Qualys. SSL Labs

SSL Report: www.sweharris.org (2600:3c00:e000:126:0:0:0:1)

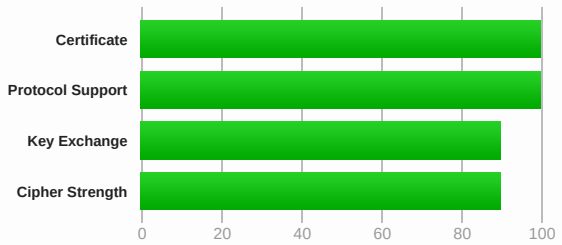
Assessed on: Sat, 08 May 2021 19:47:36 UTC | Hide | Clear cache

Scan Another »

Summary

Overall Rating

A+



Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This site works only in browsers with SNI support.

HTTP Strict Transport Security (HSTS) with long duration deployed on this server. MORE INFO »

DNS Certification Authority Authorization (CAA) Policy found for this domain. MORE INFO »

Certificate #1: EC 384 bits (SHA256withRSA)

Server Key and Certificate #1

Subject	*.sweharris.org Fingerprint SHA256: 16dfde602d65a473501018cbb9ee5fa1d4508729cbca297a0ff2bf3a22062ab3 Pin SHA256: wT1RFH93v9u3MoMFL786sk+sQprUVk0TGH/3/qSl3Ac=
Common names	*.sweharris.org
Alternative names	*.spuddy.org *.sweharris.org spuddy.org sweharris.org
Serial Number	049ecac66d6422ebcfdc162dc8e94efcc447
Valid from	Fri, 07 May 2021 15:23:43 UTC
Valid until	Thu, 05 Aug 2021 15:23:43 UTC (expires in 2 months and 27 days)
Key	EC 384 bits
Weak key (Debian)	No
Issuer	R3 AIA: http://r3.i.lencr.org/
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	OCSP OCSP: http://r3.o.lencr.org
Revocation status	Good (not revoked)
DNS CAA	Yes policy host: sweharris.org issue: letsencrypt.org flags:0
Trusted	Yes Mozilla Apple Android Java Windows

Additional Certificates (if supplied)

Certificates provided	3 (3871 bytes)
Chain issues	None

#2

Subject	R3 Fingerprint SHA256: 67add1166b020ae61b8f5fc96813c04c2aa589960796865572a3c7e737613dfd Pin SHA256: jQJTbIh0grw0/1TkHSumWb+Fs0Ggogr621gT3PvPKG0=
Valid until	Mon, 15 Sep 2025 16:00:00 UTC (expires in 4 years and 4 months)
Key	RSA 2048 bits (e 65537)
Issuer	ISRG Root X1
Signature algorithm	SHA256withRSA

#3

Subject	ISRG Root X1 Fingerprint SHA256: 6d99fb265eb1c5b3744765fcbc648f3cd8e1bffafdc4c2f99b9d47cf7ff1c24f Pin SHA256: C5+lpZ7tcVwmwQIMcRtPbsQtWLABXhQzejna0wHFr8M=
Valid until	Mon, 30 Sep 2024 18:14:03 UTC (expires in 3 years and 4 months)
Key	RSA 4096 bits (e 65537)
Issuer	DST Root CA X3
Signature algorithm	SHA256withRSA

Certification Paths

Click here to expand

Certificate #2: EC 384 bits (SHA256withRSA) No SNI

Server Key and Certificate #1

Subject	*.spuddy.org Fingerprint SHA256: c86f4fc9fa3d2b0fe7f8d0ba05147f3e4080b2d4ad2ac5f6bf4c6de02c47fd32 Pin SHA256: 43DhZlcHZS0q9XE4VmXreO3F1mlTW7t5iD5RLaMylDw=
Common names	*.spuddy.org
Alternative names	*.spuddy.org spuddy.org **MISMATCH**
Serial Number	049467586fcfd2afe9c6b98964cb374bdeb1
Valid from	Fri, 07 May 2021 15:23:37 UTC
Valid until	Thu, 05 Aug 2021 15:23:37 UTC (expires in 2 months and 27 days)
Key	EC 384 bits
Weak key (Debian)	No
Issuer	R3 AIA: http://r3.i.lencr.org/
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	OCSP OCSP: http://r3.o.lencr.org
Revocation status	Good (not revoked)
Trusted	No **NOT TRUSTED** Mozilla Apple Android Java Windows

Additional Certificates (if supplied)

Additional Certificates (if supplied)

Certificates provided	3 (3837 bytes)
Chain issues	None

#2

Subject	R3 Fingerprint SHA256: 67add1166b020ae61b8f5fc96813c04c2aa589960796865572a3c7e737613dfd Pin SHA256: jQJTbIh0grw0/1TkHSumWb+Fs0Ggogr621gT3PvPKG0=
Valid until	Mon, 15 Sep 2025 16:00:00 UTC (expires in 4 years and 4 months)
Key	RSA 2048 bits (e 65537)
Issuer	ISRG Root X1
Signature algorithm	SHA256withRSA

#3

Subject	ISRG Root X1 Fingerprint SHA256: 6d99fb265eb1c5b3744765fcbc648f3cd8e1bffafdc4c2f99b9d47cf7ff1c24f Pin SHA256: C5+lpZ7tcVwmwQIMcRtPbsQtWLABXhQzejna0wHFr8M=
Valid until	Mon, 30 Sep 2024 18:14:03 UTC (expires in 3 years and 4 months)
Key	RSA 4096 bits (e 65537)
Issuer	DST Root CA X3
Signature algorithm	SHA256withRSA

Certification Paths

Click here to expand

Certificate #3: RSA 4096 bits (SHA256withRSA)

Server Key and Certificate #1

Subject	*.sweharris.org Fingerprint SHA256: 28f79373b3d6cf960589959d4dd969dabcb604e08d90b0b91d273c8db333c441 Pin SHA256: Ss5/hz+9GJFmMi1LB1wl7lvgUpjCcb6S9+7irCLMnmA=
Common names	*.sweharris.org
Alternative names	*.spuddy.org *.sweharris.org spuddy.org sweharris.org
Serial Number	049172042c812c5c92a687bc4aefd9118977
Valid from	Fri, 07 May 2021 15:23:32 UTC
Valid until	Thu, 05 Aug 2021 15:23:32 UTC (expires in 2 months and 27 days)
Key	RSA 4096 bits (e 65537)
Weak key (Debian)	No
Issuer	R3 AIA: http://r3.i.lencr.org/
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	**Yes (certificate)**
OCSP Must Staple	No
Revocation information	OCSP OCSP: http://r3.o.lencr.org
Revocation status	Good (not revoked)
DNS CAA	**Yes** policy host: sweharris.org issue: letsencrypt.org flags:0
Trusted	**Yes** **Mozilla Apple Android Java Windows**

Additional Certificates (if supplied)

Certificates provided	3 (4304 bytes)
Chain issues	None

#2

Subject	R3 Fingerprint SHA256: 67add1166b020ae61b8f5fc96813c04c2aa589960796865572a3c7e737613dfd Pin SHA256: jQJTbIh0grw0/1TkHSumWb+Fs0Ggogr621gT3PvPKG0=
Valid until	Mon, 15 Sep 2025 16:00:00 UTC (expires in 4 years and 4 months)
Key	RSA 2048 bits (e 65537)
Issuer	ISRG Root X1
Signature algorithm	SHA256withRSA

#3

Subject	ISRG Root X1 Fingerprint SHA256: 6d99fb265eb1c5b3744765fcbc648f3cd8e1bffafdc4c2f99b9d47cf7ff1c24f Pin SHA256: C5+lpZ7tcVwmwQIMcRtPbsQtWLABXhQzejna0wHFr8M=
Valid until	Mon, 30 Sep 2024 18:14:03 UTC (expires in 3 years and 4 months)
Key	RSA 4096 bits (e 65537)
Issuer	DST Root CA X3
Signature algorithm	SHA256withRSA

Certification Paths

Click here to expand

Configuration

Protocols

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

(*) Experimental: Server negotiated using No-SNI

Cipher Suites

 # TLS 1.2 (suites in server-preferred order)

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)	ECDH secp256r1 (eq. 3072 bits RSA)	FS	256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	ECDH secp256r1 (eq. 3072 bits RSA)	FS	256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)	ECDH secp256r1 (eq. 3072 bits RSA)	FS	128
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH secp256r1 (eq. 3072 bits RSA)	FS	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	ECDH secp256r1 (eq. 3072 bits RSA)	FS WEAK	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	ECDH secp256r1 (eq. 3072 bits RSA)	FS WEAK	128

Handshake Simulation

Android 4.4.2	EC 384 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
Android 5.0.0	EC 384 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Android 6.0	EC 384 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Android 7.0	EC 384 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS

Handshake Simulation

Android 8.0	EC 384 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Android 8.1	EC 384 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Android 9.0	EC 384 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
BingPreview Jan 2015	EC 384 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Chrome 49 / XP SP3	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Chrome 69 / Win 7 R	EC 384 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Chrome 70 / Win 10	EC 384 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Chrome 80 / Win 10 R	EC 384 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Firefox 31.3.0 ESR / Win 7	EC 384 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Firefox 47 / Win 7 R	EC 384 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Firefox 49 / XP SP3	EC 384 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Firefox 62 / Win 7 R	EC 384 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Firefox 73 / Win 10 R	EC 384 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Googlebot Feb 2018	EC 384 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
IE 11 / Win 7 R	EC 384 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
IE 11 / Win 8.1 R	EC 384 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
IE 11 / Win Phone 8.1 R	EC 384 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
IE 11 / Win Phone 8.1 Update R	EC 384 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
IE 11 / Win 10 R	EC 384 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Edge 15 / Win 10 R	EC 384 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Edge 16 / Win 10 R	EC 384 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Edge 18 / Win 10 R	EC 384 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Edge 13 / Win Phone 10 R	EC 384 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Java 8u161	EC 384 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Java 11.0.3	EC 384 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Java 12.0.1	EC 384 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
OpenSSL 1.0.1l R	EC 384 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
OpenSSL 1.0.2s R	EC 384 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
OpenSSL 1.1.0k R	EC 384 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
OpenSSL 1.1.1c R	EC 384 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Safari 6 / iOS 6.0.1	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1 FS
Safari 7 / iOS 7.1 R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1 FS
Safari 7 / OS X 10.9 R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1 FS
Safari 8 / iOS 8.4 R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1 FS
Safari 8 / OS X 10.10 R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1 FS
Safari 9 / iOS 9 R	EC 384 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Safari 9 / OS X 10.11 R	EC 384 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Safari 10 / iOS 10 R	EC 384 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Safari 10 / OS X 10.12 R	EC 384 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Safari 12.1.2 / MacOS 10.14.6 Beta R	EC 384 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Safari 12.1.1 / iOS 12.3.1 R	EC 384 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Apple ATS 9 / iOS 9 R	EC 384 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
Yahoo Slurp Jan 2015	EC 384 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS
YandexBot Jan 2015	EC 384 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1 FS

 # Not simulated clients (Protocol mismatch)

Click here to expand

(1) Clients that do not support Forward Secrecy (FS) are excluded when determining support for it.

(2) No support for virtual SSL hosting (SNI). Connects to the default site if the server uses SNI.

(3) Only first connection attempt simulated. Browsers sometimes retry with a lower protocol version.

(R) Denotes a reference browser or client, with which we expect better effective security.

Handshake Simulation

(All) We use defaults, but some platforms do not use their best protocols and features (e.g., Java 6 & 7, older IE).

(All) Certificate trust is not checked in handshake simulation, we only perform TLS handshake.

Protocol Details

DROWN	No, server keys and hostname not seen elsewhere with SSLv2 **(1) For a better understanding of this test, please read this longer explanation** (2) Key usage data kindly provided by the Censys network search engine; original DROWN website here (3) Censys data is only indicative of possible key and certificate reuse; possibly out-of-date and not complete
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) TLS 1.2 : 0xc027
GOLDENDOODLE	No (more info) TLS 1.2 : 0xc027
OpenSSL 0-Length	No (more info) TLS 1.2 : 0xc027
Sleeping POODLE	No (more info) TLS 1.2 : 0xc027
Downgrade attack prevention	Unknown (requires support for at least two protocols, excl. SSL2)
SSL/TLS compression	No
RC4	No
Heartbeat (extension)	Yes
Heartbleed (vulnerability)	No (more info)
Ticketbleed (vulnerability)	No (more info)
OpenSSL CCS vuln. (CVE-2014-0224)	No (more info)
OpenSSL Padding Oracle vuln. (CVE-2016-2107)	No (more info)
ROBOT (vulnerability)	No (more info)
Forward Secrecy	**Yes (with most browsers) ROBUST** (more info)
ALPN	No
NPN	No
Session resumption (caching)	Yes
Session resumption (tickets)	Yes
OCSP stapling	No
Strict Transport Security (HSTS)	**Yes** max-age=31536000; includeSubDomains; preload
HSTS Preloading	**Chrome Edge Firefox IE**
Public Key Pinning (HPKP)	No (more info)
Public Key Pinning Report-Only	No
Public Key Pinning (Static)	No (more info)
Long handshake intolerance	No
TLS extension intolerance	No
TLS version intolerance	No
Incorrect SNI alerts	No
Uses common DH primes	No, DHE suites not supported
DH public server param (Ys) reuse	No, DHE suites not supported
ECDH public server param reuse	No
Supported Named Groups	secp256r1, secp521r1, secp384r1, secp256k1 (server preferred order)
SSL 2 handshake compatibility	No

HTTP Requests

1 **https://www.sweharris.org/** (HTTP/1.1 200 OK)

Miscellaneous

Test date	Sat, 08 May 2021 19:42:53 UTC
Test duration	141.862 seconds
HTTP status code	200
HTTP server signature	Apache
Server hostname	linode.spuddy.org

SSL Report v2.1.8