Qualys. SSL Labs

Hom

You are here: Home > Projects > SSL Server Test > turma-de-elite-app.web.app > 151.101.1.195

SSL Report: turma-de-elite-app.web.app (151.101.1.195)

Summary

Overall Rating

A+

Certificate

Protocol Support

Key Exchange

Cipher Strength

0 20

Visit our documentation page for more information, configuration guides, and books. Known

This site works only in browsers with SNI support.

This server supports TLS 1.3.

HTTP Strict Transport Security (HSTS) with long duration deployed on this serv

DNS Certification Authority Authorization (CAA) Policy found for this domain

Certificate #1: RSA 2048 bits (SHA256withRSA)

Server Key and Certificate #1

Subject	web.app Fingerprint SHA256: 8e461f08a11149c79a4ef8c5ed4345900105aa0639e1 Pin SHA256: P7YpVDZk5+TgFQuj0Q+HIU+Is62UHOvxuzn4dJluUBo=
Common names	web.app
Alternative names	web.app *.web.app
Serial Number	22552726b3fa5e1d0a00000000d6dfe7
Valid from	Wed, 19 May 2021 21:19:33 UTC
Valid until	Tue, 17 Aug 2021 21:19:32 UTC (expires in 29 days, 23 hou

Additional Certificates (if supplied)

Subject	GTS CA 1D4 Fingerprint SHA256: 64e286b76063602a372efd60cde8db2656a49ee15e84254b3d6eb5fe38 Pin SHA256: cXjPgKdVe6iojP8s0YQJ3rtmDFHTnYZxcYvmYGFiYME=
Valid until	Thu, 30 Sep 2027 00:00:42 UTC (expires in 6 years and 2 months)
Key	RSA 2048 bits (e 65537)
Issuer	GTS Root R1
Signature algorithm	SHA256withRSA

#3

Subject	GTS Root R1 Fingerprint SHA256: 3ee0278df71fa3c125c4cd487f01d774694e6fc57e0cd94c24efd769133 Pin SHA256: hxqRlPTu1bMS/0DITB1SSu0vd4u/8l8TjPgfaAp63Gc=
Valid until	Fri, 28 Jan 2028 00:00:42 UTC (expires in 6 years and 6 months)
Key	RSA 4096 bits (e 65537)
Issuer	GlobalSign Root CA
Signature algorithm	SHA256withRSA

Certification Paths

Click here to expand

Certificate #2: RSA 2048 bits (SHA256withRSA) No SNI

Click here to expand

Configuration

Protocols

TLS 1.3	
TLS 1.2	
TLS 1.1	
TLS 1.0	
SSL 3	
SSL 2	

(*) Experimental: Server negotiated using No-SNI

Handshake Simulation

Android 4.4.2	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_12
Android 5.0.0	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_12
Android 6.0	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_12
Android 7.0	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_CHACH
Android 8.0	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_CHACH
Android 8.1	-	TLS 1.3	TLS_CHACHA20_POLY1305_SHA
Android 9.0	-	TLS 1.3	TLS_CHACHA20_POLY1305_SHA
BingPreview Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_12
Chrome 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_12
Chrome 69 / Win 7 R	Protocol or cipher suite mismatch 0x7f1c | TLS_AES_128_GCM_SHA256		
Chrome 70 / Win 10	-	TLS 1.3	TLS_AES_128_GCM_SHA256 EC
Chrome 80 / Win 10 R	-	TLS 1.3	TLS_AES_128_GCM_SHA256 EC
Firefox 31.3.0 ESR / Win 7	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_12
Firefox 47 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_12
Firefox 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_12
Firefox 62 / Win 7 R	Protocol or cipher suite mismatch 0x7f1c | TLS_AES_128_GCM_SHA256		
Firefox 73 / Win 10 R	-	TLS 1.3	TLS_AES_128_GCM_SHA256 EC
Googlebot Feb 2018	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_12
IE 11 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_12
IE 11 / Win 8.1 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_12
IE 11 / Win Phone 8.1 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_12
IE 11 / Win Phone 8.1 Update R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_12
IE 11 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_12
Edge 15 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_12
Edge 16 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_12
Edge 18 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_12
Edge 13 / Win Phone 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_12
Java 8u161	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_12
Java 11.0.3	-	TLS 1.3	TLS_AES_128_GCM_SHA256 EC
Java 12.0.1	-	TLS 1.3	TLS_AES_128_GCM_SHA256 EC
OpenSSL 1.0.1l R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_12
OpenSSL 1.0.2s R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_12
OpenSSL 1.1.0k R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_12
OpenSSL 1.1.1c R	-	TLS 1.3	TLS_AES_256_GCM_SHA384 EC
Safari 6 / iOS 6.0.1	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_12
Safari 7 / iOS 7.1 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_12
Safari 7 / OS X 10.9 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_12
Safari 8 / iOS 8.4 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_12

Protocol Details

DROWN	No, server keys and hostname not seen elsewhere with SSL **(1) For a better understanding of this test, please read th** (2) Key usage data kindly provided by the Censys network s (3) Censys data is only indicative of possible key and certific
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	**Yes, TLS_FALLBACK_SCSV supported** (more info)
SSL/TLS compression	No
RC4	No
Heartbeat (extension)	No
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	Yes h2 http/1.1
NPN	No
Session resumption (caching)	Yes
Session resumption (tickets)	Yes
OCSP stapling	**Yes**
Strict Transport Security (HSTS)	**Yes** max-age=31556926; 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

Copyright © 2009-2021 Qualys, Inc. All Rights Reserved.

Try Qualys for free! Experience the award-winning Qualys Cloud Platform and the entire collection of Qualys Cloud Apps, including c