

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

The screenshot shows a security report summary for the website <https://www.skillhorizon.org.in/index.html>. The report is graded 'B'. Key findings include:

- 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.

In the 'Missing Headers' section, three items are listed:

- X-Content-Type-Options**: Described as stopping a browser from trying to MIME-sniff the content type and forcing it to stick with the declared content-type. The only valid value for this header is "X-Content-Type-Options: nosniff".
- Referrer-Policy**: Described as 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**: Described as a new header that allows a site to control which features and APIs can be used in the browser.

2. **SSL Cert Testing Sslabs.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

The screenshot shows the Network tab in the Chrome DevTools developer tools. The page content is "Learn Today Lead Tomorrow" with a subtitle "Connect, Consult & Learn - Take the First Action Towards a Future of Innovation". The Network tab displays network requests and their headers. The 'Cache-Control' header is present in many responses, such as "public, max-age=31536000, immutable" for a script file. Other headers visible include "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,j=70", "Server: cloudflare", "Server-Timing: cfExtPri", and "Vary: Accept-Encoding". The timeline shows various requests taking between 500ms and 6000ms.

Using SSL labs

Qualys. SSL Labs | ^ v ⌂ X Free Trial Contact

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](#)

[Scan Another »](#)

Summary

Overall Rating: **A**

Certificate: 98
Protocol Support: 98
Key Exchange: 90
Cipher Strength: 90

Category	Score
Certificate	98
Protocol Support	98
Key Exchange	90
Cipher Strength	90

Certificate: - A Grade

Subject	Fingerprint SHA256: 4e0c28b Pin SHA256: zjkgrqnUJk1fhk
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.c.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

Protocol	Status
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 SSI 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

The screenshot shows a web browser window with the URL www.skillhorizon.org.in. The page content includes the Skill Horizon logo and the tagline "Learn Today Lead Tomorrow". A Retire.js tooltip is displayed over a piece of code, indicating that the jQuery library version 3.5.1.min.dc5e7f18c8 is outdated and found at <https://d3e54v103jbqbb.cloudfront.net/js/jquery-3.5.1.min.dc5e7f18c8.js?site-65560ccc89c1753d3cc0230a>. The tooltip also has checkboxes for "Enabled" and "Show url".

4. Version Disclosure

Jquery version disclosed

No apache server disclosed

The screenshot shows the Wappalyzer extension in a browser. The page content features a dark teal background with white text: "Learn Today Lead Tomorrow". Below it says "Connect, Consult & Learn - Take the First Action Towards a Future of Innovation". A padlock icon indicates the site is secure. The Wappalyzer sidebar lists various technologies used on the site.

Technology	Description
GSAP 3.8.0	JavaScript framework
Cloudflare	CDN
cdnjs	Content delivery network
Google Hosted Libraries	JavaScript library
Unpkg	Content delivery network
Webflow 1.6.0	Page builder
iQuery 3.5.1	JavaScript library
core.js 3.19.0	JavaScript library
LottieFiles	Font script

5. Cookies Httponly , secure

The screenshot shows the browser's developer tools Network tab. It lists several cookies for the domain https://www.skillhorizon.org.in. The table includes columns for Name, Value, Domain, Path, Expires, Size, HttpOnly, Secure, SameSite, Partition, CrossSite, and Priority.

Name	Value	Domain	Path	Expires	Size	HttpOnly	Secure	SameSite	Partition	CrossSite	Priority
_Secure-1PAPISID	-PEpiaoAI2lH_h3bB/A2BII0qjOj9cWSPg-	.goog...	/	2027...	51	✓	✓				High
Secure-1PSID	g.a0003wgw4j9VLQ02QKu-7T_mtYdYZ0Ctt6...	.goog...	/	2027...	167	✓	✓				High
_Secure-1PSIDCC	AKEyXzWxjnnh12fmczcvcoiMukgjxhUUsVU...	.goog...	/	2026...	90	✓	✓				High
Secure-1PSIDTS	sids-CjEBflaCdVw7LYVcKcyeUlpYhi6Rv59o...	.goog...	/	2026...	93	✓	✓				High
_Secure-3PAPISID	-PEpiaoAI2lH_h3bB/A2BII0qjOj9cWSPg-	.goog...	/	2027...	51	✓	✓	None			High
Secure-3PSID	g.a0003wgw4j9VLQ02QKu-7T_mtYdYZ0Ctt6...	.goog...	/	2027...	167	✓	✓	None			High
_Secure-3PSIDCC	AKEyXzW-iKQSTUGd4GqjEkMnNo-jx74k6G...	.goog...	/	2026...	91	✓	✓	None			High
Secure-3PSIDTS	sids-CjEBflaCdVw7LYVcKcyeUlpYhi6Rv59o...	.goog...	/	2026...	93	✓	✓	None			High

6. SPF or Dmrc record

No SPF record present

The screenshot shows the SPF record lookup tool at <https://www.kitterman.com/spf/getspf3.py>. It displays the SPF record lookup and validation for the domain skillhorizon.com. The tool states that SPF records are published in DNS as TXT records. It lists the TXT records found for the domain:

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 Dmrc record exist

The screenshot shows the SuperTool interface with the title "SuperTool Beta9". At the top, there are tabs for SuperTool, MX Lookup, Blacklists, DMARC, Diagnostics, Email Health, DNS Lookup, and Analyze Headers. Below the tabs, a search bar contains "skillhorizon.com" and a dropdown menu is open, showing "DMARC Lookup". The main content area has a header "dmarc:skillhorizon.com" with buttons for "Find Problems" and "Solve Email Delivery Problems". A "dmarc" button is also present. Below this, a table shows a single row: "Test" (DMARC Record Published) and "Result" (No DMARC Record found). There are "More Info" and "Transcript" links. At the bottom, it says "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

[DIRB v2.22]
by The Dark Raver

[START_TIME: Sun Dec 14 16:28:44 2025]
[URL_BASE: https://skillhorizon.org.in/]
[WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt]

[GENERATED WORDS: 4612]

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

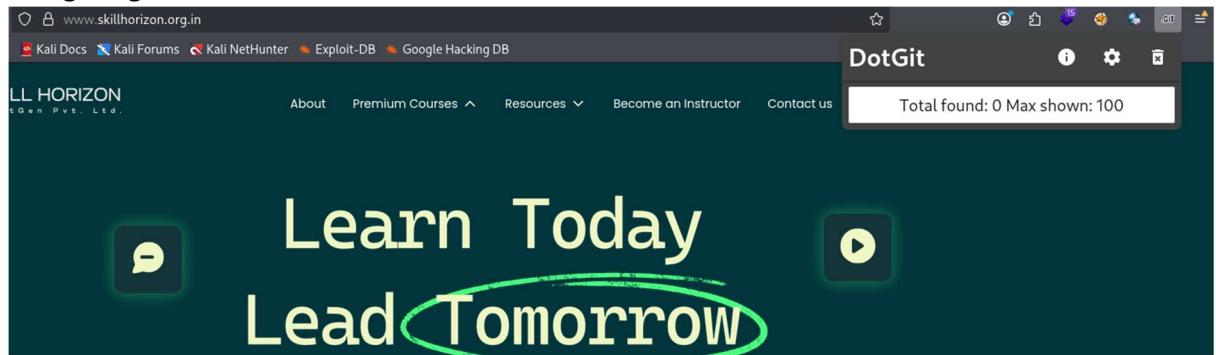
[END_TIME: Sun Dec 14 16:28:45 2025]
[DOWNLOADED: 0 - FOUND: 0]
```

Using LeakIX ,

No record exist when try using leakIX

The screenshot shows the LeakIX search results page. The URL in the address bar is "https://leakix.net/search?scope=leak&q=skillhorizon.org.in". The page features a navigation bar with links for Search, Graph, Reports, Pricing, Documentation, Community, and Statistics. Below the navigation is a search bar with "Leaks" selected and "skillhorizon.org.in" entered. A "Search" button is to the right. A message below the search bar states "By searching for results, you agree with our Terms of service". The main content area displays the message "Found no result for skillhorizon.org.in". At the bottom, there is a yellow "Filters" button.

Using Dotgit



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

Using Dorking to find files

A screenshot of a Google search results page. The search query is 'site:skillhorizon.org.in ext:sql | ext:dbf | ext:mdb'. The results section is empty, displaying the message 'Your search - site:skillhorizon.org.in ext:sql | ext:dbf | ext:mdb - did not match any documents.' Below this, there are 'Suggestions:' and a bulleted list: '• Make sure that all words are spelled correctly.', '• Try different keywords.', '• Try more general keywords.', and '• Try fewer keywords.'

A screenshot of a Google search results page. The search query is 'site:skillhorizon.org.in ext:log'. The results section is empty, displaying the message 'Your search - site:skillhorizon.org.in ext:log - did not match any documents.' Below this, there are 'Suggestions:' and a bulleted list: '• Make sure that all words are spelled correctly.', '• Try different keywords.', '• Try more general keywords.', and '• Try fewer keywords.'

A screenshot of a Google search results page. The search query is 'site:skillhorizon.org.in intitle:index.of'. The results section is empty, displaying the message 'Your search did not match any documents'. Below this, there is a link 'Need help? Take a look at other tips for searching on Google.' and a section 'You can also try these searches:'.