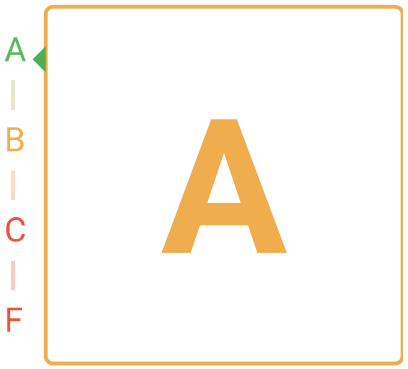
Summary of **www.gps.edu.in** [Desktop version] Website Security Test

Provided "as is" without any warranty of any kind.

www.gps.edu.in was tested **9** times during the last **12** months.

Your final score:



Date/Time:	Aug 24th, 2026 10:57 GMT+5:30
Server IP:	101.0.36.38
Reverse DNS:	-
Location:	India
Version:	for desktop

Test Results Summary for www.gps.edu.in

No third-party web software dependancies were identified. Show details.

Potential GDPR compliance issues were identified related to Privacy Policy, Cookie Disclaimer. The following checks were not performed, as no corresponding cookies with personal or tracking information seem to be sent by the website: Website Security. Show details.

The website is compliant with PCI DSS Requirement 6.3, while being non-compliant with Requirement 6.4. Show details.

All key security headers are missing. Optional HTTP headers appear to be properly configured: Server, Cache-Control. Show details.

Content-Security-Policy headers are not present. Show details.

2 cookies detected; gokuldas_public_school_khargone_session, XSRF-TOKEN have security or privacy-related configuration issues. Show details.

One external request detected; the request completed successfully. SRI is not used for one third-party JavaScript or CSS file. Show details.

No significant anti-scraping protections were detected. Show details.

DNS CNAME record detected; DNSSEC signatures are not present. Show details.

Compliance Summary for www.gps.edu.in

GDPR Compliance Failed: Potential GDPR compliance issues were identified related to Privacy Policy, Cookie Disclaimer. The following checks were not performed, as no corresponding cookies with personal or tracking information seem to be sent by the website: Website Security.

PCI DSS Compliance Failed: The website is compliant with PCI DSS Requirement 6.3, while being non-compliant with Requirement 6.4.

Full Test - Table of Contents

Web Server Configuration Test

HTTP RESPONSE

200 OK

HTTP VERSIONS

HTTP/1.0 HTTP/1.1 HTTP/2 HTTP/3

NPN

N/A

ALPN

HTTP/1.1

CONTENT ENCODING

None

SERVER SIGNATURE

Apache

WAF

No WAF detected

LOCATION

Broadband Pacenet Pvt. Ltd

HTTP METHODS ENABLED

✓ GET ✓ HEAD ✓ OPTIONS

Web Software Security Test

Fingerprinted Software & Vulnerabilities

No CMS were fingerprinted on the website.	Information

Fingerprinted Software Components & Vulnerabilities

No components were fingerprinted on the website.	Information

GDPR Compliance Test

If the website processes or stores personal data of the EU residents, the following requirements of EU GDPR may apply:

PRIVACY POLICY

Privacy Policy was not found on the website or is not easily accessible.	Misconfiguration or weakness

WEBSITE SECURITY

Website CMS and its components could not have been reliably fingerprinted. Ensure that they are up2date.	Information

TLS ENCRYPTION

HTTPS encryption is present on the web server.	Good configuration

COOKIE PROTECTION

Cookies with personal or tracking information are sent with Secure flag.	Good configuration

COOKIE DISCLAIMER

Third-party cookies or cookies with tracking information are sent, but no cookie disclaimer was found on the website.	Misconfiguration or weakness

PCI DSS Compliance Test

If the website falls into a CDE (Cardholder Data Environment) scope, the following Requirements of PCI DSS may apply:

REQUIREMENT 6.3

No publicly known vulnerabilities seem to be present in the fingerprinted versions of the website CMS and its components.	Good configuration

REQUIREMENT 6.4

No WAF was detected on the website. Implement a WAF to protect the website against common web attacks.	Misconfiguration or weakness

HTTP Headers Security Test

Some HTTP headers related to security and privacy are missing or misconfigured.	Misconfiguration or weakness

MISSING REQUIRED HTTP HEADERS

Strict-Transport-Security (HSTS) | X-Frame-Options | X-Content-Type-Options

MISSING OPTIONAL HTTP HEADERS

Access-Control-Allow-Origin | Permissions-Policy

SERVER

Web server does not disclose its version.	Good configuration

Raw HTTP Header

```
Server: Apache
```

CACHE-CONTROL

The header is properly set.	Good configuration

Raw HTTP Header

```
Cache-Control: no-cache, private
```

Content Security Policy (CSP) Test

CONTENT-SECURITY-POLICY (CSP)

The header was not sent by the server.	Misconfiguration or weakness

CONTENT-SECURITY-POLICY-REPORT-ONLY

The header was not sent by the server.	Information

Cookies Privacy and Security Test

Some cookies have missing secure flags or attributes.	Misconfiguration or weakness

COOKIE: GOKULDAS_PUBLIC_SCHOOL_KHARGONE_SESSION

The cookie has HttpOnly and SameSite attributes set.	Good configuration
The cookie is missing the Secure attribute. Make sure it does not store sensitive information.	Misconfiguration or weakness

Name	Value	Description
domain	www.gps.edu.in	Specifies which domains the browser should send the cookie to.
path	/	Specifies which paths on the domain the browser should send the cookie to.
secure	✗	Prevents browsers to send this cookie over an insecure connection.
httponly	✗	Prevents client-side scripts to access the cookie by telling browsers to only transmit the cookie over HTTP(S).
samesite	Lax	Prevents CSRF attacks by not sending the cookies when the request comes from another website.
expires	Mon, 24-Aug-2026 07:22:37 GMT	Specifies the expiration date of the cookie.

COOKIE: XSRF-TOKEN

The cookie has SameSite attribute set.	Good configuration
The cookie is missing the Secure and HttpOnly attributes. Make sure it does not store sensitive information.	Misconfiguration or weakness

Name	Value	Description
domain	www.gps.edu.in	Specifies which domains the browser should send the cookie to.
path	/	Specifies which paths on the domain the browser should send the cookie to.

Name	Value	Description
secure	✗	Prevents browsers to send this cookie over an insecure connection.
httponly	✗	Prevents client-side scripts to access the cookie by telling browsers to only transmit the cookie over HTTP(S).
samesite	Lax	Prevents CSRF attacks by not sending the cookies when the request comes from another website.
expires	Mon, 24-Aug-2026 07:22:37 GMT	Specifies the expiration date of the cookie.

External Content Security Test

SUBRESOURCE INTEGRITY

Subresource Integrity (SRI) is a security feature that allows browsers to verify that fetched resources (scripts and stylesheets) are delivered without unexpected alterations. The integrity of third-party resources is ensured by validating their cryptographic hashes.

SRI is correctly implemented for 0 out of 1 third-party JavaScripts and CSS files. Ensure that SRI is applied to all external JavaScripts and CSS files for complete security.	Information

EXTERNAL CONTENT

External web content (e.g. images, video, CSS or JavaScript) can improve website loading time. However, the external content can also put privacy of website visitors at risk given that some information about them is transmitted to the third parties operating the external resources, sometimes even without proper HTTPS encryption or user consent.

External HTTP Requests	Failed HTTP Requests
1	0

cdn.jsdelivr.net

https://cdn.jsdelivr.net/npm/bootstrap@5.3.2/dist/css/bootstrap.min.css SRI

Protection from Data Scraping Test

Many companies rely on AI bots to scrape website content, using the collected data to train their machine learning models. To safeguard information, website owners can apply different techniques to detect, limit, or block scraping activities carried out by these bots.

Robots.txt Rules	User-Agent Blocks	Meta Tags	Protection vs. Bots
0	0	0	0

Default Rules

The website has the following default access rules for all crawlers defined in robots.txt, unless overridden by more specific rules below.

`User-agent: *` `Disallow:`	Raw Value

GPTBot by OpenAI

Robots.txt Directives

No specific rule for GPTBot User-Agent(s) was found in robots.txt; default rules apply.	Information

Server-side Blocking

No server-side User-Agent-based blocking detected for GPTBot.	Information

SHOW 10 MORE

DNSSEC Configuration Test

DNSSEC (Domain Name System Security Extensions) is a security protocol that protects against DNS spoofing by ensuring the authenticity and integrity of DNS data.

Domain **www.gps.edu.in** has 1 unsigned DNS record of CNAME type:

Type	Domain name	Canonical Name
CNAME	www.gps.edu.in	gps.edu.in.

Share this report: