Summary of www.justsomethoughts.fyi:443 (HTTPS) SSL Security Test

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

www.justsomethoughts.fyi was tested 5 times during the last 12 months.

Your final score:

A
B
C
F

A+

Date/Time: Dec 26th, 2024 22:21:35 GMT+0

Source IP/Port: 172.64.80.1:443

Type: HTTPS

PCI DSS Compliance Test	HIPAA Compliance Test	NIST Compliance Test	Industry Best Practices	External Content Security
COMPLIANT	COMPLIANT	COMPLIANT	NO ISSUES FOUND	NOT FOUND

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

Full Test Results: https://www.immuniweb.com/ssl/www.justsomethoughts.fyi/WbUJyiel/

SSL Certificate Analysis

RSA CERTIFICATE INFORMATION

Issuer	WR1
Trusted	Yes
Common Name	www.justsomethoughts.fyi
Key Type/Size	RSA 2048 bits
Serial Number	368538689205943255296242230962123849 10
Signature Algorithm	sha256WithRSAEncryption
Subject Alternative Names	DNS:www.justsomethoughts.fyi
Transparency	Yes
Validation Level	DV
CRL	http://c.pki.goog/wr1/LVOQywEuoSU.crl
OCSP	http://o.pki.goog/s/wr1/G7k
OCSP Must-Staple	No
Supports OCSP Stapling	Yes
Valid From	December 16, 2024 21:25 CET
Valid To	March 16, 2025 22:25 CET

ECDSA CERTIFICATE INFORMATION

Issuer	WE1
Trusted	Yes
Common Name	www.justsomethoughts.fyi
Key Type/Size	ECDSA 256 bits
Serial Number	0xE49DDFF94CDEA3CA0E842FB635B4D38D
Signature Algorithm	ecdsa-with-SHA256
Subject Alternative Names	DNS:www.justsomethoughts.fyi
Transparency	Yes
Validation Level	DV
CRL	http://c.pki.goog/we1/tVFs5tB-aco.crl
OCSP	http://o.pki.goog/s/we1/5J0
OCSP Must-Staple	No
Supports OCSP Stapling	Yes

Full Test Results: https://www.immuniweb.com/ssl/www.justsomethoughts.fyi/WbUJyiel/

Valid From	December 16, 2024 21:25 CET
Valid To	March 16, 2025 22:25 CET

CERTIFICATE CHAIN

Root CA	**GlobalSign Root CA**
Type/Size	RSA 2048 bits
Serial Number	48357032784597076690052 04
Signature	sha1WithRSAEncryption
SHA256	ebd41040e4bb3ec742… cef3c1df6cd4331c99
PIN	K87oWBWM9UZfyddvDf… yoUB2ptGtn0fv6G2Q=
Expires in	1,128 days
Comment	Self-signed

Intermediate CA	**GTS Root R1**
Type/Size	RSA 4096 bits
Serial Number	159159747900478145820483398898491642637
Signature	sha256WithRSAEncryption
SHA256	3ee0278df71fa3c125… 4c24efd769133918e5
PIN	hxqRlPTu1bMS/0DITB… u/8l8TjPgfaAp63Gc=
Expires in	1,127 days
Comment	-

Intermediate CA	**WR1**
Type/Size	RSA 2048 bits
Serial Number	169943283142817666033504407772870502567
Signature	sha256WithRSAEncryption
SHA256	b10b6f00e609509e87… cdc40c3a2a0d0d0e45
PIN	yDu9og255NN5GEf+Bw… 0EydZ0r1FCh9TdAW4=
Expires in	1,517 days
Comment	-

Server certificate	**www.justsomethoughts.fyi**
Type/Size	RSA 2048 bits
Serial Number	368538689205943255296242230962123849 10
Signature	sha256WithRSAEncryption
SHA256	0ac0081568dafd17b8… da25d723d042819a44
PIN	BEOwPWQl4z2+IshNmP… oNbhMI8LF5huOJeuE=
Expires in	80 days
Comment	-

Root CA	**GTS Root R1**
Type/Size	RSA 4096 bits
Serial Number	159662320309726417404178440727
Signature	sha384WithRSAEncryption
SHA256	947432abde7b7fa90f… a3c6887fff57a7f4cf
PIN	hxqRlPTu1bMS/0DITB… u/8l8TjPgfaAp63Gc=
Expires in	4,195 days
Comment	Self-signed

Intermediate CA	**GTS Root R4**
Type/Size	ECDSA 384 bits
Serial Number	170001980149335831901244157168837298715
Signature	sha256WithRSAEncryption
SHA256	76b27b80a58027dc3c… 2fadbe85012493b5a7
PIN	mEflZT5enoR1FuXLgY… vmf9c2bVBpiOjYQ0c=
Expires in	1,127 days
Comment	-

Intermediate CA	**WE1**
Type/Size	ECDSA 256 bits

Server certificate	**www.justsomethoughts.fyi**
Type/Size	ECDSA 256 bits

Full Test Results: https://www.immuniweb.com/ssl/www.justsomethoughts.fyi/WbUJyiel/

Serial Number	170074200136485300614847617070429275619
Signature	ecdsa-with-SHA384
SHA256	1dfc1605fbad358d8b… 857ffaf2864fbebf96
PIN	kIdp6NNEd8wsugYyyI… CED3hZbSR8ZFsa/A4=
Expires in	1,517 days
Comment	-

Serial Number	0xE49DDFF94CDEA3CA0E842FB635B4D38D
Signature	ecdsa-with-SHA256
SHA256	0d505d06b45342e1e1… bcbc938d21f38b3f99
PIN	gulRA4yTrDQwEhgojB… oxT6nbpHY46PxJXIk=
Expires in	80 days
Comment	-

Root CA	**GlobalSign**
Type/Size	ECDSA 256 bits
Serial Number	159662223612894884239637590694
Signature	ecdsa-with-SHA256
SHA256	b085d70b964f191a73… 0862138ab7325a24a2
PIN	CLOmM1/OXvSPjw5UOY… ImEp9hhku9W90fHMk=
Expires in	4,771 days
Comment	Self-signed

Intermediate CA	**WE1**
Type/Size	ECDSA 256 bits
Serial Number	170075456458877775515960875597933907487
Signature	ecdsa-with-SHA256
SHA256	a287ffab762cc69a26… a7e5cb88bb9b419cbb
PIN	kIdp6NNEd8wsugYyyI… CED3hZbSR8ZFsa/A4=
Expires in	1,517 days
Comment	-

Root CA	**GTS Root R4**
Type/Size	ECDSA 384 bits
Serial Number	159662532700760215368942768210
Signature	ecdsa-with-SHA384
SHA256	349dfa4058c5e26312… 93556cd5e8031b3c7d
PIN	mEflZT5enoR1FuXLgY… vmf9c2bVBpiOjYQ0c=
Expires in	4,195 days
Comment	Self-signed

PCI DSS Compliance Test

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_128_CBC_SHA	Good configuration
TLS_RSA_WITH_AES_128_GCM_SHA256	Good configuration
TLS_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	Good configuration
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_RSA_WITH_AES_256_GCM_SHA384	Good configuration
TLS_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	Good configuration

Full Test Results: https://www.immuniweb.com/ssl/www.justsomethoughts.fyi/WbUJyiel/

TLS_RSA_WITH_AES_128_CBC_SHA256	Good configuration
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	Good configuration
TLS_RSA_WITH_AES_256_CBC_SHA256	Good configuration
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	Good configuration
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	Good configuration
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	Good configuration
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_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-256 (prime256v1) (256 bits)	Good configuration
P-384 (secp384r1) (384 bits)	Good configuration
P-521 (secp521r1) (521 bits)	Good configuration
X25519 (253 bits)	Good configuration

POODLE OVER TLS

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

GOLDENDOODLE

Full Test Results: https://www.immuniweb.com/ssl/www.justsomethoughts.fyi/WbUJyiel/

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_128_CBC_SHA	Good configuration
TLS_RSA_WITH_AES_128_GCM_SHA256	Good configuration
TLS_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	Good configuration
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	Good configuration

Full Test Results: https://www.immuniweb.com/ssl/www.justsomethoughts.fyi/WbUJyiel/

TLS_RSA_WITH_AES_256_GCM_SHA384	Good configuration
TLS_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	Good configuration
TLS_RSA_WITH_AES_128_CBC_SHA256	Good configuration
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	Good configuration
TLS_RSA_WITH_AES_256_CBC_SHA256	Good configuration
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	Good configuration
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	Good configuration
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	Good configuration
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_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-256 (prime256v1) (256 bits)	Good configuration
P-384 (secp384r1) (384 bits)	Good configuration
P-521 (secp521r1) (521 bits)	Good configuration
X25519 (253 bits)	Good configuration

EC_POINT_FORMAT EXTENSION

Full Test Results: https://www.immuniweb.com/ssl/www.justsomethoughts.fyi/WbUJyiel/

The server supports the EC_POINT_FORMAT TLS extension.

Good configuration

Industry Best Practices Test

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 following certificates are NOT Extended Validation (EV) certificates: RSA, ECDSA. **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 HAS CIPHER PREFERENCE

The server enforces cipher suites preference. **Good configuration**

SERVER PREFERRED CIPHER SUITES

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

TLSv1.2 **TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256** **Good configuration**

Full Test Results: https://www.immuniweb.com/ssl/www.justsomethoughts.fyi/WbUJyiel/

SERVER PREFERS CIPHER SUITES PROVIDING PFS

For TLS family of protocols, the server prefers cipher suite(s) providing Perfect Forward Secrecy (PFS).

Good configuration

ALWAYS-ON SSL

The HTTP version of the website redirects to the HTTPS version.

Good configuration

SERVER PROVIDES HSTS WITH LONG DURATION

The server provides HTTP Strict Transport Security for more than 6 months: **15552000 seconds**

Good configuration

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

Full Test Results: https://www.immuniweb.com/ssl/www.justsomethoughts.fyi/WbUJyiel/

External Content Privacy and Security Analysis

No External Content appears to be loaded by the website.	Information

Need More? Upgrade to ImmuniWeb® AI Platform

Get remediation advice and ensure compliance with ImmuniWeb AI Platform:

The End of Report

Upgrade from Free Community Edition to ImmuniWeb® AI Platform