

Home Projects Qualys Free Trial Contact

You are here: Home > Projects > SSL Server Test > ourshopee.com > 2606:4700:3108:0:0:ac42:2b3b

SSL Report: <u>ourshopee.com</u> (2606:4700:3108:0:0:0:ac42:2b3b)

Assessed on: Sun, 07 Jul 2024 10:31:13 UTC | Hide | Clear cache

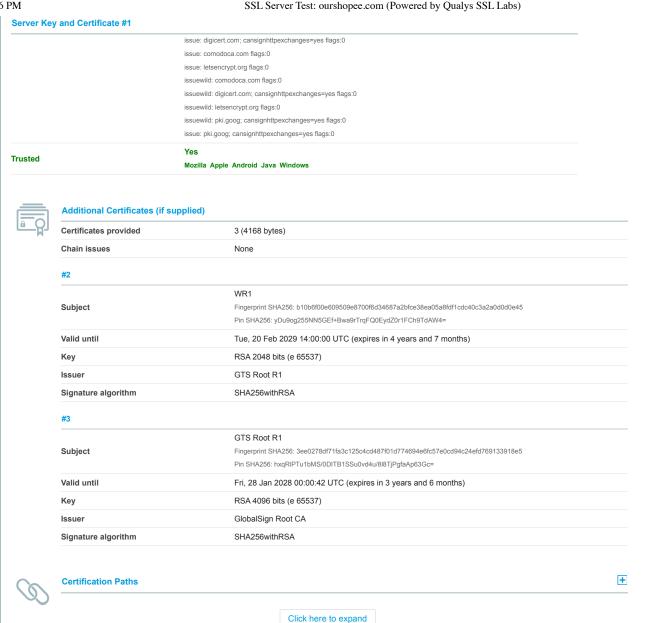
Scan Another »

Overall Rating Certificate Protocol Support Key Exchange Cipher Strength 0 20 40 60 80 100 Visit our documentation page for more information, configuration guides, and books. Known issues are documented here. This server supports TLS 1.0 and TLS 1.1. Grade capped to B. MORE INFO > This site works only in browsers with SNI support. This server supports TLS 1.3. DNS Certification Authority Authorization (CAA) Policy found for this domain. MORE INFO >

Certificate #1: RSA 2048 bits (SHA256withRSA)



	ourshopee.com	
Subject	Fingerprint SHA256: febe2688df1afe54777be13afbc075b848e141ccddd64f7999cae34e1e7434ff	
	Pin SHA256: sckBbG9MIIF5osO3KeDno5Q8PM1q5djAZnsKyGaBGrw=	
Common names	ourshopee.com	
Alternative names	ourshopee.com saudi.ourshopee.com www.saudi.ourshopee.com www.bahrain.ourshopee.com www.kuwait-	
	$. our shope e. com\ www. oman. our shope e. com\ *. our shope e. com\ www. qatar. our shope e.$	
Serial Number	00a54c05c0f8e6b4c91133aead2cfa613d	
/alid from	Fri, 28 Jun 2024 01:15:51 UTC	
Valid until	Thu, 26 Sep 2024 02:12:56 UTC (expires in 2 months and 18 days)	
Key	RSA 2048 bits (e 65537)	
Weak key (Debian)	No	
Issuer	WR1	
	AIA: http://i.pki.goog/wr1.crt	
Signature algorithm	SHA256withRSA	
Extended Validation	No	
Certificate Transparency	Yes (certificate)	
OCSP Must Staple	No	
	CRL, OCSP	
Revocation information	CRL: http://c.pki.goog/wr1/OPAcs8oa8qo.crl	
	OCSP: http://o.pki.goog/s/wr1/pUw	
Revocation status	Good (not revoked)	
DNS CAA	Yes	
	policy host: ourshopee.com	



Click here to expand

Certificate #2: EC 256 bits (SHA256withECDSA) Server Key and Certificate #1 ourshopee.com Subject Fingerprint SHA256: 8427e6053cf3c8f0651c6e5909c92d3e81143253849ea3d9c07e9c812a2fee69 Pin SHA256: YlfZn55pXzkvODs+LqRcwCYThOMrm7GBWkEJO072PhQ= Common names ourshopee.com ourshopee.com saudi.ourshopee.com www.saudi.ourshopee.com www.bahrain.ourshopee.com www.kuwait-Alternative names .ourshopee.com www.oman.ourshopee.com www.qatar.ourshopee.com *.ourshopee.com Serial Number 27889eef7888091413cbb3651daab422 Valid from Fri, 28 Jun 2024 01:16:26 UTC Valid until Thu, 26 Sep 2024 02:15:58 UTC (expires in 2 months and 18 days) EC 256 bits Key Weak key (Debian) No Issuer AIA: http://i.pki.goog/we1.crt

SHA256withECDSA

Signature algorithm

Extended Validation

Server Key and Certificate #1 **Certificate Transparency** Yes (certificate) **OCSP Must Staple** No CRI OCSP Revocation information CRL: http://c.pki.goog/we1/n0dx7V1Gbbo.crl OCSP: http://o.pki.goog/s/we1/J4g Revocation status Good (not revoked) Yes policy host: ourshopee.com issue: digicert.com; cansignhttpexchanges=yes flags:0 issue: comodoca.com flags:0 issue: letsencrypt.org flags:0 **DNS CAA** issuewild: comodoca.com flags:0 issuewild: digicert.com; cansignhttpexchanges=yes flags:0 issuewild: letsencrypt.org flags:0 issuewild: pki.goog; cansignhttpexchanges=yes flags:0 issue: pki.goog: cansignhttpexchanges=ves flags:0 Trusted Mozilla Apple Android Java Windows **Additional Certificates (if supplied)** Certificates provided 3 (2663 bytes) Chain issues None #2 WE1 Subject Fingerprint SHA256: 1dfc1605fbad358d8bc844f76d15203fac9ca5c1a79fd4857ffaf2864fbebf96 Pin SHA256: kldp6NNEd8wsugYyylYFsi1ylMCED3hZbSR8ZFsa/A4= Valid until Tue, 20 Feb 2029 14:00:00 UTC (expires in 4 years and 7 months) EC 256 bits Key Issuer GTS Root R4 Signature algorithm SHA384withECDSA #3 GTS Root R4 Subject Fingerprint SHA256: 76b27b80a58027dc3cf1da68dac17010ed93997d0b603e2fadbe85012493b5a7 Pin SHA256: mEflZT5enoR1FuXLgYYGqnVEoZvmf9c2bVBpiOjYQ0c= Valid until Fri, 28 Jan 2028 00:00:42 UTC (expires in 3 years and 6 months) Key EC 384 bits GlobalSign Root CA Issuer Signature algorithm SHA256withRSA **Certification Paths** +

Click here to expand

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



Cipher Suites

#TLS 1.3 (server has no preference)	=
TLS_AES_128_GCM_SHA256 (0x1301) ECDH x25519 (eq. 3072 bits RSA) FS	128
TLS_AES_256_GCM_SHA384 (0x1302) ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_CHACHA20_POLY1305_SHA256 (0x1303) ECDH x25519 (eq. 3072 bits RSA) FS	256
#TLS 1.2 (suites in server-preferred order)	_
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b) ECDH x25519 (eq. 3072 bits RSA) FS	128
OLD_TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcc14) ECDH x25519 (eq. 3072 bits RSA) FS	256 ^P
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9) ECDH x25519 (eq. 3072 bits RSA) FS	256 ^P
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) ECDH x25519 (eq. 3072 bits RSA) FS WEAK	128
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c) ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) ECDH x25519 (eq. 3072 bits RSA) FS WEAK	256
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023) ECDH x25519 (eq. 3072 bits RSA) FS WEAK	128
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024) ECDH x25519 (eq. 3072 bits RSA) FS WEAK	256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ECDH x25519 (eq. 3072 bits RSA) FS	128
OLD_TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcc13) ECDH x25519 (eq. 3072 bits RSA) FS	256 ^P
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8) ECDH x25519 (eq. 3072 bits RSA) FS	256 ^P
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH x25519 (eq. 3072 bits RSA) FS WEAK	128
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c) WEAK	128
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) WEAK	128
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH x25519 (eq. 3072 bits RSA) FS WEAK	256
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d) WEAK	256
TLS_RSA_WITH_AES_256_CBC_SHA (0x35) WEAK	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ECDH x25519 (eq. 3072 bits RSA) FS WEAK	128
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c) WEAK	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ECDH x25519 (eq. 3072 bits RSA) FS WEAK	256
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d) WEAK	256
#TLS 1.1 (suites in server-preferred order)	
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH x25519 (eq. 3072 bits RSA) FS WEAK	128
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) WEAK	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH x25519 (eq. 3072 bits RSA) FS WEAK	256
TLS_RSA_WITH_AES_256_CBC_SHA (0x35) WEAK	256
#TLS 1.0 (suites in server-preferred order)	
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH x25519 (eq. 3072 bits RSA) FS WEAK	128
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) WEAK	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH x25519 (eq. 3072 bits RSA) FS WEAK	256
TLS_RSA_WITH_AES_256_CBC_SHA (0x35) WEAK	256
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) WEAK	112
(D) T1:	



Handshake Simulation

Android 2.3.7 No SNI ²	Server sent fatal alert: handshake_failure		
Android 4.0.4	RSA 2048 (SHA256) TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS	
Android 4.1.1	RSA 2048 (SHA256) TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS	
Android 4.2.2	RSA 2048 (SHA256) TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS	
Android 4.3	RSA 2048 (SHA256) TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS	
Android 4.4.2	EC 256 (SHA256) TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS	

(P) This server prefers ChaCha20 suites with clients that don't have AES-NI (e.g., Android devices)

Android 5.0.0	EC 256 (SHA256)	TLS 1.2	OLD TIS ECDUE ECDSA WITH CHACHASA DOLVASOE SHASES FORLY ASSAULT
			OLD_TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256_ECDH_secp256r1_F
Android 6.0	EC 256 (SHA256)		OLD_TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 ECDH secp256r1 F
Android 7.0	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 ECDH x25519 FS
Android 8.0	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 ECDH x25519 FS
Android 8.1	-	TLS 1.3	TLS_CHACHA20_POLY1305_SHA256 ECDH x25519 FS
Android 9.0	-	TLS 1.3	TLS_CHACHA20_POLY1305_SHA256 ECDH x25519 FS
Baidu Jan 2015	RSA 2048 (SHA256)		TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_ECDH secp256r1_FS
BingPreview Jan 2015	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Chrome 49 / XP SP3	RSA 2048 (SHA256)		TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Chrome 69 / Win 7 R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS
Chrome 70 / Win 10	-	TLS 1.3	TLS_AES_128_GCM_SHA256 ECDH x25519 FS
Chrome 80 / Win 10 R	-	TLS 1.3	TLS_AES_128_GCM_SHA256 ECDH x25519 FS
Firefox 31.3.0 ESR / Win 7	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Firefox 47 / Win 7 R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Firefox 49 / XP SP3	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Firefox 62 / Win 7 R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS
Firefox 73 / Win 10 R	-	TLS 1.3	TLS_AES_128_GCM_SHA256 ECDH x25519 FS
Googlebot Feb 2018	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS
E 7 / Vista	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
E8/XP No FS ¹ No SNI ²	Server sent fatal a	lert: handshake_fail	ure
<u>E 8-10 / Win 7</u> R	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
<u>E 11 / Win 7</u> R	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
<u>E 11 / Win 8.1</u> R	EC 256 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
E 10 / Win Phone 8.0	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
IE 11 / Win Phone 8.1 R	EC 256 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
IE 11 / Win Phone 8.1 Update R	EC 256 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
<u>E 11 / Win 10</u> R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Edge 15 / Win 10 R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS
Edge 16 / Win 10 R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS
Edge 18 / Win 10 R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS
Edge 13 / Win Phone 10 R	EC 256 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Java 6u45 No SNI ²	Server sent fatal a	lert: handshake_fail	ure
Java 7u25	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Java 8u161			
the state of the s	EC 256 (SHA256)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Java 11.0.3	EC 256 (SHA256)	TLS 1.2 TLS 1.3	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS TLS_AES_128_GCM_SHA256 ECDH secp256r1 FS
	EC 256 (SHA256)		
Java 11.0.3 Java 12.0.1	EC 256 (SHA256) - RSA 2048 (SHA256)	TLS 1.3 TLS 1.3	TLS_AES_128_GCM_SHA256 ECDH secp256r1 FS
Java 11.0.3	-	TLS 1.3 TLS 1.3	TLS_AES_128_GCM_SHA256
Java 11.0.3 Java 12.0.1 OpenSSL 0.9.8y	- RSA 2048 (SHA256)	TLS 1.3 TLS 1.3	TLS_AES_128_GCM_SHA256 ECDH secp256r1 FS TLS_AES_128_GCM_SHA256 ECDH secp256r1 FS TLS_RSA_WITH_AES_128_CBC_SHA No FS
Java 11.0.3 Java 12.0.1 OpenSSL 0.9.8y OpenSSL 1.0.1 R	- RSA 2048 (SHA256) EC 256 (SHA256)	TLS 1.3 TLS 1.3 TLS 1.0 TLS 1.2	TLS_AES_128_GCM_SHA256 ECDH secp256r1 FS TLS_AES_128_GCM_SHA256 ECDH secp256r1 FS TLS_RSA_WITH_AES_128_CBC_SHA No FS TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
DenSSL 1.0.1 R OpenSSL 1.0.2s R OpenSSL 1.1.0k R	- RSA 2048 (SHA256) EC 256 (SHA256) EC 256 (SHA256)	TLS 1.3 TLS 1.0 TLS 1.2 TLS 1.2	TLS_AES_128_GCM_SHA256 ECDH secp256r1 FS TLS_AES_128_GCM_SHA256 ECDH secp256r1 FS TLS_RSA_WITH_AES_128_CBC_SHA No FS TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
DenSSL 1.0.1 R DenSSL 1.0.2 R DenSSL 1.1.0 R DenSSL 1.1.0 R	- RSA 2048 (SHA256) EC 256 (SHA256) EC 256 (SHA256)	TLS 1.3 TLS 1.0 TLS 1.2 TLS 1.2 TLS 1.2 TLS 1.2 TLS 1.3	TLS_AES_128_GCM_SHA256 ECDH secp256r1 FS TLS_AES_128_GCM_SHA256 ECDH secp256r1 FS TLS_RSA_WITH_AES_128_CBC_SHA No FS TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 ECDH x25519 FS
DenSSL 1.0.1 R DenSSL 1.0.1 R DenSSL 1.0.1 R DenSSL 1.0.1 R DenSSL 1.1.0 R DenSSL 1.1.0 R DenSSL 1.1.1 R	- RSA 2048 (SHA256) EC 256 (SHA256) EC 256 (SHA256) EC 256 (SHA256)	TLS 1.3 TLS 1.0 TLS 1.2 TLS 1.2 TLS 1.2 TLS 1.2 TLS 1.3	TLS_AES_128_GCM_SHA256 ECDH secp256r1 FS TLS_AES_128_GCM_SHA256 ECDH secp256r1 FS TLS_RSA_WITH_AES_128_CBC_SHA No FS TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 ECDH x25519 FS TLS_AES_256_GCM_SHA384 ECDH x25519 FS
DenSSL 0.9.8y DenSSL 1.0.11 R DenSSL 1.0.2s R DenSSL 1.1.0k R DenSSL 1.1.1c R Safari 6.10S 6.0.1	- RSA 2048 (SHA256) EC 256 (SHA256) EC 256 (SHA256) EC 256 (SHA256) - RSA 2048 (SHA256)	TLS 1.3 TLS 1.0 TLS 1.2 TLS 1.2 TLS 1.2 TLS 1.2 TLS 1.2 TLS 1.3 TLS 1.3	TLS_AES_128_GCM_SHA256 ECDH secp256r1 FS TLS_AES_128_GCM_SHA256 ECDH secp256r1 FS TLS_RSA_WITH_AES_128_CBC_SHA No FS TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 ECDH x25519 FS TLS_AES_256_GCM_SHA384 ECDH x25519 FS TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
DpenSSL 0.9.8y DpenSSL 1.0.11 R DpenSSL 1.0.2s R DpenSSL 1.1.0k R DpenSSL 1.1.1c R Safari 5.1.9 / OS X 10.6.8 Safari 6 / iOS 6.0.1 Safari 6.0.4 / OS X 10.8.4 R	- RSA 2048 (SHA256) EC 256 (SHA256) EC 256 (SHA256) EC 256 (SHA256) - RSA 2048 (SHA256) EC 256 (SHA256)	TLS 1.3 TLS 1.0 TLS 1.2 TLS 1.2 TLS 1.2 TLS 1.2 TLS 1.2 TLS 1.3 TLS 1.0 TLS 1.0	TLS_AES_128_GCM_SHA256 ECDH secp256r1 FS TLS_AES_128_GCM_SHA256 ECDH secp256r1 FS TLS_RSA_WITH_AES_128_CBC_SHA No FS TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 ECDH x25519 FS TLS_AES_256_GCM_SHA384 ECDH x25519 FS TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
DenSSL 0.9.8y DenSSL 1.0.1I R DenSSL 1.0.2s R DenSSL 1.1.0k R DenSSL 1.1.1c R Safari 5.1.9 / OS X 10.6.8 Safari 6.0.4 / OS X 10.8.4 R Safari 7 / iOS 7.1 R	- RSA 2048 (SHA256) EC 256 (SHA256) EC 256 (SHA256) EC 256 (SHA256) - RSA 2048 (SHA256) EC 256 (SHA256) EC 256 (SHA256) EC 256 (SHA256)	TLS 1.3 TLS 1.0 TLS 1.2 TLS 1.2 TLS 1.2 TLS 1.2 TLS 1.2 TLS 1.3 TLS 1.0 TLS 1.2 TLS 1.2	TLS_AES_128_GCM_SHA256 ECDH secp256r1 FS TLS_AES_128_GCM_SHA256 ECDH secp256r1 FS TLS_RSA_WITH_AES_128_CBC_SHA No FS TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 ECDH x25519 FS TLS_AES_256_GCM_SHA384 ECDH x25519 FS TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Dava 11.0.3 Java 12.0.1 OpenSSL 0.9.8y OpenSSL 1.0.1 R OpenSSL 1.0.2s R OpenSSL 1.1.0k R OpenSSL 1.1.1c R Safari 5.1.9 / OS X 10.6.8 Safari 6 / iOS 6.0.1 Safari 6.0.4 / OS X 10.8.4 R Safari 7 / iOS 7.1 R Safari 7 / iOS 7.1 R	- RSA 2048 (SHA256) EC 256 (SHA256) EC 256 (SHA256) - RSA 2048 (SHA256) EC 256 (SHA256)	TLS 1.3 TLS 1.0 TLS 1.2 TLS 1.2 TLS 1.2 TLS 1.2 TLS 1.2 TLS 1.3 TLS 1.0 TLS 1.2 TLS 1.2 TLS 1.2	TLS_AES_128_GCM_SHA256 ECDH secp256r1 FS TLS_AES_128_GCM_SHA256 ECDH secp256r1 FS TLS_RSA_WITH_AES_128_CBC_SHA No FS TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 ECDH x25519 FS TLS_AES_256_GCM_SHA384 ECDH x25519 FS TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Dava 11.0.3 Java 12.0.1 OpenSSL 0.9.8y OpenSSL 1.0.1I R OpenSSL 1.0.2s R OpenSSL 1.1.0k R OpenSSL 1.1.1c R Safari 5.1.9 / OS X 10.6.8 Safari 6 / iOS 6.0.1 Safari 6.0.4 / OS X 10.8.4 R Safari 7 / iOS 7.1 R Safari 7 / OS X 10.9 R Safari 8 / iOS 8.4 R	- RSA 2048 (SHA256) EC 256 (SHA256) EC 256 (SHA256) EC 256 (SHA256) - RSA 2048 (SHA256) EC 256 (SHA256)	TLS 1.3 TLS 1.0 TLS 1.2 TLS 1.2 TLS 1.2 TLS 1.2 TLS 1.2 TLS 1.3 TLS 1.0 TLS 1.2 TLS 1.0 TLS 1.2 TLS 1.0 TLS 1.2	TLS_AES_128_GCM_SHA256 ECDH secp256r1 FS TLS_AES_128_GCM_SHA256 ECDH secp256r1 FS TLS_RSA_WITH_AES_128_CBC_SHA No FS TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 ECDH x25519 FS TLS_AES_256_GCM_SHA384 ECDH x25519 FS TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Dava 11.0.3 Java 12.0.1 OpenSSL 0.9.8y OpenSSL 1.0.1I R OpenSSL 1.0.2s R OpenSSL 1.1.0k R OpenSSL 1.1.1c R Safari 5.1.9 / OS X 10.6.8 Safari 6 / iOS 6.0.1 Safari 6.0.4 / OS X 10.8.4 R Safari 7 / iOS 7.1 R Safari 7 / iOS 7.1 R Safari 8 / iOS 8.4 R Safari 8 / iOS 8.4 R	- RSA 2048 (SHA256) EC 256 (SHA256) EC 256 (SHA256) EC 256 (SHA256) - RSA 2048 (SHA256) EC 256 (SHA256)	TLS 1.3 TLS 1.0 TLS 1.2 TLS 1.2 TLS 1.2 TLS 1.2 TLS 1.2 TLS 1.3 TLS 1.0 TLS 1.2 TLS 1.2 TLS 1.2 TLS 1.2 TLS 1.2 TLS 1.2	TLS_AES_128_GCM_SHA256 ECDH secp256r1 FS TLS_AES_128_GCM_SHA256 ECDH secp256r1 FS TLS_RSA_WITH_AES_128_CBC_SHA No FS TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 ECDH x25519 FS TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Dava 11.0.3 Java 12.0.1 OpenSSL 0.9.8y OpenSSL 1.0.1I R OpenSSL 1.0.2s R OpenSSL 1.1.0k R OpenSSL 1.1.1c R Safari 5.1.9 / OS X 10.6.8 Safari 6 / iOS 6.0.1 Safari 6.0.4 / OS X 10.8.4 R Safari 7 / iOS 7.1 R Safari 7 / OS X 10.9 R Safari 8 / iOS 8.4 R	- RSA 2048 (SHA256) EC 256 (SHA256) EC 256 (SHA256) EC 256 (SHA256) - RSA 2048 (SHA256) EC 256 (SHA256)	TLS 1.3 TLS 1.0 TLS 1.2 TLS 1.2 TLS 1.2 TLS 1.2 TLS 1.2 TLS 1.3 TLS 1.0 TLS 1.2 TLS 1.0 TLS 1.2 TLS 1.0 TLS 1.2	TLS_AES_128_GCM_SHA256 ECDH secp256r1 FS TLS_AES_128_GCM_SHA256 ECDH secp256r1 FS TLS_RSA_WITH_AES_128_CBC_SHA No FS TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 ECDH x25519 FS TLS_AES_256_GCM_SHA384 ECDH x25519 FS TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS

Handshake Simulation Safari 10 / OS X 10.12 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS Safari 12.1.2 / MacOS 10.14.6 TLS 1.3 TLS_CHACHA20_POLY1305_SHA256 ECDH x25519 FS Beta R Safari 12.1.1 / iOS 12.3.1 R TLS 1.3 TLS_CHACHA20_POLY1305_SHA256 ECDH x25519 FS Apple ATS 9 / iOS 9 R EC 256 (SHA256) TLS 1.2 > h2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS Yahoo Slurp Jan 2015 EC 256 (SHA256) TLS 1.2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS YandexBot Jan 2015 EC 256 (SHA256) TLS 1.2 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS

Not simulated clients (Protocol mismatch)



IE 6 / XP No FS ¹ No SNI ²

Protocol mismatch (not simulated)

- (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.
- (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	
Secure Renegotiation	Supported
Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No
BEAST attack	Not mitigated server-side (more info) TLS 1.0: 0xc013
POODLE (SSLv3)	No, SSL 3 not supported (more info)
POODLE (TLS)	No (more info)
Zombie POODLE	No (more info) TLS 1.2: 0xc009
GOLDENDOODLE	No (more info) TLS 1.2: 0xc009
OpenSSL 0-Length	No (more info) TLS 1.2: 0xc009
Sleeping POODLE	No (more info) TLS 1.2: 0xc009
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	With modern browsers (more info)
ALPN	Yes h2 http/1.1
NPN	Yes h2 http/1.1
Session resumption (caching)	No (IDs assigned but not accepted)
Session resumption (tickets)	Yes
OCSP stapling	Yes
Strict Transport Security (HSTS)	No
HSTS Preloading	Not in: 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

Protocol Details DH public server param (Ys) reuse No, DHE suites not supported ECDH public server param reuse Supported Named Groups x25519, secp256r1, secp384r1, secp521r1 (server preferred order) SSL 2 handshake compatibility No 0-RTT enabled No + **HTTP Requests** 1 https://ourshopee.com/ (HTTP/1.1 301 Moved Permanently) Miscellaneous Test date Sun, 07 Jul 2024 10:29:23 UTC Test duration 109.918 seconds HTTP status code 301 HTTP forwarding https://www.ourshopee.com HTTP server signature cloudflare Server hostname

SSL Report v2.3.0

Copyright © 2009-2024 Qualys, Inc. All Rights Reserved. Privacy Policy.

Terms and Conditions

<u>Try Qualys for free!</u> Experience the award-winning <u>Qualys Cloud Platform</u> and the entire collection of <u>Qualys Cloud Apps</u>, including <u>certificate security</u> solutions.