



You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > [buyabans.com](#) > 104.26.15.207

SSL Report: [buyabans.com](#) (104.26.15.207)

Assessed on: Mon, 27 Mar 2023 09:38:28 UTC | [Hide](#) | [Clear cache](#)

[Scan Another »](#)

Summary

Overall Rating

B

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)



Server Key and Certificate #1

Subject	*.buyabans.com
	Fingerprint SHA256: 7667e00482ecb5ed2de03dfe63238a7076416772a25577d406c557ac31b5b782
	Pin SHA256: h/KRmGBF6E9AyZkzrX4fqTM7NK1Qx8T8IXhT8z1Lv6k=
Common names	*.buyabans.com
Alternative names	*.buyabans.com buyabans.com
Serial Number	00b611ec3b9c1e75670e4c700e7e54b1c5
Valid from	Mon, 27 Feb 2023 11:38:05 UTC
Valid until	Sun, 28 May 2023 11:38:04 UTC (expires in 2 months and 1 day)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	GTS CA 1P5 AIA: http://pki.goog/repo/certs/gts1p5.der
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	CRL, OCSP CRL: http://crls.pki.goog/gts1p5/QCTFvWRh6mE.crl OCSP: http://ocsp.pki.goog/s/gts1p5/AzsOXF4yWRY
Revocation status	Good (not revoked)
DNS CAA	Yes policy host: buyabans.com issue: comodoca.com flags:0 issue: digicert.com; cansignhttpexchanges=yes flags:0 issue: letsencrypt.org flags:0 issue: pki.goog; cansignhttpexchanges=yes flags:0 issuewild: comodoca.com flags:0 issuewild: digicert.com; cansignhttpexchanges=yes flags:0 issuewild: letsencrypt.org flags:0 issuewild: pki.goog; cansignhttpexchanges=yes flags:0
Trusted	Yes Mozilla Apple Android Java Windows




Additional Certificates (if supplied)

Certificates provided	3 (4201 bytes)
Chain issues	None
#2	
	GTS CA 1P5
Subject	Fingerprint SHA256: 97d42003e132552946097f20ef956f5b1cd570aa4372d780033a65efbe69758d Pin SHA256: 81Wf12bcLIFHQAfJluxnzZ6Frg+oJ9PWY/Wrwur8viQ=

Additional Certificates (if supplied)


Valid until	Thu, 30 Sep 2027 00:00:42 UTC (expires in 4 years and 6 months)
Key	RSA 2048 bits (e 65537)
Issuer	GTS Root R1
Signature algorithm	SHA256withRSA
#3	
Subject	GTS Root R1 Fingerprint SHA256: 3ee0278d771fa3c125c4cd487f01d774694e6fc57e0cd94c24efd769133918e5 Pin SHA256: hxqRIPTu1bMS/0DITB1SSu0vd4u/8l8TjPgfaAp63Gc=
Valid until	Fri, 28 Jan 2028 00:00:42 UTC (expires in 4 years and 10 months)
Key	RSA 4096 bits (e 65537)
Issuer	GlobalSign Root CA
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_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

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



Handshake Simulation

Android 2.3.7 No SNI² Server sent fatal alert: handshake_failure

Handshake Simulation

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	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Android 5.0.0	RSA 2048 (SHA256)	TLS 1.2	OLD_TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	ECDH secp256r1	FS
Android 6.0	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	OLD_TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	ECDH secp256r1	FS
Android 7.0	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	ECDH x25519	FS
Android 8.0	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_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 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1	FS
BingPreview Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Chrome 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Chrome 69 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_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	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Firefox 47 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Firefox 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Firefox 62 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_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	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH x25519	FS
IE 7 / Vista	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1	FS
IE 8 / XP No FS ¹ No SNI ²	Server sent fatal alert: handshake_failure				
IE 8-10 / Win 7 R	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1	FS
IE 11 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1	FS
IE 11 / Win 8.1 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1	FS
IE 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	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1	FS
IE 11 / Win Phone 8.1 Update R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1	FS
IE 11 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Edge 15 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH x25519	FS
Edge 16 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH x25519	FS
Edge 18 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH x25519	FS
Edge 13 / Win Phone 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Java 6u45 No SNI ²	Server sent fatal alert: handshake_failure				
Java 7u25	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1	FS
Java 8u161	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Java 11.0.3	-	TLS 1.3	TLS_AES_128_GCM_SHA256	ECDH secp256r1	FS
Java 12.0.1	-	TLS 1.3	TLS_AES_128_GCM_SHA256	ECDH secp256r1	FS
OpenSSL 0.9.8y	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA	No FS	
OpenSSL 1.0.1l R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
OpenSSL 1.0.2s R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
OpenSSL 1.1.0k R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	ECDH x25519	FS
OpenSSL 1.1.1c R	-	TLS 1.3	TLS_AES_256_GCM_SHA384	ECDH x25519	FS
Safari 5.1.9 / OS X 10.6.8	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1	FS
Safari 6 / iOS 6.0.1	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1	FS
Safari 6.0.4 / OS X 10.8.4 R	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1	FS
Safari 7 / iOS 7.1 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1	FS
Safari 7 / OS X 10.9 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1	FS
Safari 8 / iOS 8.4 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1	FS
Safari 8 / OS X 10.10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1	FS
Safari 9 / iOS 9 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Safari 9 / OS X 10.11 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Safari 10 / iOS 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Safari 10 / OS X 10.12 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Safari 12.1.2 / MacOS 10.14.6 Beta R	-	TLS 1.3	TLS_CHACHA20_POLY1305_SHA256	ECDH x25519	FS
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	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Yahoo Slurp Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
YandexBot Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_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.

Handshake Simulation

(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

	Unable to perform this test due to an internal error. (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 INTERNAL ERROR: connect timed out INTERNAL ERROR: connect timed out	
DROWN		
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 : 0xc013	
GOLDENDOODLE	No (more info) TLS 1.2 : 0xc013	
OpenSSL 0-Length	No (more info) TLS 1.2 : 0xc013	
Sleeping POODLE	No (more info) TLS 1.2 : 0xc013	
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)	Unknown	
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	x25519, secp256r1, secp384r1, secp521r1 (server preferred order)	
SSL 2 handshake compatibility	No	
0-RTT enabled	No	



HTTP Requests



1 https://buyabans.com/ (HTTP/1.1 200 OK)



Miscellaneous

Test date	Mon, 27 Mar 2023 09:22:17 UTC
Test duration	163.996 seconds
HTTP status code	200
HTTP server signature	cloudflare
Server hostname	-

