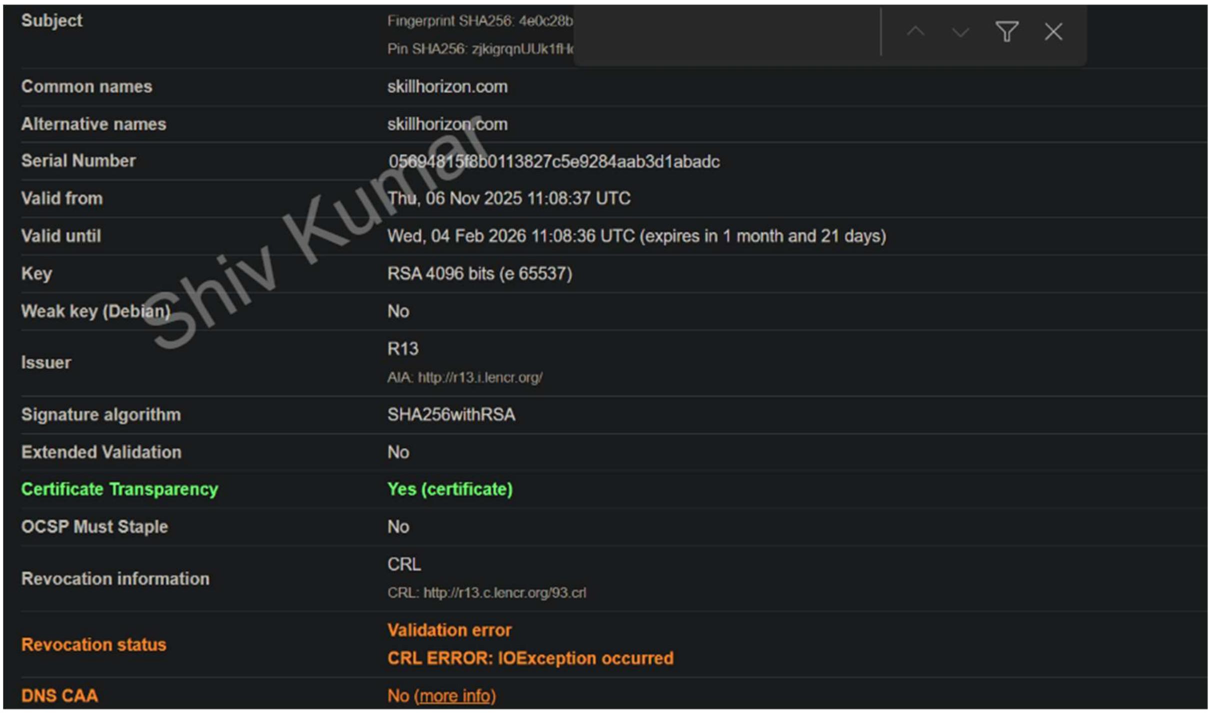
Assessed on: Sun, 14 Dec 2025 09:23:55 UTC | Hide | Clear cache

Summary

Overall Rating

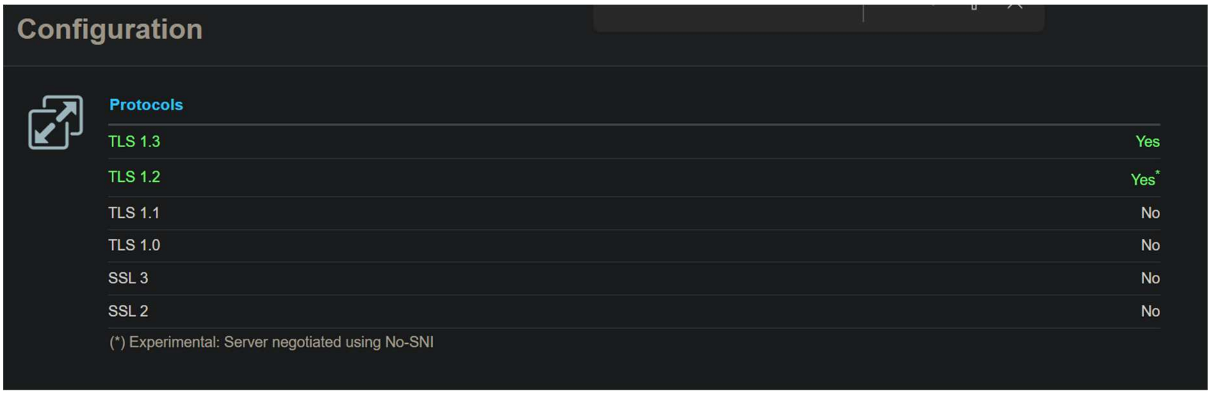
A

Certificate: - A Grade



Subject	Fingerprint SHA256: 4e0c28b Pin SHA256: zjkigrqnUUk1fH
Common names	skillhorizon.com
Alternative names	skillhorizon.com
Serial Number	05694815f8b0113827c5e9284aab3d1abadc
Valid from	Thu, 06 Nov 2025 11:08:37 UTC
Valid until	Wed, 04 Feb 2026 11:08:36 UTC (expires in 1 month and 21 days)
Key	RSA 4096 bits (e 65537)
Weak key (Debian)	No
Issuer	R13 AIA: http://r13.i.lencr.org/
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	CRL CRL: http://r13.c.lencr.org/93.crl
Revocation status	Validation error CRL ERROR: IOException occurred
DNS CAA	No (more info)

Certification is Still valid and valid till 4 Feb 2026



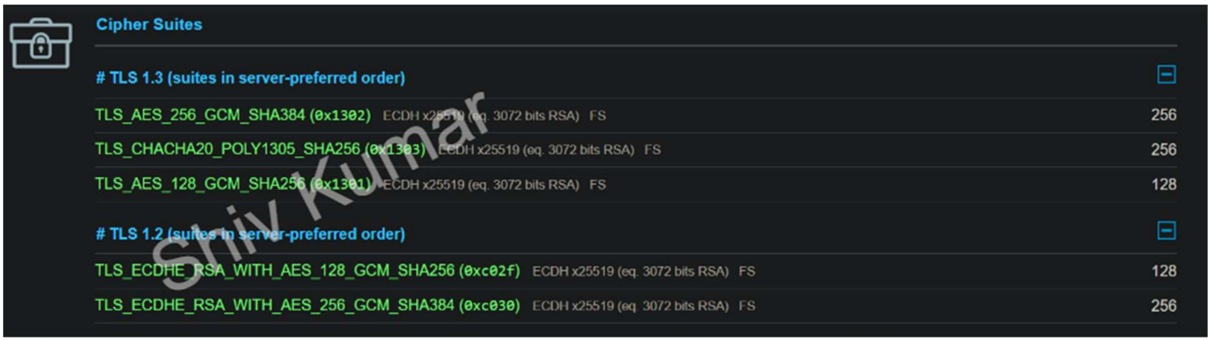
Configuration

Protocols	
TLS 1.3	Yes
TLS 1.2	Yes*
TLS 1.1	No
TLS 1.0	No
SSL 3	No
SSL 2	No

(*) Experimental: Server negotiated using No-SNI

TSL and SSl Certificates used

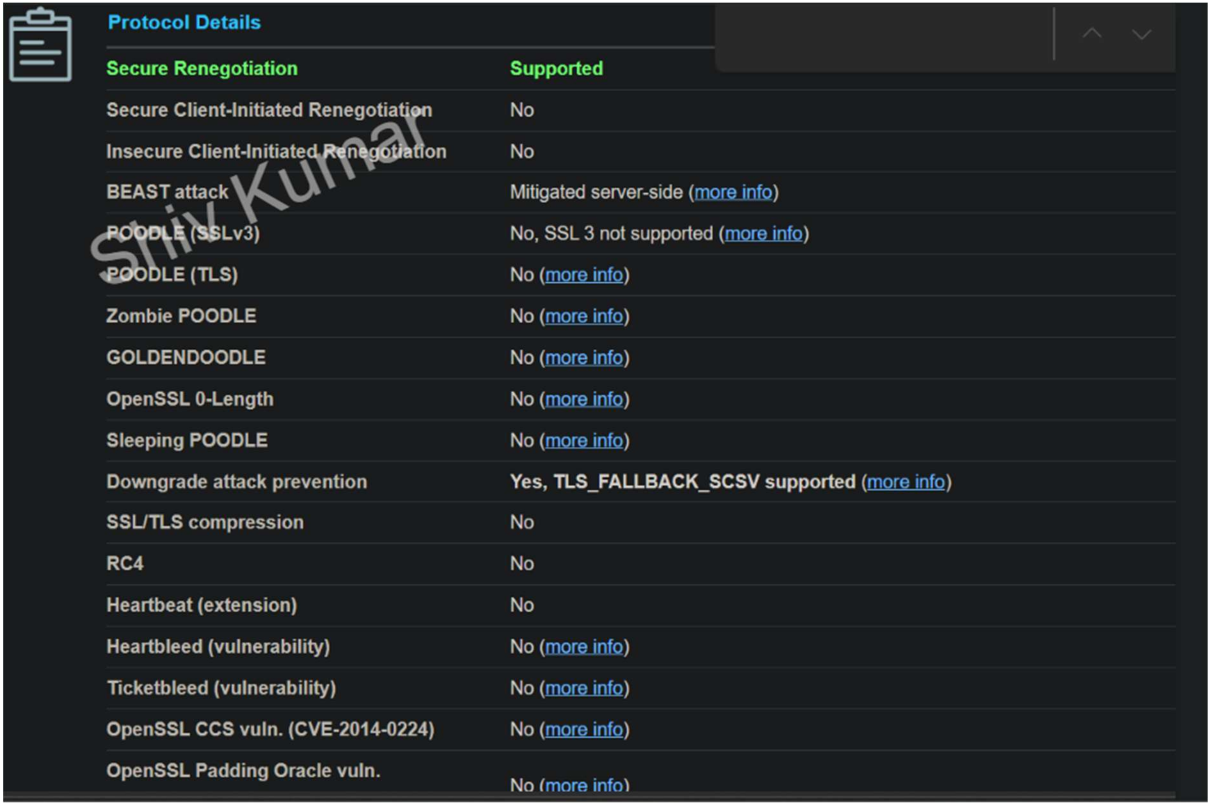
Cipher Suites Used are secure and safe no weak suites present



Cipher Suites

# TLS 1.3 (suites in server-preferred order)		
TLS_AES_256_GCM_SHA384 (0x1302)	ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_CHACHA20_POLY1305_SHA256 (0x1303)	ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_AES_128_GCM_SHA256 (0x1301)	ECDH x25519 (eq. 3072 bits RSA) FS	128

# TLS 1.2 (suites in server-preferred order)		
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH x25519 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	ECDH x25519 (eq. 3072 bits RSA) FS	256

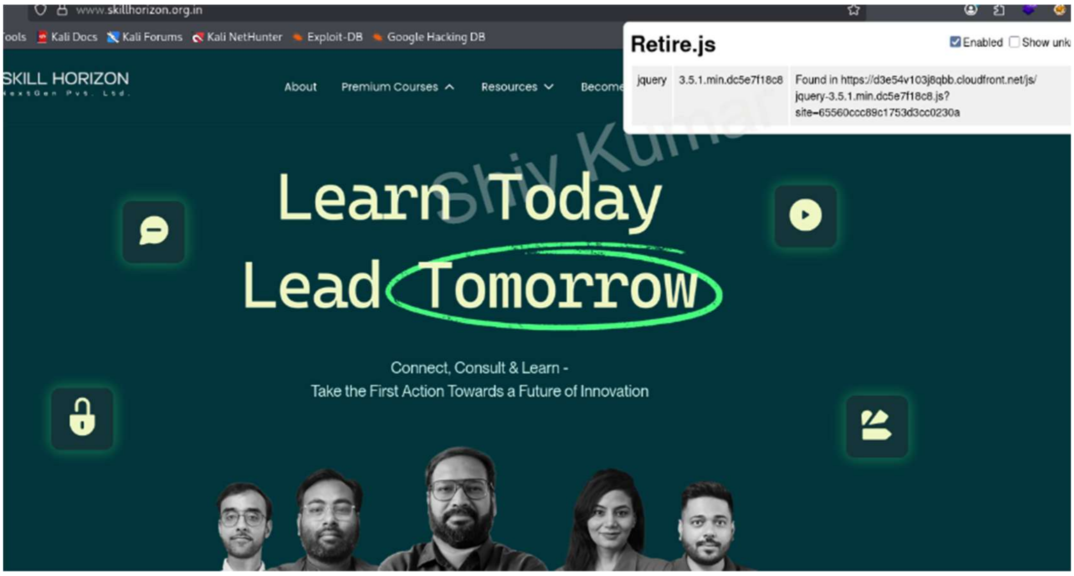


Protocol Details

Secure Renegotiation	Supported
Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No
BEAST attack	Mitigated server-side (more info)
POODLE (SSLv3)	No, SSL 3 not supported (more info)
POODLE (TLS)	No (more info)
Zombie POODLE	No (more info)
GOLDENDOODLE	No (more info)
OpenSSL 0-Length	No (more info)
Sleeping POODLE	No (more info)
Downgrade attack prevention	Yes, TLS_FALLBACK_SCSV supported (more info)
SSL/TLS compression	No
RC4	No
Heartbeat (extension)	No
Heartbleed (vulnerability)	No (more info)
Ticketbleed (vulnerability)	No (more info)
OpenSSL CCS vuln. (CVE-2014-0224)	No (more info)
OpenSSL Padding Oracle vuln.	No (more info)

3. **Outdated Js lib (Retire.js add-on)**

Identification of outdated libraries



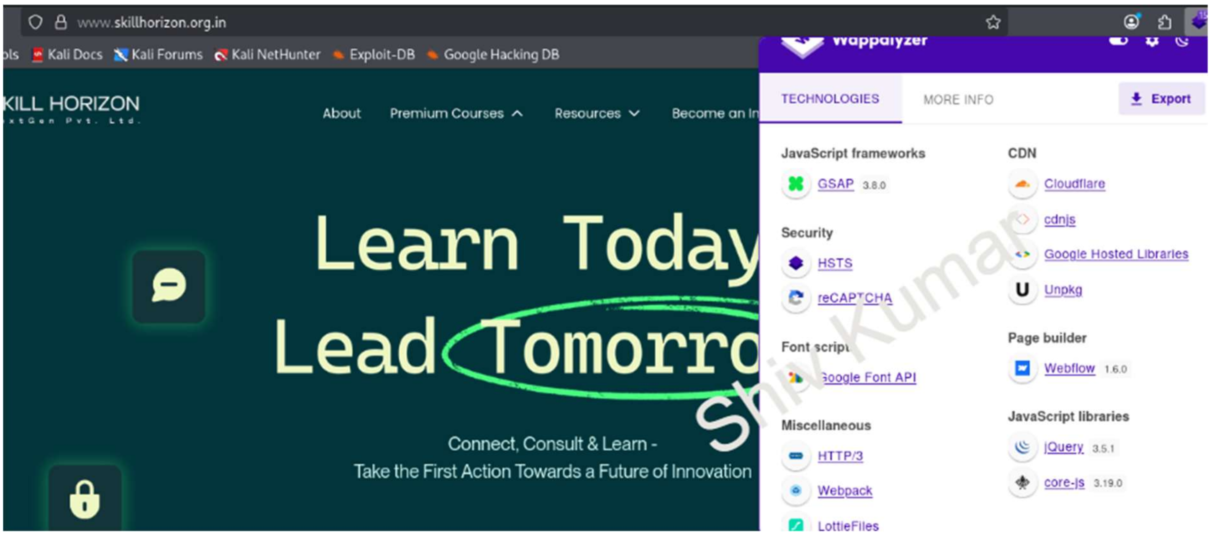
Retire.js ☑ Enabled □ Show unk

jquery	3.5.1.min.dc5e7f18c8	Found in https://d3e54v103j8qbb.cloudfront.net/js/jquery-3.5.1.min.dc5e7f18c8.js?site=65560ccc89c1753d3cc0230a

4. **Version Disclosure**

Jquery version disclosed

No apache server disclosed



JavaScript frameworks
GSAP 3.8.0

Security
HSTS
reCAPTCHA

Font script
Google Font API

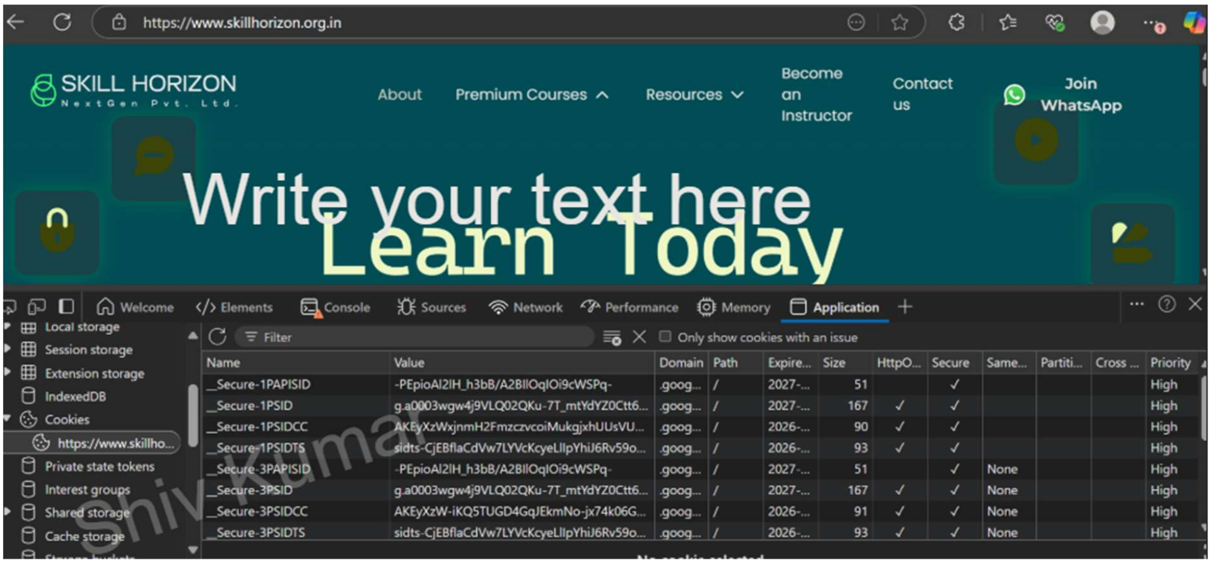
Miscellaneous
HTTP/3
Webpack
LottieFiles

CDN
Cloudflare
cdnjs
Google Hosted Libraries
Unpkg

Page builder
Webflow 1.6.0

JavaScript libraries
jQuery 3.5.1
core-js 3.19.0

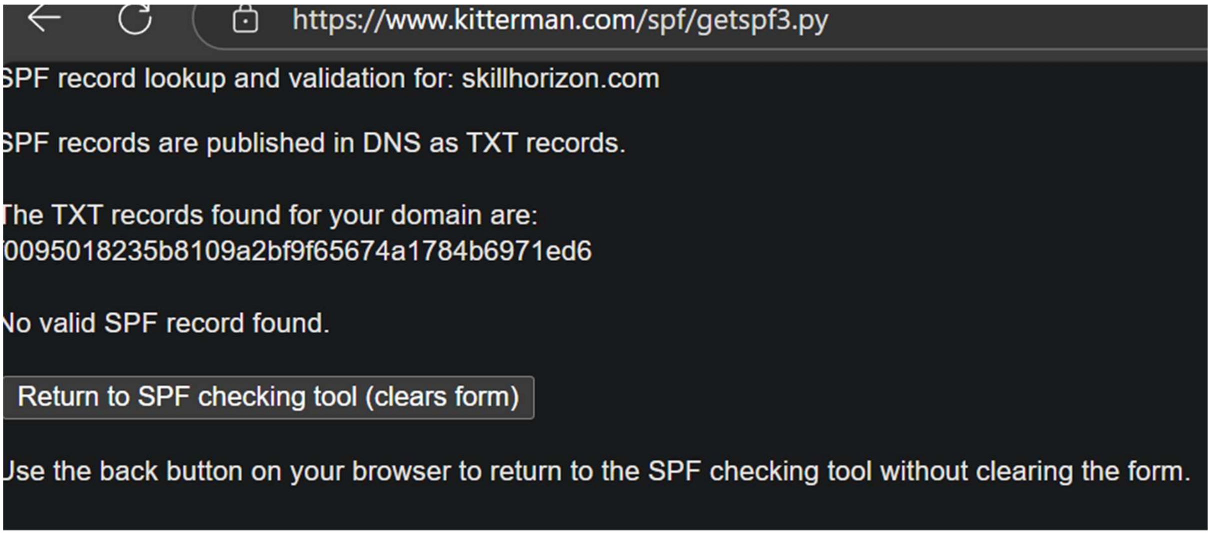
5. **Cookies Httponly** , secure



Name	Value	Domain	Path	Expire...	Size	HttpO...	Secure	Same...	Partiti...	Cross ...	Priority
__Secure-1PAPISID	-PEpioAl2IH_h3bB/A2BllOqlOi9cWSPq-	.goog...	/	2027-...	51		✓				High
__Secure-1PSID	g.a0003wgw4j9VLQ02QKu-7T_mtYdYZ0Ctt6...	.goog...	/	2027-...	167	✓	✓				High
__Secure-1PSIDCC	AKEyXzWxjnmH2FmzczvcoiMukgjxhUUsVU...	.goog...	/	2026-...	90	✓	✓				High
__Secure-1PSIDTS	sidts-CjEBflaCdVw7LYVcKcyeLllpYhiJ6Rv59o...	.goog...	/	2026-...	93	✓	✓				High
__Secure-3PAPISID	-PEpioAl2IH_h3bB/A2BllOqlOi9cWSPq-	.goog...	/	2027-...	51		✓	None			High
__Secure-3PSID	g.a0003wgw4j9VLQ02QKu-7T_mtYdYZ0Ctt6...	.goog...	/	2027-...	167	✓	✓	None			High
__Secure-3PSIDCC	AKEyXzW-iKQ5TUGD4GqJEkmNo-jx74k06G...	.goog...	/	2026-...	91	✓	✓	None			High
__Secure-3PSIDTS	sidts-CjEBflaCdVw7LYVcKcyeLllpYhiJ6Rv59o...	.goog...	/	2026-...	93	✓	✓	None			High

6. **SPF or Dmarc record**

No spf record present



SPF record lookup and validation for: skillhorizon.com

SPF records are published in DNS as TXT records.

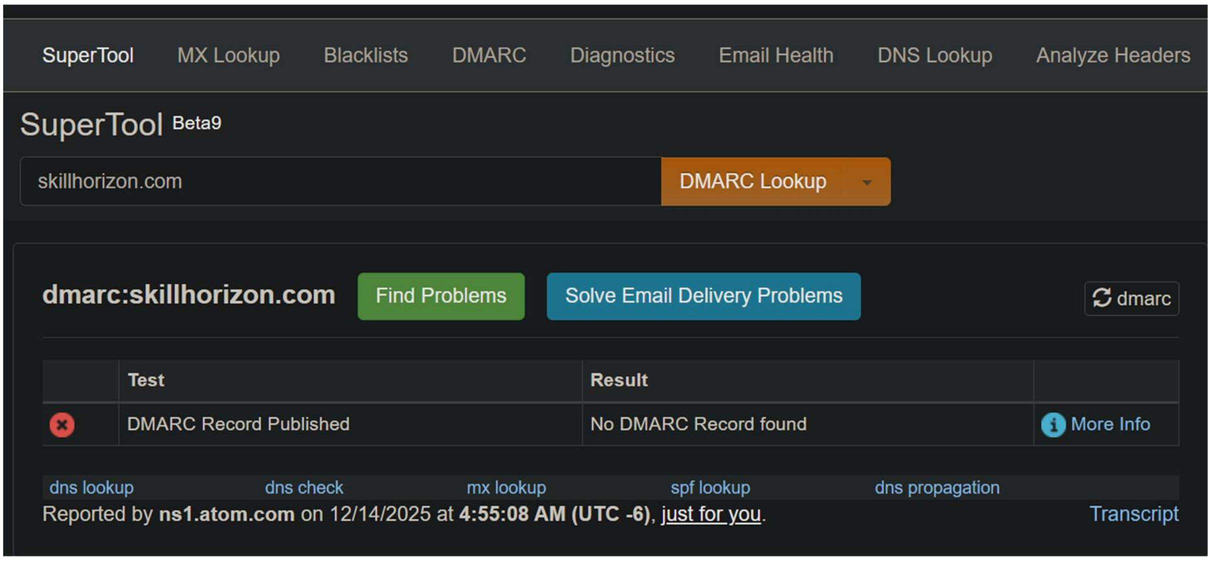
The TXT records found for your domain are:
0095018235b8109a2bf9f65674a1784b6971ed6

No valid SPF record found.

Return to SPF checking tool (clears form)

Use the back button on your browser to return to the SPF checking tool without clearing the form.

No Dmarc record exist



skillhorizon.com

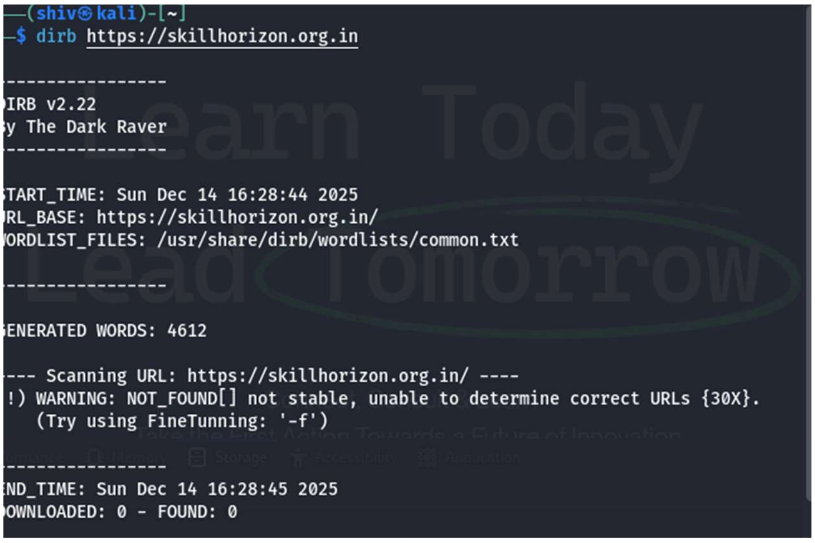
dmarc:skillhorizon.com

	Test	Result	
✗	DMARC Record Published	No DMARC Record found	More Info

Reported by **ns1.atom.com** on 12/14/2025 at **4:55:08 AM (UTC -6)**, just for you.

7. If any sensitive dir/file is leaked Dirb / dirsearch Leakix.net dotgit (add-on) .env .svn

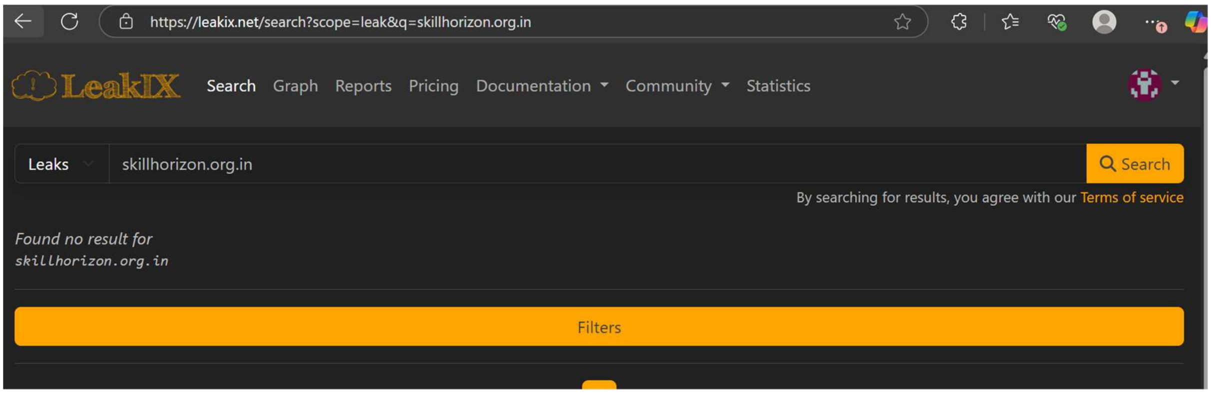
Using Dirb



```
──(shiv㉿kali)-[~]
─$ dirb https://skillhorizon.org.in

----------------
IRB v2.22
y The Dark Raver
----------------

TART_TIME: Sun Dec 14 16:28:44 2025
RL_BASE: https://skillhorizon.org.in/
ORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

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

ENERATED WORDS: 4612

--- Scanning URL: https://skillhorizon.org.in/ ----
!) WARNING: NOT_FOUND[] not stable, unable to determine correct URLs {30X}.
  (Try using FineTunning: '-f')

----------------
ND_TIME: Sun Dec 14 16:28:45 2025
OWNLOADED: 0 - FOUND: 0
```

Using LeakIX ,

No record exist when try using leakIX



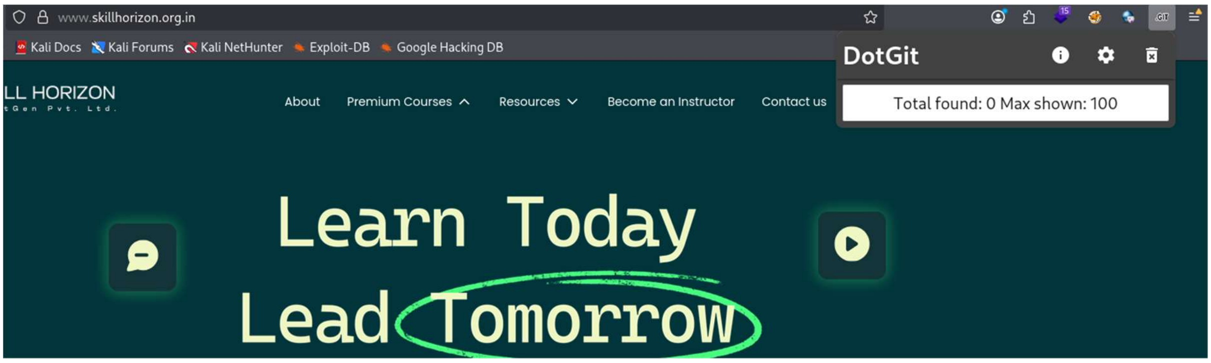
https://leakix.net/search?scope=leak&q=skillhorizon.org.in

skillhorizon.org.in

By searching for results, you agree with our Terms of service

Found no result for
skillhorizon.org.in

Using Dotgit

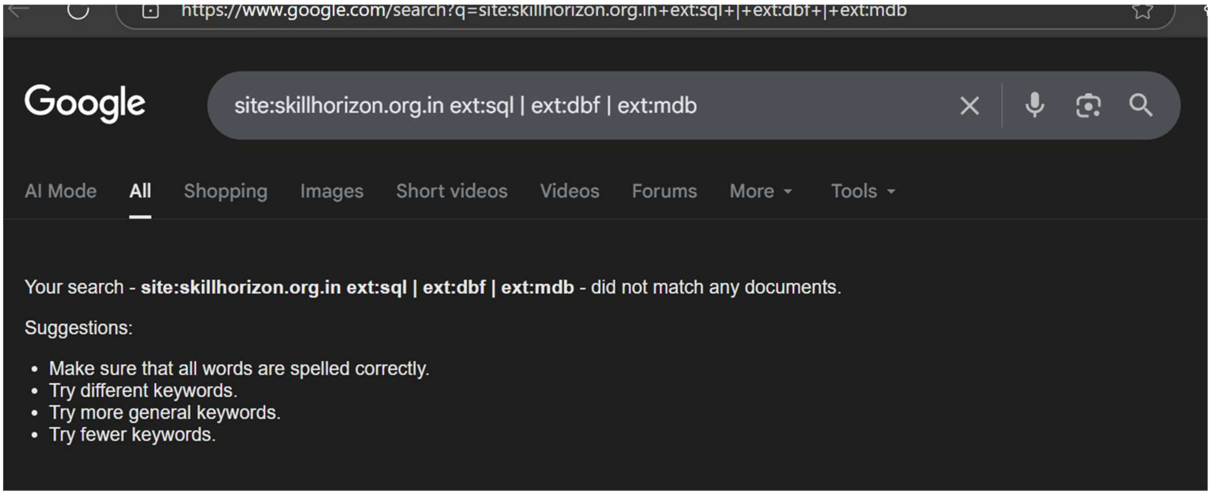


DotGit

Total found: 0 Max shown: 100

8. **Google Dorking** Site:target.com DORK Exploit-db.co

Using Dorking to find files



https://www.google.com/search?q=site:skillhorizon.org.in+ext:sql+|+ext:dbf+|+ext:mdb

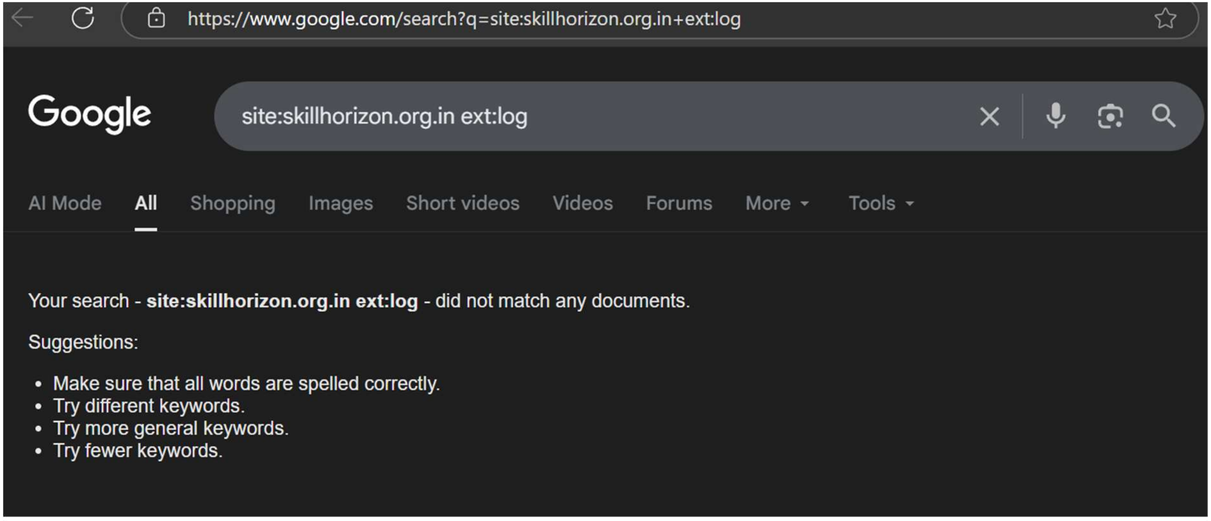
Google

site:skillhorizon.org.in ext:sql | ext:dbf | ext:mdb

Your search - **site:skillhorizon.org.in ext:sql | ext:dbf | ext:mdb** - did not match any documents.

Suggestions:

- Make sure that all words are spelled correctly.
- Try different keywords.
- Try more general keywords.
- Try fewer keywords.



https://www.google.com/search?q=site:skillhorizon.org.in+ext:log

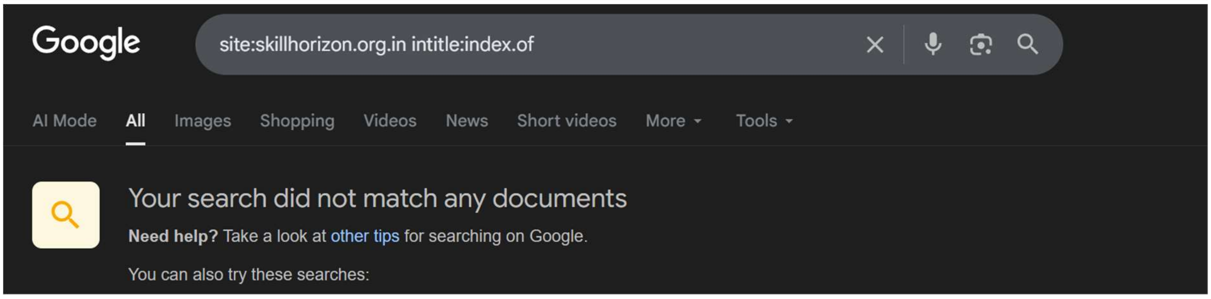
Google

site:skillhorizon.org.in ext:log

Your search - **site:skillhorizon.org.in ext:log** - did not match any documents.

Suggestions:

- Make sure that all words are spelled correctly.
- Try different keywords.
- Try more general keywords.
- Try fewer keywords.



Google

site:skillhorizon.org.in intitle:index.of

Your search did not match any documents

Need help? Take a look at other tips for searching on Google.

You can also try these searches: