Qualys. SSL Labs

Home Projects Qualys Free Trial Contact

**You are here:** Home > Projects > SSL Server Test > www.flowtraders.com

# SSL Report: www.flowtraders.com (83.217.84.138)

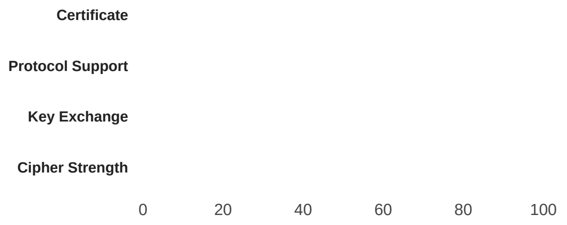
**Assessed on:** Mon, 18 Feb 2019 16:42:00 UTC | Hide | Clear cache

**Scan Another »**

## Summary

**Overall Rating**

A



**Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.**

**Renegotiation test has been disabled temporarily due to an Apache httpd 2.4.37 bug. MORE INFO »**

## Certificate #1: RSA 2048 bits (SHA256withRSA)

### Server Key and Certificate #1

| | |
|---|---|
| **Subject** | www.flowtraders.com<br>Fingerprint SHA256: b03185f78ebb513efca1569c38127aba0d9f9443545e17c0e391d098612d4e66<br>Pin SHA256: MyVQd8WDsF/n02IOBa/j7ZblfR765DYdr9cf3B3KaK4= |
| **Common names** | www.flowtraders.com |
| **Alternative names** | www.flowtraders.com flowtraders.com |
| **Serial Number** | 00b4074297a14557080a370378d58850a7 |
| **Valid from** | Fri, 18 Jan 2019 00:00:00 UTC |
| **Valid until** | Sat, 18 Jan 2020 23:59:59 UTC (expires in 11 months) |
| **Key** | RSA 2048 bits (e 65537) |
| **Weak key (Debian)** | No |
| **Issuer** | Sectigo RSA Domain Validation Secure Server CA<br>AIA: http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt |
| **Signature algorithm** | SHA256withRSA |
| **Extended Validation** | No |
| **Certificate Transparency** | **Yes (certificate)** |
| **OCSP Must Staple** | No |
| **Revocation information** | OCSP<br>OCSP: http://ocsp.sectigo.com |
| **Revocation status** | Good (not revoked) |
| **DNS CAA** | No (more info) |
| **Trusted** | **Yes**<br>**Mozilla Apple Android Java Windows** |

### Additional Certificates (if supplied)

| | |
|---|---|
| **Certificates provided** | 3 (4605 bytes) |
| **Chain issues** | **Contains anchor** |

**#2**

| | |
|---|---|
| **Subject** | Sectigo RSA Domain Validation Secure Server CA<br>Fingerprint SHA256: 7fa4ff68ec04a99d7528d5085f94907f4d1dd1c5381bacdc832ed5c960214676<br>Pin SHA256: 4a6cPehI7OG6cuDZka5NDZ7FR8a60d3auda+sKfg4Ng= |

### Additional Certificates (if supplied)

| | |
|---|---|
| Valid until | Tue, 31 Dec 2030 23:59:59 UTC (expires in 11 years and 10 months) |
| Key | RSA 2048 bits (e 65537) |
| Issuer | USERTrust RSA Certification Authority |
| Signature algorithm | SHA384withRSA |

#### #3

| | |
|---|---|
| Subject | USERTrust RSA Certification Authority In trust store<br>Fingerprint SHA256: e793c9b02fd8aa13e21c31228accb08119643b749c898964b1746d46c3d4cbd2<br>Pin SHA256: x4QzPSC810K5/cMjb05Qm4k3Bw5zBn4lTdO/nEW/Td4= |
| Valid until | Mon, 18 Jan 2038 23:59:59 UTC (expires in 18 years and 11 months) |
| Key | RSA 4096 bits (e 65537) |
| Issuer | USERTrust RSA Certification Authority Self-signed |
| Signature algorithm | SHA384withRSA |

### Certification Paths

Click here to expand

## Configuration

### Protocols

| | |
|---|---|
| TLS 1.3 | No |
| TLS 1.2 | Yes |
| TLS 1.1 | Yes |
| TLS 1.0 | Yes |
| SSL 3 | No |
| SSL 2 | No |

For TLS 1.3 tests, we only support RFC 8446.

### Cipher Suites

#### # TLS 1.2 (suites in server-preferred order)

| | |
|---|---|
| TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ECDH secp256r1 (eq. 3072 bits RSA) FS | 256 |
| TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ECDH secp256r1 (eq. 3072 bits RSA) FS | 128 |
| TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f) DH 2048 bits FS | 256 |
| TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e) DH 2048 bits FS | 128 |
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ECDH secp256r1 (eq. 3072 bits RSA) FS | 256 |
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ECDH secp256r1 (eq. 3072 bits RSA) FS | 128 |
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH secp256r1 (eq. 3072 bits RSA) FS | 256 |
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH secp256r1 (eq. 3072 bits RSA) FS | 128 |
| TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b) DH 2048 bits FS | 256 |
| TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67) DH 2048 bits FS | 128 |
| TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) DH 2048 bits FS | 256 |
| TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) DH 2048 bits FS | 128 |
| TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d) **WEAK** | 256 |
| TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c) **WEAK** | 128 |
| TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d) **WEAK** | 256 |
| TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c) **WEAK** | 128 |
| TLS_RSA_WITH_AES_256_CBC_SHA (0x35) **WEAK** | 256 |
| TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) **WEAK** | 128 |

#### # TLS 1.1 (suites in server-preferred order)

#### # TLS 1.0 (suites in server-preferred order)

### Handshake Simulation

| | | | | | |
|---|---|---|---|---|---|
| Android 2.3.7 No SNI [2] | RSA 2048 (SHA256) | TLS 1.0 | TLS_DHE_RSA_WITH_AES_128_CBC_SHA | DH 2048 | FS |
| Android 4.0.4 | RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA | ECDH secp256r1 | FS |
| Android 4.1.1 | RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA | ECDH secp256r1 | FS |
| Android 4.2.2 | RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA | ECDH secp256r1 | FS |
| Android 4.3 | RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA | ECDH secp256r1 | FS |
| Android 4.4.2 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | 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 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 | FS |
| Baidu Jan 2015 | RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA | ECDH secp256r1 | FS |
| BingPreview Jan 2015 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 | FS |
| Chrome 49 / XP SP3 | RSA 2048 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 | FS |
| Chrome 69 / Win 7 R | RSA 2048 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 | FS |
| Chrome 70 / Win 10 | RSA 2048 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 | 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 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 | FS |
| Firefox 49 / XP SP3 | RSA 2048 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 | FS |
| Firefox 62 / Win 7 R | RSA 2048 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 | FS |
| Googlebot Feb 2018 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 | FS |
| IE 7 / Vista | RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_256_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_256_CBC_SHA | ECDH secp256r1 | FS |
| IE 11 / Win 7 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 | DH 2048 | FS |
| IE 11 / Win 8.1 R | RSA 2048 (SHA256) | TLS 1.2 > http/1.1 | TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 | DH 2048 | FS |
| IE 10 / Win Phone 8.0 | RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_256_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_SHA256 | ECDH secp256r1 | FS |
| IE 11 / Win Phone 8.1 Update R | RSA 2048 (SHA256) | TLS 1.2 > http/1.1 | TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 | DH 2048 | FS |
| IE 11 / Win 10 R | RSA 2048 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 | FS |
| Edge 15 / Win 10 R | RSA 2048 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 | FS |
| Edge 13 / Win Phone 10 R | RSA 2048 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 | FS |
| Java 6u45 No SNI [2] | Client does not support DH parameters > 1024 bits<br>RSA 2048 (SHA256) \| TLS 1.0 \| TLS_DHE_RSA_WITH_AES_128_CBC_SHA \| DH 2048 | | | | |
| 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_256_GCM_SHA384 | ECDH secp256r1 | FS |
| OpenSSL 0.9.8y | RSA 2048 (SHA256) | TLS 1.0 | TLS_DHE_RSA_WITH_AES_256_CBC_SHA | DH 2048 | FS |
| OpenSSL 1.0.1l R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 | FS |
| OpenSSL 1.0.2e R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 | FS |
| Safari 5.1.9 / OS X 10.6.8 | RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA | ECDH secp256r1 | FS |
| Safari 6 / iOS 6.0.1 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 | ECDH secp256r1 | FS |
| Safari 6.0.4 / OS X 10.8.4 R | RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA | ECDH secp256r1 | FS |
| Safari 7 / iOS 7.1 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 | ECDH secp256r1 | FS |
| Safari 7 / OS X 10.9 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 | ECDH secp256r1 | FS |
| Safari 8 / iOS 8.4 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 | ECDH secp256r1 | FS |
| Safari 8 / OS X 10.10 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 | ECDH secp256r1 | FS |
| Safari 9 / iOS 9 R | RSA 2048 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 | FS |
| Safari 9 / OS X 10.11 R | RSA 2048 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 | FS |
| Safari 10 / iOS 10 R | RSA 2048 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 | FS |
| Safari 10 / OS X 10.12 R | RSA 2048 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 | FS |
| Apple ATS 9 / iOS 9 R | RSA 2048 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 | FS |
| Yahoo Slurp Jan 2015 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ECDH secp256r1 | FS |
| YandexBot Jan 2015 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | 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

| | |
|---|---|
| **DROWN** | No, server keys and hostname not seen elsewhere with SSLv2<br>**(1) For a better understanding of this test, please read this longer explanation**<br>(2) Key usage data kindly provided by the Censys network search engine; original DROWN website here<br>(3) Censys data is only indicative of possible key and certificate reuse; possibly out-of-date and not complete |
| **BEAST attack** | Not mitigated server-side (more info) TLS 1.0: 0xc014 |
| **POODLE (SSLv3)** | No, SSL 3 not supported (more info) |
| **POODLE (TLS)** | No (more info) |
| **Downgrade attack prevention** | **Yes, TLS_FALLBACK_SCSV supported** (more info) |
| **SSL/TLS compression** | No |
| **RC4** | No |
| **Heartbeat (extension)** | Yes |
| **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 http/1.1 |
| **NPN** | No |
| **Session resumption (caching)** | Yes |
| **Session resumption (tickets)** | Yes |
| **OCSP stapling** | No |
| **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 |
| **DH public server param (Ys) reuse** | No |
| **ECDH public server param reuse** | No |
| **Supported Named Groups** | secp256r1, secp521r1, brainpoolP512r1, brainpoolP384r1, secp384r1, brainpoolP256r1, secp256k1, sect571r1, sect571k1, sect409k1, sect409r1, sect283k1, sect283r1 (server preferred order) |
| **SSL 2 handshake compatibility** | Yes |

## HTTP Requests

1 **https://www.flowtraders.com/** (HTTP/1.1 200 OK)

## Miscellaneous

| | |
|---|---|
| **Test date** | Mon, 18 Feb 2019 16:39:42 UTC |
| **Test duration** | 138.447 seconds |
| **HTTP status code** | 200 |
| **HTTP server signature** | Apache |
| **Server hostname** | 83.217.84.138.static.hosted.by.combell.com |

SSL Report v1.32.16

Terms and Conditions