Summary of gps.edu.in:443 (HTTPS) SSL Security Test

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

gps.edu.in was tested 1 time during the last 12 months.

Your final score:

A
B
C
F

A+

Date/Time: Jul 10th, 2024 16:19:54 GMT+5:30
Source IP/Port: 103.74.54.30:443
Type: HTTPS

PCI DSS Compliance Test	HIPAA Compliance Test	NIST Compliance Test	Industry Best Practices
COMPLIANT	COMPLIANT	COMPLIANT	NO MAJOR ISSUES FOUND

External Content Security: NOT FOUND

The server supports the most recent and secure TLS protocol version of TLS 1.3.	Good configuration

Meet Regulatory and Compliance Requirements

Looking for a comprehensive security audit and compliance-ready report? You are at the right place.


Attack Surface Management


Web Security Scanning


Cybersecurity Compliance


Trusted by 1,000+ customers from over 50 countries


50+ international awards and industry recognitions

FREE DEMO

Because prevention is better

Discovered Subdomains

Hostname	Protocol/Port	Certificate(s)	Tested on	Compliances	Grade
gps.edu.in:25	SMTP / 25	The RSA certificate is valid till Oct 6th 2024	Not tested yet	–	–
gps.edu.in:110	POP3 / 110	The RSA certificate is valid till Oct 6th 2024	Not tested yet	–	–
gps.edu.in:143	IMAP / 143	The RSA certificate is valid till Oct 6th 2024	Not tested yet	–	–
gps.edu.in	HTTPS / 443	The RSA certificate is valid till Oct 6th 2024	Jul 10th, 2024 16:19:54 GMT+5:30	PCI DSS HIPAA NIST	A+

SHOW 84 MORE

SSL Certificate Analysis

RSA CERTIFICATE INFORMATION

Issuer	R11
Trusted	Yes
Common Name	gps.edu.in
Key Type/Size	RSA 2048 bits
Serial Number	0x03F8C18BAA9205B0133CB86DAE28503DC64F
Signature Algorithm	sha256WithRSAEncryption
Subject Alternative Names	DNS:gps.edu.in, DNS:mail.gps.edu.in, DNS:www.gps.edu.in
Transparency	Yes
Validation Level	DV
CRL	No
OCSP	http://r11.o.lencr.org
OCSP Must-Staple	No
Supports OCSP Stapling	Yes
Valid From	July 08, 2024 10:31 CET
Valid To	October 06, 2024 10:31 CET

CERTIFICATE CHAIN

Root CA	ISRG Root X1
Type/Size	RSA 4096 bits
Serial Number	0x8210CFB0D240E3594463E0BB63828B00
Signature	sha256WithRSAEncryption
SHA256	96bcec06264976f374... 8ffcee05c0bddf08c6
PIN	C5+lpZ7tcVwmwQIMcR... ABXhQzejna0wHFr8M=
Expires in	3,981 days
Comment	Self-signed

Intermediate CA	R11
Type/Size	RSA 2048 bits
Serial Number	0x8A7D3E13D62F30EF2386BD29076B34F8
Signature	sha256WithRSAEncryption
SHA256	591e9ce6c863d3a079... 95211361024ae31a44
PIN	bdrBhpj38ffhxpubzk... yossdhcBYj+Zx2fcc=
Expires in	976 days
Comment	-

Server certificate	gps.edu.in
Type/Size	RSA 2048 bits
Serial Number	0x03F8C18BAA9205B0133CB86DAE28503DC64F

Signature	sha256WithRSAEncryption
SHA256	1b5d274247027a4596... dfdd170f26a8e87de8
PIN	3kueE5v2UrrKyoGKGB... 2sJD7n+shYBz7cn7c=
Expires in	88 days
Comment	-

PCI DSS Compliance Test of gps.edu.in

Reference: PCI DSS 4.0, Requirement 4.2

CERTIFICATES ARE TRUSTED

All the certificates provided by the server are trusted. — Good configuration

SUPPORTED CIPHERS

List of all cipher suites supported by the server:

TLSV1.3

TLS_CHACHA20_POLY1305_SHA256	Good configuration
TLS_AES_256_GCM_SHA384	Good configuration
TLS_AES_128_GCM_SHA256	Good configuration

TLSV1.2

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	Good configuration
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	Good configuration

SUPPORTED PROTOCOLS

List of all SSL/TLS protocols supported by the server:

TLSv1.2	Good configuration
TLSv1.3	Good configuration

SUPPORTED ELLIPTIC CURVES

List of all elliptic curves supported by the server:

P-384 (secp384r1) (384 bits)	Good configuration
P-521 (secp521r1) (521 bits)	Good configuration
P-256 (prime256v1) (256 bits)	Good configuration
X25519 (253 bits)	Good configuration
X448 (448 bits)	Good configuration

POODLE OVER TLS

The server is not vulnerable to POODLE over TLS. — Not vulnerable

GOLDENDOODLE

The server is not vulnerable to GOLDENDOODLE. — Not vulnerable

ZOMBIE POODLE

The server is not vulnerable to Zombie POODLE. Not vulnerable

SLEEPING POODLE

The server is not vulnerable to Sleeping POODLE. Not vulnerable

0-LENGTH OPENSSL

The server is not vulnerable 0-Length OpenSSL. Not vulnerable

CVE-2016-2107

The server is not vulnerable to CVE-2016-2107. Not vulnerable

SERVER DOES NOT SUPPORT CLIENT-INITIATED INSECURE RENEGOTIATION

The server does not support client-initiated insecure renegotiation. Good configuration

ROBOT

The server is not vulnerable to ROBOT vulnerability. Not vulnerable

HEARTBLEED

The server version of OpenSSL is not vulnerable to Heartbleed attack. Not vulnerable

CVE-2014-0224

The server is not vulnerable to CCS Injection. Not vulnerable

CVE-2021-3449

The server is not vulnerable to CVE-2021-3449 (OpenSSL Maliciously Crafted Renegotiation Vulnerability). Not vulnerable

HIPAA and NIST Compliance Test

Reference: HIPAA Security Rule (Ref. NIST SP 800-52: "Guidelines for the Selection and Use of TLS Implementations")

X.509 CERTIFICATES ARE IN VERSION 3

All the X509 certificates provided by the server are in version 3. — Good configuration

SERVER SUPPORTS OCSP STAPLING

The server supports OCSP stapling, which allows better verification of the certificate validation status. — Good configuration

SUPPORTED CIPHERS

List of all cipher suites supported by the server:

TLSV1.3

TLS_CHACHA20_POLY1305_SHA256	Good configuration
TLS_AES_256_GCM_SHA384	Good configuration
TLS_AES_128_GCM_SHA256	Good configuration

TLSV1.2

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	Good configuration
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	Good configuration

SUPPORTED PROTOCOLS

List of all SSL/TLS protocols supported by the server:

TLSv1.2	Good configuration
TLSv1.3	Good configuration

SUPPORTED ELLIPTIC CURVES

List of all elliptic curves supported by the server:

P-384 (secp384r1) (384 bits)	Good configuration
P-521 (secp521r1) (521 bits)	Good configuration
P-256 (prime256v1) (256 bits)	Good configuration
X25519 (253 bits)	Good configuration
X448 (448 bits)	Good configuration

EC_POINT_FORMAT EXTENSION

The server supports the EC_POINT_FORMAT TLS extension.

Good configuration

Industry Best Practices Test of gps.edu.in

DNSCAA

This domain does not have a Certification Authority Authorization (CAA) record. **Information**

CERTIFICATES HAVE A VALIDITY PERIOD OF 398 DAYS OR LESS

All the server certificates provided have been validated for less than 398 days (13 months). Good configuration

CERTIFICATES DO NOT PROVIDE EV

The RSA certificate provided is NOT an Extended Validation (EV) certificate. **Information**

TLS 1.3 SUPPORTED

The server supports TLS 1.3 which is the only version of TLS that currently has no known flaws or exploitable weaknesses. Good configuration

TLS 1.3 EARLY DATA (0-RTT)

Server's TLS 1.3 Early Data (RFC 8446, page 17) is not enabled. **Information**

SERVER DOES NOT HAVE CIPHER PREFERENCE

The server does not prefer cipher suites. We advise to enable this feature in order to enforce usage of the best cipher suites selected. Misconfiguration or weakness

SERVER PREFERRED CIPHER SUITES

Preferred cipher suite for each protocol supported (except SSLv2). Expected configuration are ciphers allowed by PCI DSS and enabling PFS.

HTTP SITE DOES NOT REDIRECT

The HTTP version of the website does not redirect to the HTTPS version. We advise to enable redirection. Misconfiguration or weakness

SERVER DOES NOT PROVIDE HSTS

The server does not enforce HTTP Strict Transport Security. We advise to enable it to enforce the user to browse the website in HTTPS. Misconfiguration or weakness

HSTS PRELOAD

This domain does not support HSTS Preload, which means it may not enforce HTTPS connections strictly and could be more vulnerable to security threats like protocol downgrade attacks. **Information**

TLS_FALLBACK_SCSV

The server supports TLS_FALLBACK_SCSV extension for protocol downgrade attack prevention.

Good configuration

SERVER DOES NOT SUPPORT CLIENT-INITIATED SECURE RENEGOTIATION

The server does not support client-initiated secure renegotiation.

Good configuration

SERVER-INITIATED SECURE RENEGOTIATION

The server supports secure server-initiated renegotiation.

Good configuration

SERVER DOES NOT SUPPORT TLS COMPRESSION

TLS compression is not supported by the server.

Good configuration

External Content Privacy and Security Analysis

No external content found on tested page.	Information

Meet Regulatory and Compliance Requirements

Looking for a comprehensive security audit and compliance-ready report? You are at the right place.

Attack Surface Management

Web Security Scanning

Cybersecurity Compliance

Trusted by 1,000+ customers from over 50 countries

50+ international awards and industry recognitions

FREE DEMO

Because prevention is better

Vedavati AB
Principal
GOKULDAS PUBLIC SCHOOL
KHARGONE (M.P.)

GOKULDAS PUBLIC SCHOOL * KHARGONE * CBSE AFFILIATION