Website Comparisons

In this project, I evaluated the TLS configuration of 10 different websites. Websites like Google, .NET, Stack Overflow, Canvas, and GitHub are popular and get large amounts of web traffic every day. Others, like STARI Labs, UTK's website for Engineering Fundamentals, Knox Election Commission, ASEE PEER, and the NSF portal, are used by smaller groups due to their niche services. All the websites listed provide basic cryptographic security, and none score lower than a B according to the SSL Labs ratings. Interestingly, the size of the platform does not correlate with a higher rating or better security features; in fact, one of the largest platforms, Google, has a relatively "low" score because it supports TLS 1.0 and 1.1. A summary of the results is below.

	Subject, Name or Alternative Names *From Subject, Common names, and Alternative Names in Certificate*	Validity Period *From Valid Dates in Certificate*	Type of Cryptographic Key *From Key in Certificate*	Certificate Chain Details *From Issuer in Certificates*	Authentication Algorithm *From Signature algorithm in certificate*	Symmetric Encryption Algorithm, Key Size, Mode *From Cipher Suites*	Hashing Algorithm *From Cipher Suites*	Confidentiality, Integrity, Forward Secrecy *If strong symmetric cipher, GCM or SHA, FS flag*	TLS Support *From Configuration*	Protocol Vulnerabilities or Misconfigurations *From Protocol Details*	OCSP Must Staple *From Certificate*	Overall Rating *From Summary*
STARI Labs	*stari.labs.utk.edu*	9/17/25–12/16/25 (3 mo.)	RSA 2048 bits (e 65537)	WR GTS Root R1 GlobalSign Root CA	RSA	AES, 128, GCM	SHA-256	yes, yes, yes	1.3, 1.2	no session resumption	no	A
Google	*www.google.com*	10/1/25–12/24/25 (3 mo.)	EC 256 bits	WE2 GTS Root R4 GlobalSign Root CA	ECDSA	AES, 128, GCM	SHA-256	yes, yes, yes	1.3, 1.2, 1.1, 1.0	no session resumption, no strict transport security (HSTS)	no	B
EF Website	*efcms.engr.utk.edu*, efdata.engr.utk.edu, efdev.engr.utk.edu, efold.engr.utk.edu	1/10/25 – 2/10/26 (1 yr.)	RSA 2048 bits (e 65537)	incomplete	RSA	AES, 256, GCM	SHA-384	yes, yes, yes	1.2	none	no	B
.NET Documentation	*learn.microsoft.com*, www.learn.microsoft.com	7/17/25 – 7/12/26 (1 yr.)	EC 256 bits	Microsoft Azure ECC TLS Issuing CA 04 DigiCert Global Root G3	ECDSA	AES, 256, GCM	SHA-384	yes, yes, yes	1.3, 1.2	none	no	A+
Knox Election Commission	*knoxcounty.org*, *.knoxcounty.org, *.kcgweb.org	4/15/25–5/14/26 (1 yr.)	RSA 2048 bits (e 65537)	Amazon RSA 2048 M02 Amazon Root CA 1 Starfield Services Root Certificate Authority - G2	RSA	AES, 128, GCM	SHA-256	yes, yes, yes	1.3, 1.2	no session resumption, no strict transport security (HSTS)	no	A
StackOverflow	*stackoverflow.com*	10/17/25–1/15/26 (3 mo.)	RSA 2048 bits (e 65537)	R12 ISRG Root X1	RSA	AES, 128, GCM	SHA-256	yes, yes, yes	1.3, 1.2	no session resumption	no	A+

ASEE PEER	*peer.asee.org*, www.peer.asee.org	12/3/24–12/3/25 (1 yr.)	RSA 2048 bits (e 65537)	Sectigo RSA Domain Validation Secure Server CA USERTrust RSA Certification Authority AAA Certificate Services AAA Certificate Services	RSA	AES, 256, GCM	SHA-384	yes, yes, yes	1.3, 1.2	no session resumption	no	A+
Canvas	*cluster95.canvas-user-content.com*, *.instructure.com, instructure.com, canvaslms.com, *.canvaslms.com, *.cluster95.canvas-user-content.com	6/2/25–7/1/26 (1 yr.)	RSA 2048 bits (e 65537)	Amazon RSA 2048 M03 Amazon Root CA 1 Starfield Services Root Certificate Authority - G2	RSA	AES, 128, GCM	SHA-256	yes, yes, yes	1.3, 1.2	none	no	A+
GitHub	*github.com*, www.github.com	3/10/25–3/10/26 (1 yr.)	RSA 4096 bits (e 65537)	Sectigo RSA Domain Validation Secure Server CA USERTrust RSA Certification Authority AAA Certificate Services	RSA	AES, 128, GCM	SHA-256	yes, yes, yes	1.3, 1.2	no session resumption	no	A+
NSF Portal	*www.research.gov*	8/12/25–9/9/26 (1 yr.)	RSA 2048 bits (e 65537)	DigiCert Global G2 TLS RSA SHA256 2020 CA1 DigiCert Global Root G2 DigiCert Global Root G2	RSA	AES, 128, GCM	SHA-256	yes, yes, yes	1.2	DH public server param (Ys) reuse	No	A-

Similarities and Differences

All the websites tested used AES-128 with GCM as their symmetric encryption algorithm, and none required OCSP Must Staple. Every website offered confidentiality, integrity, and forward secrecy. The validity period of each certificate varied by website, with some operating on a 3-month renewal cycle and others on a 1-year cycle. The cryptographic key types were either RSA 2048, RSA 4096, or EC 256 bits. Most certificates had three certificates in their chain. Some were self-signed, and one website (UTK Engineering Fundamentals) had no chain at all, which may have resulted from a retrieval error. The hashing algorithm was either SHA-256 or SHA-384. While every website supported TLS 1.2 and most supported TLS 1.3, Google also supported TLS 1.1 and 1.0. The most common protocol vulnerability was "no session resumption"; a few websites didn't support HSTS, and one website reused Diffie-Hellman keys.

Questions

1. Why is "no session resumption" dangerous?
2. Why don't any websites require OCSP Must Staple?
3. How does Google stay secure while still supporting TLS 1.0 and 1.1?

This report was reviewed by Colsen Murray.