1. For each website, a summary of key properties. Include the following information:

ssllabs.com

- Subject, common name, and alternative names
    1. www.ssllabs.com
    2. www.ssllabs.com
    3. www.ssllabs.com ssllabs.com api.ssllabs.com clienttest.ssllabs.com plaintext.ssllabs.com entrust.ssllabs.com globalsign.ssllabs.com casecurity.ssllabs.com wosign.ssllabs.com akamai.ssllabs.com ota.ssllabs.com trustzone.ssllabs.com biznet.ssllabs.com comodo.ssllabs.com globaltrust.ssllabs.com secure128.ssllabs.com networking4all.ssllabs.com geocerts.ssllabs.com staging.ssllabs.com
- Validity period
    1. Valid From: Fri, 25 Jul 2025 00:00:00 UTC
    2. Valid until: Fri, 24 Jul 2026 23:59:59 UTC (expires in 8 months and 29 days)
- Type of cryptographic key
    1. RSA 2048 bits (e 65537)
- Details about the certificate chain
    1. Leaf: www.ssllabs.com
    2. Intermediate: DigiCert Global G2 TLS RSA SHA256 2020 CA1
    3. Root: DigiCert Global Root G2
- The authentication algorithm (how the client authenticates the server)
    1. ECDHE_RSA or DHE_RSA
- The symmetric encryption algorithm, key size, and mode
    1. AES_128_GCM, CHACHA20_POLY1305, AES_256_GCM,
- The hashing algorithm
    1. SHA256 and 384
- A list of the cryptographic guarantees (confidentiality, integrity, forward secrecy) provided by this configuration
    1. Confidentiality: Yes
    2. Integrity: Yes
    3. Forward Secrecy: Yes (with most browsers)
- Three other properties that you find interesting
    1. Very low test duration

2. Kinda funny this website doesn't have an A+

slack.com

- Subject, common name, and alternative names
  1. slack.com
  2. slack.com
  3. *.slack.com slack.com
- Validity period
  1. Valid from Tue, 30 Sep 2025 09:04:43 UTC
  2. Valid until Mon, 29 Dec 2025 09:04:42 UTC (expires in 2 months and 3 days)
- Type of cryptographic key
  1. RSA 2048 bits (e 65537)
- Details about the certificate chain
  1. Leaf: slack.com
  2. Intermediate: R13
  3. ISRG Root X1
- The authentication algorithm (how the client authenticates the server)
  1. ECDHE_RSA
- The symmetric encryption algorithm, key size, and mode
  1. AES_128_GCM, AES_256_GCM, CHACHA20_POLY1305
- The hashing algorithm
  1. SHA256 and 384
- A list of the cryptographic guarantees (confidentiality, integrity, forward secrecy) provided by this configuration
  1. Confidentiality: Yes
  2. Integrity: Yes
  3. Forward Secrecy: Yes (with most browsers)
- Three other properties that you find interesting
  1. Very few cipher suites

wikipedia.org

- Subject, common name, and alternative names
  1. *.wikipedia.org
  2. *.wikipedia.org
  3. *.m.mediawiki.org *.m.wikibooks.org *.m.wikidata.org *.m.wikimedia.org *.m.wikinews.org *.m.wikipedia.org *.m.wikiquote.org *.m.wikisource.org *.m.wikiversity.org *.m.wikivoyage.org *.m.wiktionary.org *.mediawiki.org

*.planet.wikimedia.org *.wikibooks.org *.wikidata.org *.wikifunctions.org *.wikimedia.org *.wikimediafoundation.org *.wikinews.org *.wikipedia.org *.wikiquote.org *.wikisource.org *.wikiversity.org *.wikivoyage.org *.wiktionary.org *.wmfusercontent.org mediawiki.org w.wiki wikibooks.org wikidata.org wikifunctions.org wikimedia.org wikimediafoundation.org wikinews.org wikipedia.org wikiquote.org wikisource.org wikiversity.org wikivoyage.org wiktionary.org wmfusercontent.org

- Validity period
    1. Valid from Thu, 09 Oct 2025 23:02:03 UTC
    2. Valid until Wed, 07 Jan 2026 23:02:02 UTC (expires in 2 months and 13 days)
- Type of cryptographic key
    1. EC 256 bits
- Details about the certificate chain
    1. Leaf: *.wikipedia.org
    2. Intermediate: E7
    3. Root: ISRG Root X1
- The authentication algorithm (how the client authenticates the server)
    1. ECDHE_ECDSA
- The symmetric encryption algorithm, key size, and mode
    1. AES_128_GCM, CHACHA20_POLY1305, AES_256_GCM
- The hashing algorithm
    1. SHA256 and 384
- A list of the cryptographic guarantees (confidentiality, integrity, forward secrecy) provided by this configuration
    1. Confidentiality: Yes
    2. Integrity: Yes
    3. Forward Secrecy: Yes (with most browsers)
- Three other properties that you find interesting
    1. Very few Cipher suites
    2. HSTS Preloading on chrome, edge, and firefox, and IE

google.com

- Subject, common name, and alternative names
    1. *.google.com
    2. *.google.com

3. *.google.com *.appengine.google.com *.bdn.dev *.origin-test.bdn.dev *.cloud.google.com *.crowdsource.google.com *.datacompute.google.com *.google.ca *.google.cl *.google.co.in *.google.co.jp *.google.co.uk *.google.com.ar *.google.com.au *.google.com.br *.google.com.co *.google.com.mx *.google.com.tr *.google.com.vn *.google.de *.google.es *.google.fr *.google.hu *.google.it *.google.nl *.google.pl *.google.pt *.googleapis.cn *.googlevideo.com *.gstatic.cn *.gstatic-cn.com googlecnapps.cn *.googlecnapps.cn googleapps-cn.com *.googleapps-cn.com gkecnapps.cn *.gkecnapps.cn googledownloads.cn *.googledownloads.cn recaptcha.net.cn *.recaptcha.net.cn recaptcha-cn.net *.recaptcha-cn.net widevine.cn *.widevine.cn ampproject.org.cn *.ampproject.org.cn ampproject.net.cn *.ampproject.net.cn google-analytics-cn.com *.google-analytics-cn.com googleadservices-cn.com *.googleadservices-cn.com googlevads-cn.com *.googlevads-cn.com googleapis-cn.com *.googleapis-cn.com googleoptimize-cn.com *.googleoptimize-cn.com doubleclick-cn.net *.doubleclick-cn.net *.fls.doubleclick-cn.net *.g.doubleclick-cn.net doubleclick.cn *.doubleclick.cn *.fls.doubleclick.cn *.g.doubleclick.cn dartsearch-cn.net *.dartsearch-cn.net googletraveladservices-cn.com *.googletraveladservices-cn.com googletagservices-cn.com *.googletagservices-cn.com googletagmanager-cn.com *.googletagmanager-cn.com googlesyndication-cn.com *.googlesyndication-cn.com *.safeframe.googlesyndication-cn.com app-measurement-cn.com *.app-measurement-cn.com gvt1-cn.com *.gvt1-cn.com gvt2-cn.com *.gvt2-cn.com 2mdn-cn.net *.2mdn-cn.net googleflights-cn.net *.googleflights-cn.net admob-cn.com *.admob-cn.com *.gemini.cloud.google.com googlesandbox-cn.com *.googlesandbox-cn.com *.safenup.googlesandbox-cn.com *.gstatic.com *.metric.gstatic.com *.gvt1.com *.gcpcdn.gvt1.com *.gvt2.com *.gcp.gvt2.com *.url.google.com *.youtube-nocookie.com *.ytimg.com ai.android android.com *.android.com *.flash.android.com g.cn *.g.cn g.co *.g.co goo.gl

www.goo.gl google-analytics.com *.google-analytics.com google.com googlecommerce.com *.googlecommerce.com ggpht.cn *.ggpht.cn urchin.com *.urchin.com youtu.be youtube.com *.youtube.com music.youtube.com *.music.youtube.com youtubeeducation.com *.youtubeeducation.com youtubekids.com *.youtubekids.com yt.be *.yt.be android.clients.google.com *.android.google.cn *.chrome.google.cn *.developers.google.cn *.aistudio.google.com

- Validity period
    1. Valid from Wed, 01 Oct 2025 14:32:25 UTC
    2. Valid until Wed, 24 Dec 2025 14:32:24 UTC (expires in 1 month and 28 days)
    3. Valid from Wed, 01 Oct 2025 14:32:04 UTC
    4. Valid until Wed, 24 Dec 2025 14:32:03 UTC (expires in 1 month and 28 days)
- Type of cryptographic key
    1. EC 256 bits, RSA 2048 bits (e 65537)
- Details about the certificate chain

i. Certificate 1
    1. Leaf: *.google.com
    2. Intermediate: WE2
    3. Root: GTS Root R4
    4. Leaf: *.google.com
    5. Intermediate: WE2
    6. Root: Globalsign
    7. Leaf: *.google.com
    8. Intermediate: WE2
    9. Root: GTS Root R4
    10. Root: Globalsign Root CA

ii. Certificate 2
    1. Leaf: *.google.com
    2. Intermediate: WR2
    3. Root: GTS Root R1
    4. Leaf: *.google.com
    5. Intermediate: WR2
    6. Root: GTS Root R1
    7. Root: GlobalSign Root CA

- The authentication algorithm (how the client authenticates the server)
    1. ECDHE_ECDSA, ECDHE_RSA, RSA
- The symmetric encryption algorithm, key size, and mode
    1. AES_128_GCM, AES_256_GCM, CHACHA20_POLY1305, AES_128_CBC, AES_256_CBC, 3DES_EDE_CBC
- The hashing algorithm
    1. SHA256 and 384
- A list of the cryptographic guarantees (confidentiality, integrity, forward secrecy) provided by this configuration
    1. Confidentiality: Yes (if not using TLS 1.0/1.1)
    2. Integrity: Yes (if not using TLS 1.0/1.1)
    3. Forward secrecy: Yes (with modern browsers)
- Three other properties that you find interesting
    1. Two certificates
    2. Allows tls 1.0/1.1
    3. Multiple certification paths

pokemonshowdown.com

- Subject, common name, and alternative names
    1. pokemonshowdown.com
    2. pokemonshowdown.com
    3. pokemonshowdown.com *.pokemonshowdown.com
- Validity period
    1. Valid from Thu, 11 Sep 2025 02:14:16 UTC
    2. Valid until Wed, 10 Dec 2025 03:10:54 UTC (expires in 1 month and 14 days)
    3. Valid from Thu, 11 Sep 2025 02:14:28 UTC
    4. Valid until Wed, 10 Dec 2025 03:14:25 UTC (expires in 1 month and 14 days)
- Type of cryptographic key
    1. RSA 2048 bits (e 65537), EC 256 bits
- Details about the certificate chain

i. Certificate 1:
    1. Leaf: pokemonshowdown.com
    2. Intermediate: WR1
    3. GTS Root R1
    4. Leaf: pokemonshowdown.com

5. Intermediate: WR1
6. Root: GTS Root R1
7. GlobalSign Root CA

ii. Certificate 2:

1. Leaf: pokemonshowdown.com
2. Intermediate: WE1
3. Root: GTS Root R4
4. Leaf: pokemonshowdown.com
5. Intermediate WE1
6. Root: Globalsign
7. Leaf: pokemonshowdown.com
8. Intermediate: WE1
9. Root: GTS Root R4
10. Root: Globalsign Root CA

- The authentication algorithm (how the client authenticates the server)
  1. ECDHE_ECDSA, ECDHE_RSA, RSA, RSA
- The symmetric encryption algorithm, key size, and mode
  1. AES_128_GCM, AES_256_GCM, CHACHA20_POLY1305, AES_128_CBC, AES_256_CBC, 3DES_EDE_CBC
- The hashing algorithm
  1. SHA256 and 384
- A list of the cryptographic guarantees (confidentiality, integrity, forward secrecy) provided by this configuration
  1. Confidentiality: Yes (if not using TLS 1.0/1.1)
  2. Integrity: Yes (if not using TLS 1.0/1.1)
  3. Forward Secrecy: Yes (with modern browsers
- Three other properties that you find interesting
  1. Similar layout to google
  2. Beast attack not mitigated server side
  3. No strict transport security

angelarium.net

- Subject, common name, and alternative names
  1. angelarium.net
  2. angelarium.net
  3. angelarium.net
- Validity period
  1. Valid from Thu, 04 Sep 2025 04:32:52 UTC

        2. Valid until Wed, 03 Dec 2025 04:32:51 UTC (expires in 1 month and 7 days)
    - Type of cryptographic key
        1. RSA 2048 bits (e 65537)
    - Details about the certificate chain
        1. Leaf: angelarium.net
        2. Intermediate: R13
        3. Root: ISRG Root X1
    - The authentication algorithm (how the client authenticates the server)
        1. ECDHE_RSA,
    - The symmetric encryption algorithm, key size, and mode
        1. AES_128_GCM, AES_256_GCM, CHACHA20_POLY1305, AES_128_CBC, AES_256_CBC
    - The hashing algorithm
        1. SHA256 and 384
    - A list of the cryptographic guarantees (confidentiality, integrity, forward secrecy) provided by this configuration
        1. Confidentiality: Yes
        2. Integrity: Yes
        3. Forward Secrecy: Yes (with most browsers)
    - Three other properties that you find interesting
        1. Very highly rated for a niche website
        2. Has a second experimental certificate with no SNI that seems to be based out of squarespace
        3. Only works in browsers with SNI support

cachemonet.com

    - Subject, common name, and alternative names
        1. internet-of-everywhere.com.spent2000.com
        2. internet-of-everywhere.com.spent2000.com
        3. cachemonet.com cachemonet.com.spent2000.com cpanel.cachemonet.com cpcalendars.cachemonet.com cpcontacts.cachemonet.com internet-of-everywhere.com.spent2000.com webdisk.cachemonet.com webmail.cachemonet.com www.cachemonet.com www.cachemonet.com.spent2000.com www.internet-of-everywhere.com.spent2000.com
    - Validity period

1. Valid from Mon, 15 Sep 2025 02:04:49 UTC
2. Valid until Sun, 14 Dec 2025 02:04:48 UTC (expires in 1 month and 18 days)

- Type of cryptographic key
  1. RSA 2048 bits (e 65537)
- Details about the certificate chain
  1. Leaf: internet-of-everywhere.com.spent2000.com
  2. Intermediate: R13
  3. Root: ISRG Root X1
- The authentication algorithm (how the client authenticates the server)
  1. ECDHE_RSA or DHE_RSA
- The symmetric encryption algorithm, key size, and mode
  1. AES_256_GCM, AES_128_GCM
- The hashing algorithm
  1. SHA384 and 256
- A list of the cryptographic guarantees (confidentiality, integrity, forward secrecy) provided by this configuration
  1. Confidentiality: yes
  2. Integrity: yes
  3. Forward secrecy: yes (with most browsers)
- Three other properties that you find interesting
  1. Pretty good score despite being an old niche website
  2. Doesn't use TLS 1.3
  3. Unknown downgrade attack prevention

magic.wizards.com

- Subject, common name, and alternative names
  1. media.wizards.com
  2. media.wizards.com
  3. media.wizards.com accounts.platform-dev.wizards.com accounts.platform-ref.wizards.com accounts.platform.wizards.com accounts.wizards.com admin-dev.wizards.com admin.api.lantern-stage.wizards.com admin.api.lantern.wizards.com admin.wizards.com api.blitz-stage.wizards.com api.blitz.wizards.com api.coderedemption.dev.wizards.com api.coderedemption.int.wizards.com api.coderedemption.ref.wizards.com

api.coth-stage.wizards.com api.coth.wizards.com
api.dev.tabletop.wizards.com api.ecom-reference.wizards.com
api.ecom.wizards.com api.hunterer-stage.wizards.com
api.hunterer.wizards.com api.platform-dev.wizards.com
api.platform-ref.wizards.com api.platform.wizards.com
api.tabletop-dev.wizards.com api.tabletop-stage.wizards.com
api.tabletop.wizards.com api.tiamat.cloud
arena-stage.api.bi-redshell.wizards.com
arena-stage.api.bi.wizards.com
arena.api.bi-redshell.wizards.com arena.api.bi.wizards.com
assets.blitz.wizards.com avalonhill.wizards.com
blitz-milestone.auth.api.wizards.com
blitz-stage.api.admin.wizards.com
blitz-stage.api.auth.wizards.com blitz-stage.api.bi.wizards.com
blitz-stage.api.image.wizards.com
blitz-stage.api.logging.wizards.com
blitz-stage.api.search.wizards.com
blitz.api.admin.wizards.com blitz.api.auth.wizards.com
blitz.api.bi.wizards.com blitz.api.image.wizards.com
blitz.api.logging.wizards.com blitz.api.search.wizards.com
blitz.auth.api.wizards.com cdn.blitz.wizards.com
cdn.platform-dev.wizards.com cdn.wizards.com
company.wizards.com dnd.wizards.com edit.wpn.wizards.com
eventlink.dev.tabletop.wizards.com
eventlink.stage.tabletop.wizards.com
gideonprodlinks.wizards.com images.hunterer.wizards.com
lantern-stage.api.bi-sumo.wizards.com
lantern-stage.api.bi.wizards.com
lantern.api.bi-sumo.wizards.com lantern.api.bi.wizards.com
lantern.api.logging.wizards.com learnmtg.wizards.com
magic.wizards.com magic2.wizards.com
marketing.api.bi-sumo.wizards.com
marketing.api.bi.wizards.com
mtga-stage.auth.api.wizards.com
mtga.api.clogging.wizards.com
mtgarena.api.bi-installs.wizards.com
mtgarenapasswordreset.wizards.com
oauth2.platform-dev.wizards.com
oauth2.platform.wizards.com pfval.mtga.api.wizards.com

platform-stage.api.bi.wizards.com platform.api.bi.wizards.com platform.wizards.com qa.magic.wizards.com service.wer.api.wizards.com sts.tiamat.cloud sumologic.wizards.com support.tiamat.cloud tabletop.api.braze.wizards.com tiamat.cloud web.tabletop-stage.wizards.com web.tabletop.wizards.com webr00accounts.wizards.com webr02accounts.wizards.com webr11accounts.wizards.com webr12accounts.wizards.com webr20accounts.wizards.com wotc-blitz.logs.tiamat.cloud wpn.wizards.com ww2.wizards.com www.tiamat.cloud www.wizards.com

- Validity period
    1. Valid from Fri, 18 Jul 2025 00:00:00 UTC
    2. Valid until Fri, 17 Jul 2026 23:59:59 UTC (expires in 8 months and 21 days)
- Type of cryptographic key
    1. RSA 2048 bits (e 65537)
- Details about the certificate chain
    1. Leaf: media.wizards.com
    2. Intermediate: GeoTrust TLS RSA CA G1
    3. Root: DigiCert Global Root G2
- The authentication algorithm (how the client authenticates the server)
    1. ECDHE_RSA, RSA
- The symmetric encryption algorithm, key size, and mode
    1. AES_256_GCM, CHACHA20_POLY1305, AES_128_GCM, AES_128_CCM_8, AES_128_CCM
- The hashing algorithm
    1. SHA384 and 256
- A list of the cryptographic guarantees (confidentiality, integrity, forward secrecy) provided by this configuration
    1. Confidentiality: Yes (if not using TLS 1.0/1.1)
    2. Integrity: Yes (if not using TLS 1.0/1.1)
    3. Forward Security: Yes (with modern browsers)
- Three other properties that you find interesting
    1. Two http requests, which I had only seen before for login redirects
    2. So many alternative names

code.ornl.gov

- Subject, common name, and alternative names
    1. code.ornl.gov
    2. code.ornl.gov
    3. code.ornl.gov, code-cloud.ornl.gov
- Validity period
    1. Valid from Fri, 12 Sep 2025 00:00:00 UTC
    2. Valid until Tue, 13 Oct 2026 23:59:59 UTC (expires in 11 months and 18 days)
- Type of cryptographic key
    1. RSA 2048 bits (e 65537)
- Details about the certificate chain
    1. Leaf: code.ornl.gov
    2. Intermediate: InCommon RSA Server CA 2
    3. Root: USERTrust RSA Certification Authority
    4. Leaf: code.ornl.gov
    5. Intermediate: InCommon RSA Server CA 2
    6. Root: USERTrust RSA Certification Authority
    7. Root: AAA Certificate Services
- The authentication algorithm (how the client authenticates the server)
    1. ECDHE_RSA
- The symmetric encryption algorithm, key size, and mode
    1. AES_128_GCM, AES_256_GCM, CHACHA20_POLY1305
- The hashing algorithm
    1. SHA256 and 384
- A list of the cryptographic guarantees (confidentiality, integrity, forward secrecy) provided by this configuration
    1. Confidentiality: Yes
    2. Integrity: Yes
    3. Forward Secrecy: Yes (with most browsers)
- Three other properties that you find interesting
    1. Very few cipher suites
    2. Two HTTP requests
    3. Certificate valid for a long time

wco.tv

- Subject, common name, and alternative names

        1. wco.tv
        2. wco.tv
        3. wco.tv *.wco.tv
    - Validity period
        1. Valid from Mon, 29 Sep 2025 12:34:01 UTC
        2. Valid until Sun, 28 Dec 2025 13:32:32 UTC (expires in 2 months and 2 days)
    - Type of cryptographic key
        1. RSA 2048 bits (e 65537)
    - Details about the certificate chain
        1. Leaf: wco.tv
        2. Intermediate: WE1
        3. Root: GTS Root R4
    - The authentication algorithm (how the client authenticates the server)
        1. ECDHE_ECDSA, ECDHE_RSA, RSA,
    - The symmetric encryption algorithm, key size, and mode
        1. AES_128_GCM, AES_256_GCM, CHACHA20_POLY1305, AES_128_CBC, AES_256_CBC, 3DES_EDE_CBC
    - The hashing algorithm
        1. SHA256 and 384
    - A list of the cryptographic guarantees (confidentiality, integrity, forward secrecy) provided by this configuration
        1. Confidentiality: Yes, if not using TLS 1.0/1.1
        2. Integrity: Yes, if not using TLS 1.0/1.1
        3. Forward Secrecy: With modern browsers
    - Three other properties that you find interesting
        1. Allows outdated versions of TLS
        2. Had multiple ip addresses when searching for it
        3. Had a lot of handshake failures
2. A textual summary of any interesting differences or common features that you observe.
    - Every website used the same hashing algorithm
    - Every site used TLS 1.2 as one of its preferred TLS. Almost every website used 1.3 as well except for cachemonet.com
    - Every site had all the cryptographic guarantees, though sometimes it was conditional.
    - No site was worse than a B, and every one that was worse than an A- was ranked so because it allowed TLS 1.0 and 1.1.

3. List questions about any information you don't understand or would like to know more about.
    - I don't really get what exactly was supposed to be especially interesting, other than things I assume would be pretty rare such as huge security flaws. I didn't see anything super out there like being weak to heartbleed, but I did find one that was susceptible to beast attack and another that didn't have TLS 1.3 so I guess that's interesting.

Reviewed by Eli Smith