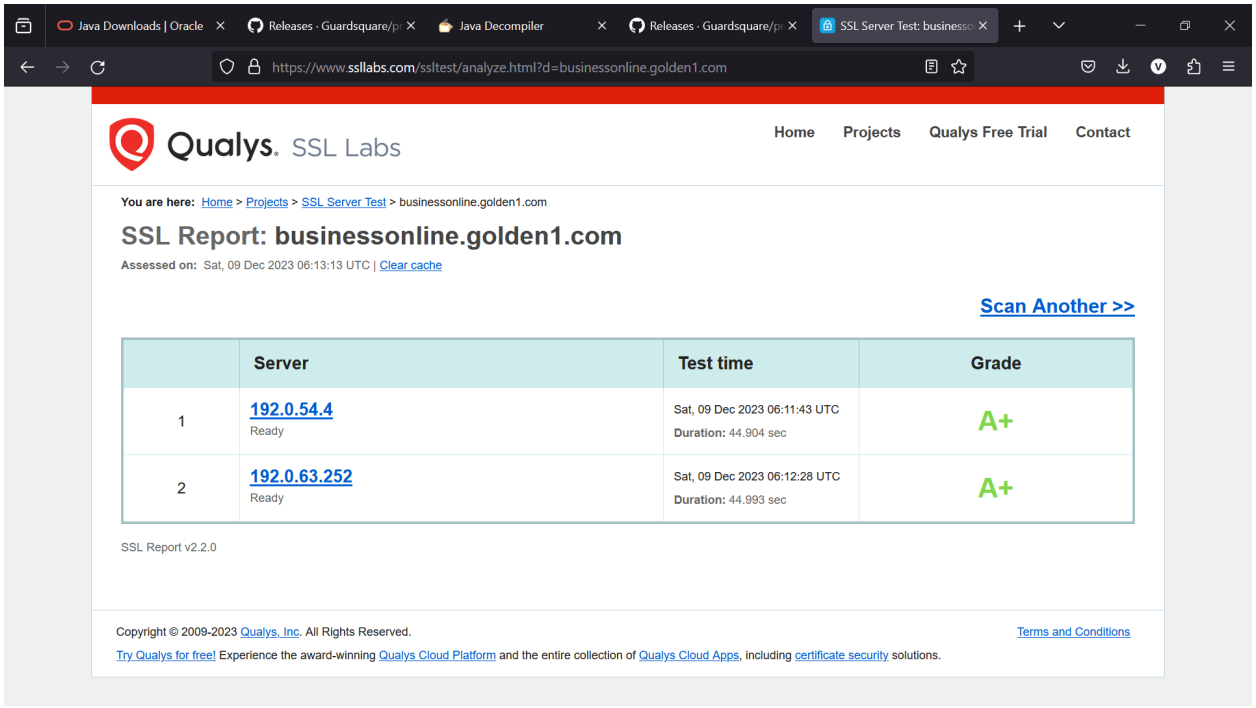
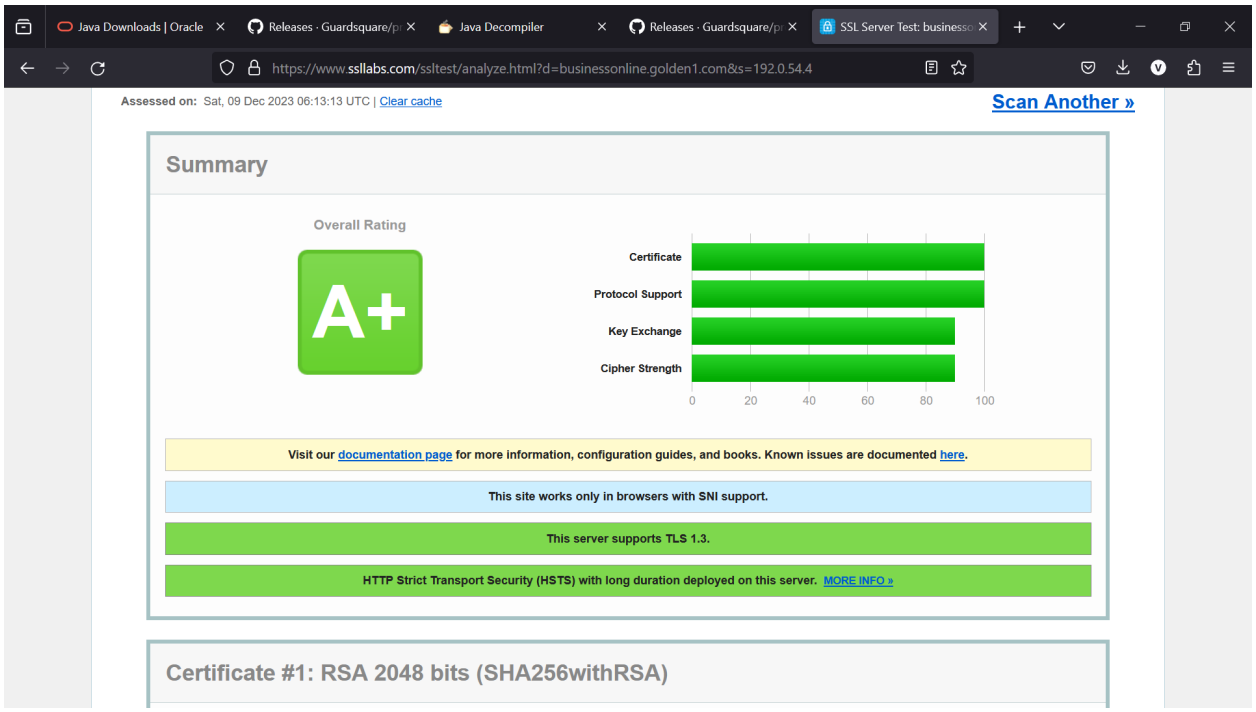
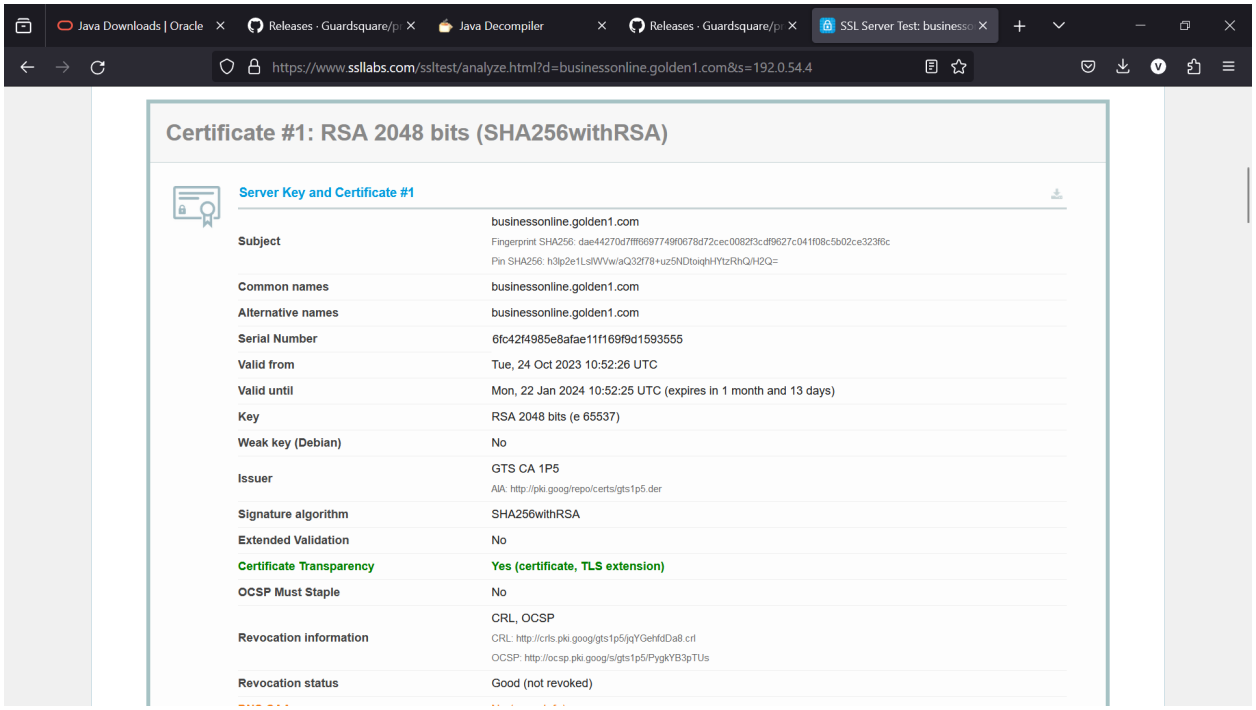

Java Downloads | Oracle
Releases · Guardsquare/p
Java Decompiler
Releases · Guardsquare/p
SSL Server Test: businesso
https://www.ssllabs.com/ssltest/analyze.html?d=businessonline.golden1.com
Qualys. SSL Labs
Home
Projects
Qualys Free Trial
Contact
You are here: Home > Projects > SSL Server Test > businessonline.golden1.com
SSL Report: businessonline.golden1.com
Assessed on: Sat, 09 Dec 2023 06:13:13 UTC | Clear cache
Scan Another >>
Server
Test time
Grade
1
192.0.54.4
Ready
Sat, 09 Dec 2023 06:11:43 UTC
Duration: 44.904 sec
A+
2
192.0.63.252
Ready
Sat, 09 Dec 2023 06:12:28 UTC
Duration: 44.993 sec
A+
SSL Report v2.2.0
Copyright © 2009-2023 Qualys, Inc. All Rights Reserved.
Terms and Conditions
Try Qualys for free! Experience the award-winning Qualys Cloud Platform and the entire collection of Qualys Cloud Apps, including certificate security solutions.

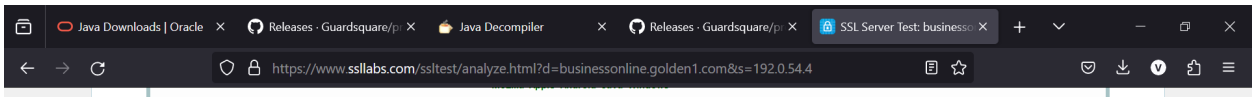

Java Downloads | Oracle
Releases · Guardsquare/p
Java Decompiler
Releases · Guardsquare/p
SSL Server Test: businesso
https://www.ssllabs.com/ssltest/analyze.html?d=businessonline.golden1.com&s=192.0.54.4
Assessed on: Sat, 09 Dec 2023 06:13:13 UTC | Clear cache
Scan Another »
Summary
Overall Rating
A+
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 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 server. MORE INFO »
Certificate #1: RSA 2048 bits (SHA256withRSA)



Certificate #1: RSA 2048 bits (SHA256withRSA)

Server Key and Certificate #1

Subject	businessonline.golden1.com Fingerprint SHA256: dae44270d7fff6697749f0678d72cec0082f3cdf9627c041f08c5b02ce323f6c Pin SHA256: h3lp2e1LslWVw/aQ32f78+uz5NDtoiqhHYtzRhQ/H2Q=
Common names	businessonline.golden1.com
Alternative names	businessonline.golden1.com
Serial Number	6fc42f4985e8afae11f169f9d1593555
Valid from	Tue, 24 Oct 2023 10:52:26 UTC
Valid until	Mon, 22 Jan 2024 10:52:25 UTC (expires in 1 month and 13 days)
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, TLS extension)
OCSP Must Staple	No
Revocation information	CRL, OCSP CRL: http://crls.pki.goog/gts1p5/jqYGehfdDa8.crl OCSP: http://ocsp.pki.goog/s/gts1p5/PygkYB3pTUs
Revocation status	Good (not revoked)



Additional Certificates (if supplied)

Certificates provided	3 (4208 bytes)
Chain issues	None

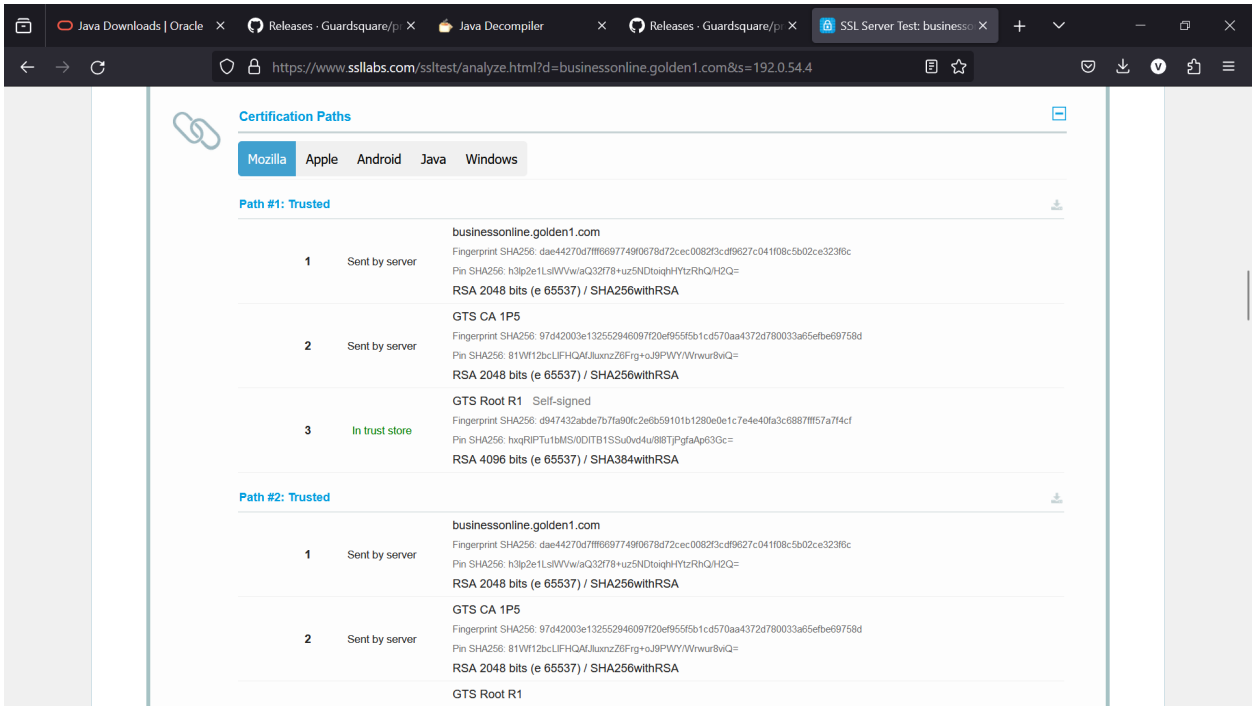
#2

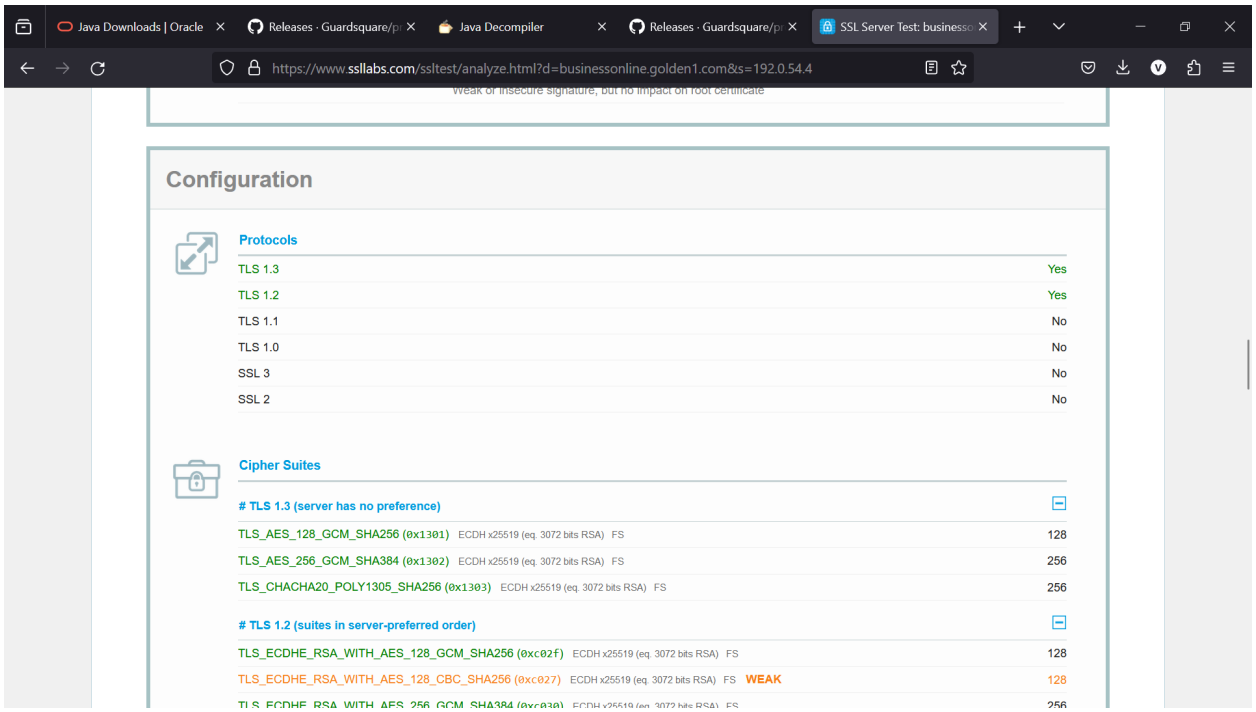
Subject	GTS CA 1P5 Fingerprint SHA256: 97d42003e132552946097f20ef955f5b1cd570aa4372d780033a65efbe69758d Pin SHA256: 81Wf12bcLIFHQAfJluxnzZ6Frg+oJ9PWY/Wrwur8viQ=
Valid until	Thu, 30 Sep 2027 00:00:42 UTC (expires in 3 years and 9 months)
Key	RSA 2048 bits (e 65537)
Issuer	GTS Root R1
Signature algorithm	SHA256withRSA

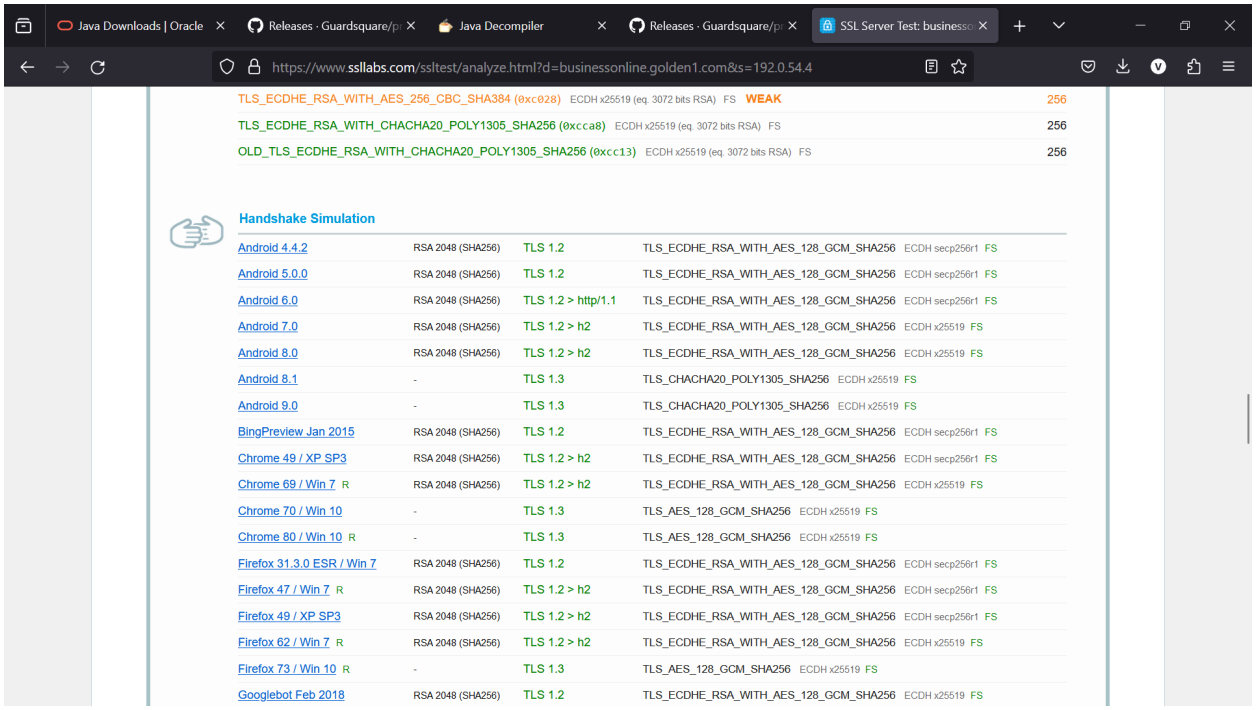
#3

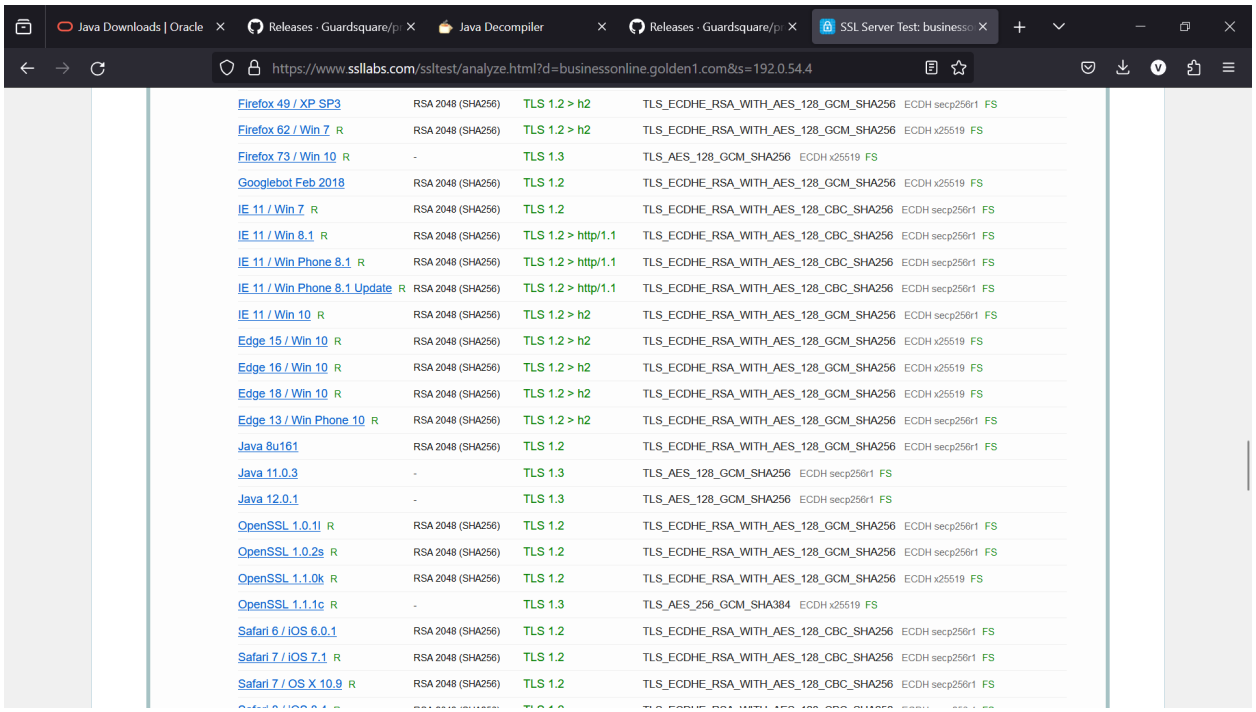
Subject	GTS Root R1 Fingerprint SHA256: 3ee0278df71fa3c125c4cd487f01d774694e6fc57e0cd94c24efd769133918e5 Pin SHA256: hxqRlPTu1bMS/0DITB1SSu0vd4u/8l8TjPgfaAp63Gc=
Valid until	Fri, 28 Jan 2028 00:00:42 UTC (expires in 4 years and 1 month)
Key	RSA 4096 bits (e 65537)
Issuer	GlobalSign Root CA
Signature algorithm	SHA256withRSA

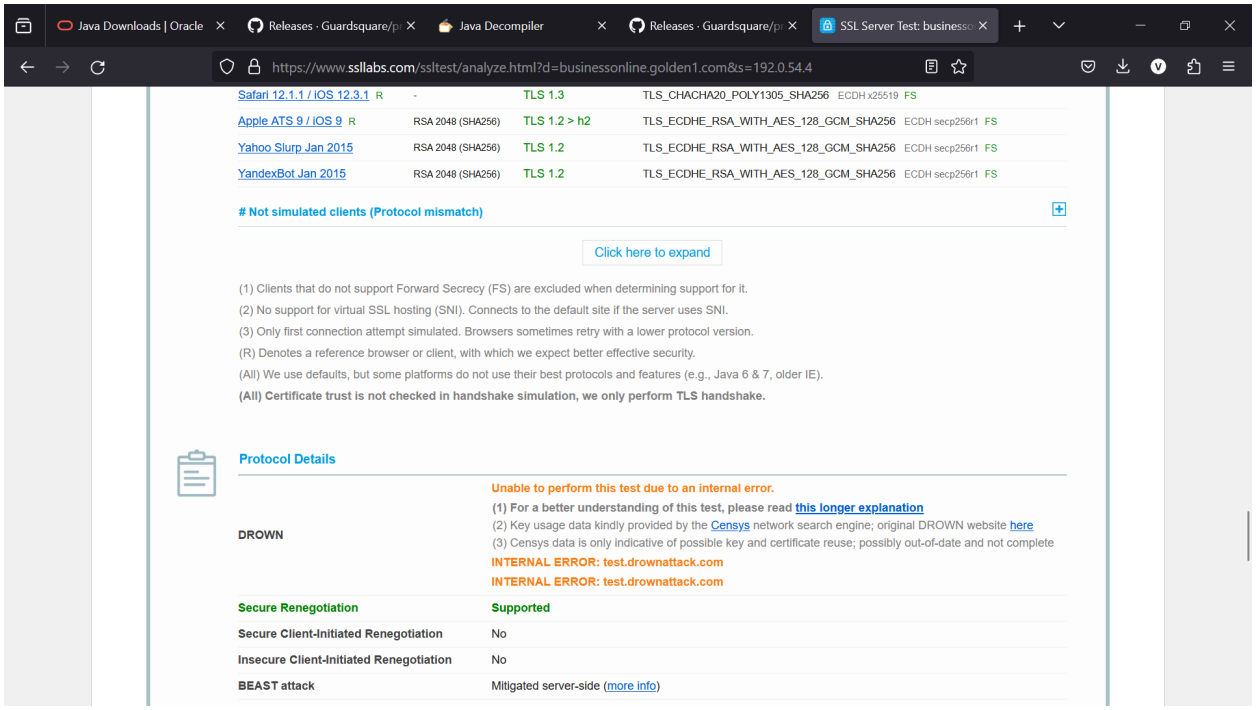
Certification Paths

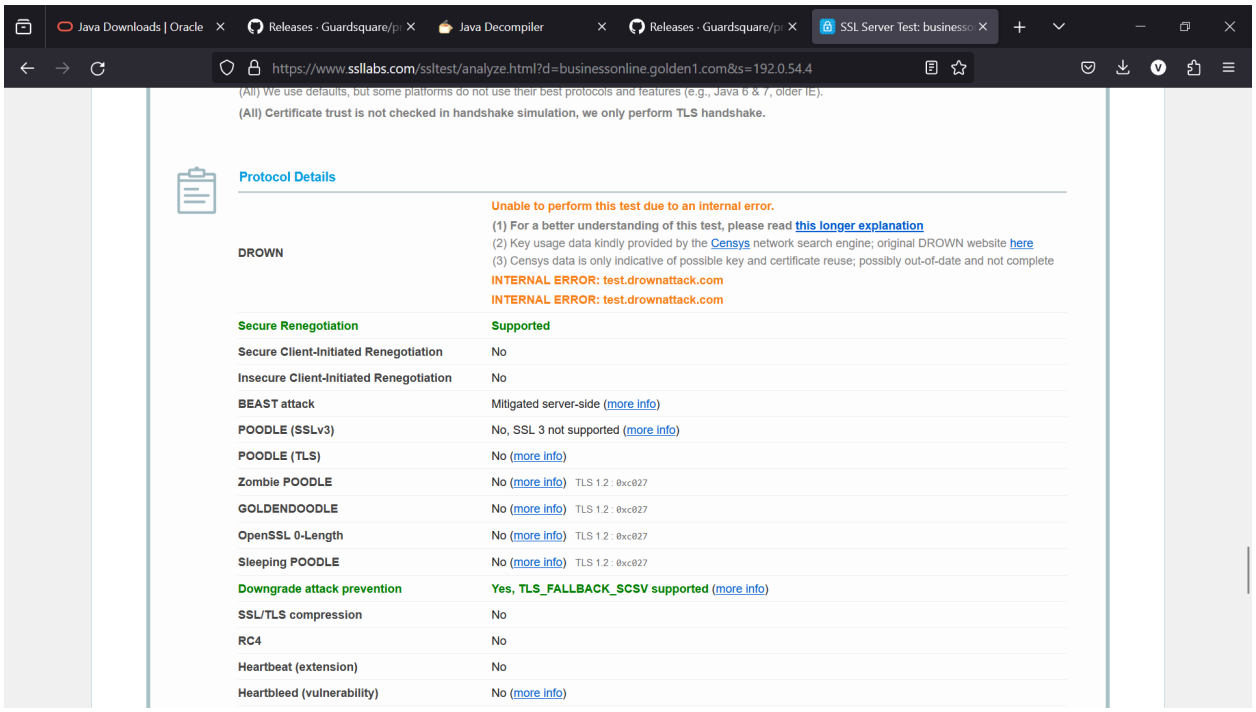

Java Downloads | Oracle
Releases · Guardsquare/pr
Java Decompiler
Releases · Guardsquare/pr
SSL Server Test: businesso
https://www.ssllabs.com/ssltest/analyze.html?d=businessonline.golden1.com&s=192.0.54.4
Certification Paths
Mozilla
Apple
Android
Java
Windows
Path #1: Trusted
1
Sent by server
businessonline.golden1.com
Fingerprint SHA256: dae44270d7fff6697749f0678d72cec0082f3cdf9627c041f08c5b02ce323f6c
Pin SHA256: h3lp2e1LslWVw/aQ32f78+uz5NDtoiqhHYtzRhQ/H2Q=
RSA 2048 bits (e 65537) / SHA256withRSA
2
Sent by server
GTS CA 1P5
Fingerprint SHA256: 97d42003e132552946097f20ef955f5b1cd570aa4372d780033a65efbe69758d
Pin SHA256: 81Wf12bcLIFHQAfJluxnzZ6Frg+oJ9PWY/Wrwur8viQ=
RSA 2048 bits (e 65537) / SHA256withRSA
3
In trust store
GTS Root R1 Self-signed
Fingerprint SHA256: d947432abde7b7fa90fc2e6b59101b1280e0e1c7e4e40fa3c6887fff57a7f4cf
Pin SHA256: hxqRlPTu1bMS/0DITB1SSu0vd4u/8l8TjPgfaAp63Gc=
RSA 4096 bits (e 65537) / SHA384withRSA
Path #2: Trusted
1
Sent by server
businessonline.golden1.com
Fingerprint SHA256: dae44270d7fff6697749f0678d72cec0082f3cdf9627c041f08c5b02ce323f6c
Pin SHA256: h3lp2e1LslWVw/aQ32f78+uz5NDtoiqhHYtzRhQ/H2Q=
RSA 2048 bits (e 65537) / SHA256withRSA
2
Sent by server
GTS CA 1P5
Fingerprint SHA256: 97d42003e132552946097f20ef955f5b1cd570aa4372d780033a65efbe69758d
Pin SHA256: 81Wf12bcLIFHQAfJluxnzZ6Frg+oJ9PWY/Wrwur8viQ=
RSA 2048 bits (e 65537) / SHA256withRSA
GTS Root R1

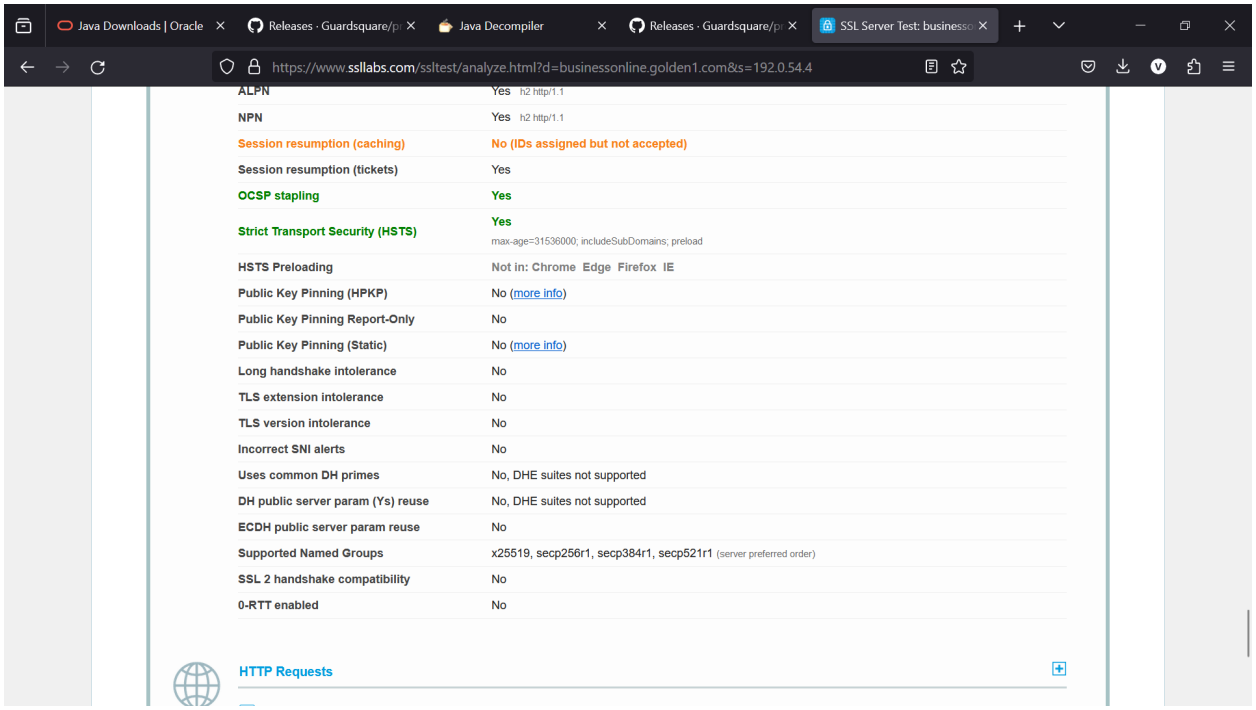

Java Downloads | Oracle
Releases · Guardsquare/pr
Java Decompiler
Releases · Guardsquare/pr
SSL Server Test: businesso
https://www.ssllabs.com/ssltest/analyze.html?d=businessonline.golden1.com&s=192.0.54.4
Weak or insecure signature, but no impact on root certificate
Configuration
Protocols
TLS 1.3 Yes
TLS 1.2 Yes
TLS 1.1 No
TLS 1.0 No
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
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ECDH x25519 (eq. 3072 bits RSA) FS WEAK 128
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ECDH x25519 (eq. 3072 bits RSA) FS 256

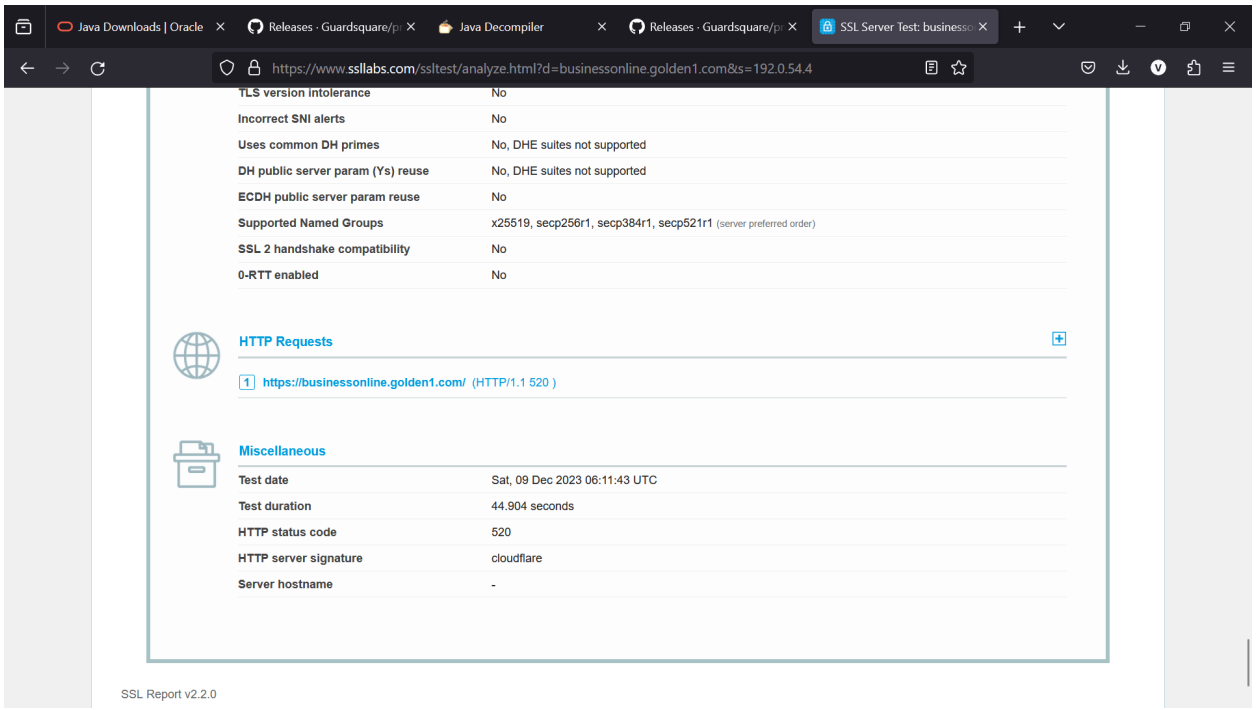

Java Downloads | Oracle
Releases · Guardsquare/pr
Java Decompiler
Releases · Guardsquare/pr
SSL Server Test: businesso
https://www.ssllabs.com/ssltest/analyze.html?d=businessonline.golden1.com&s=192.0.54.4
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ECDH x25519 (eq. 3072 bits RSA) FS WEAK 256
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8) ECDH x25519 (eq. 3072 bits RSA) FS 256
OLD_TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcc13) ECDH x25519 (eq. 3072 bits RSA) FS 256
Handshake Simulation
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 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Android 6.0 RSA 2048 (SHA256) TLS 1.2 > http/1.1 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Android 7.0 RSA 2048 (SHA256) TLS 1.2 > h2 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS
Android 8.0 RSA 2048 (SHA256) TLS 1.2 > h2 TLS_ECDHE_RSA_WITH_AES_128_GCM_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
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


Java Downloads | Oracle
Releases · Guardsquare/pr
Java Decompiler
Releases · Guardsquare/pr
SSL Server Test: businesso
https://www.ssllabs.com/ssltest/analyze.html?d=businessonline.golden1.com&s=192.0.54.4
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 11 / Win 7 R RSA 2048 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 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_SHA256 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_SHA256 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_SHA256 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 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 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_AES_128_GCM_SHA256 ECDH x25519 FS
OpenSSL 1.1.1c R - TLS 1.3 TLS_AES_256_GCM_SHA384 ECDH x25519 FS
Safari 6 / iOS 6.0.1 RSA 2048 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ECDH secp256r1 FS
Safari 7 / iOS 7.1 R RSA 2048 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ECDH secp256r1 FS
Safari 7 / OS X 10.9 R RSA 2048 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ECDH secp256r1 FS


Java Downloads | Oracle
Releases · Guardsquare/pr
Java Decompiler
Releases · Guardsquare/pr
SSL Server Test: businesso
https://www.ssllabs.com/ssltest/analyze.html?d=businessonline.golden1.com&s=192.0.54.4
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)
Click here to expand
(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
DROWN
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: test.drownattack.com
INTERNAL ERROR: test.drownattack.com
Secure Renegotiation
Supported
Secure Client-Initiated Renegotiation
No
Insecure Client-Initiated Renegotiation
No
BEAST attack
Mitigated server-side (more info)


Java Downloads | Oracle
Releases · Guardsquare/pr
Java Decompiler
Releases · Guardsquare/pr
SSL Server Test: businesso
https://www.ssllabs.com/ssltest/analyze.html?d=businessonline.golden1.com&s=192.0.54.4
(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
DROWN
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: test.drownattack.com
INTERNAL ERROR: test.drownattack.com
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)





SSL Report v2.2.0