

Home Projects Qualys Free Trial Contact

You are here: <u>Home</u> > <u>Projects</u> > <u>SSL Server Test</u> > rubberduckiesftw.wpcomstaging.com

## SSL Report: rubberduckiesftw.wpcomstaging.com (192.0.78.20)

Assessed on: Sun, 01 Dec 2024 03:32:27 UTC | HIDDEN | 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 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 >> DNS Certification Authority Authorization (CAA) Policy found for this domain, MORE INFO >>

# Certificate #1: EC 256 bits (SHA384withECDSA)

wpcomstaging.com

OCSP: http://e5.o.lencr.org

Good (not revoked)

Yes

Server Key and Certificate #1



Subject

**OCSP Must Staple** 

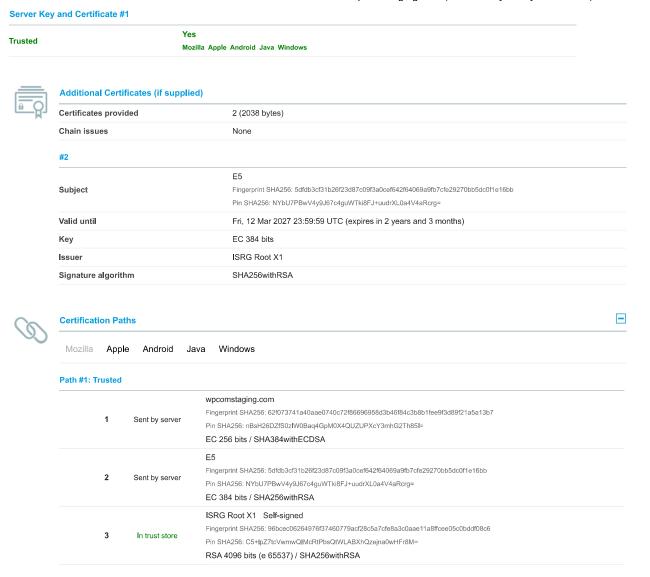
Revocation status

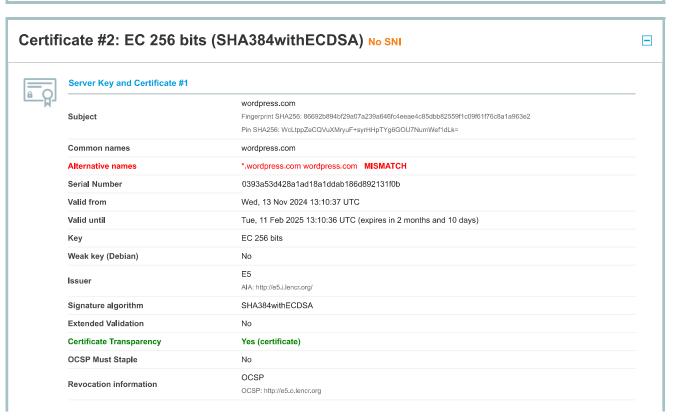
DNS CAA

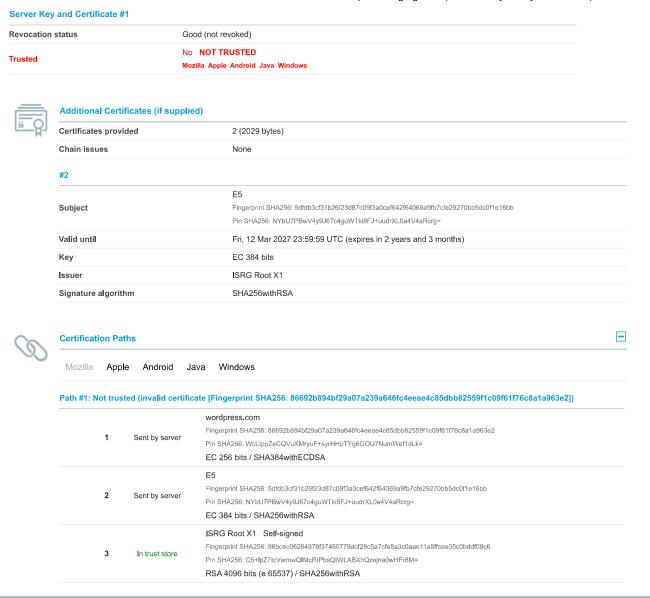
Revocation information

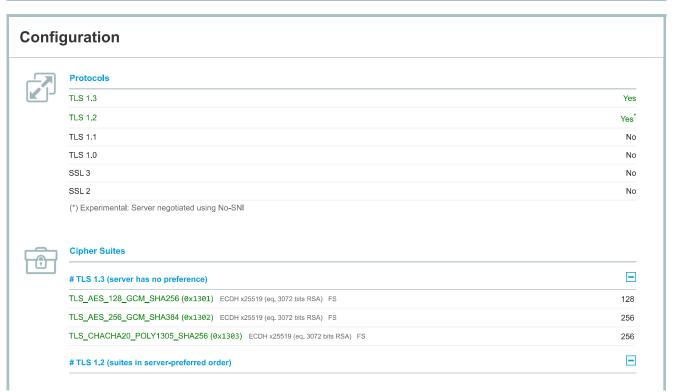
Certificate Transparency	Yes (certificate)		
Extended Validation	No		
Signature algorithm	SHA384withECDSA		
Issuer	E5 AIA: http://e5.i.lencr.org/		
Weak key (Debian)	No		
Key	EC 256 bits		
Valid until	Mon, 03 Feb 2025 01:25:39 UTC (expires in 2 months and 1 day)		
Valid from	Tue, 05 Nov 2024 01:25:40 UTC		
Serial Number	044339bee1dc7f03a059f2503666ef323e45		
Alternative names	*.wpcomstaging.com wpcomstaging.com		
Common names	wpcomstaging.com		
	Pin SHA256: nBsH26DZfS0zIW0Baq4GpM0X4QUZUPXcY3mhG2Th85I=		

Fingerprint SHA256: 62f073741a40aae0740c72f86696958d3b46f84c3b8b1fee9f3d89f21a5a13b7









### **Cipher Suites**

128
256 <sup>P</sup>
256
128
256

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



Handshake Simulation			
Android 4.4.2	EC 256 (SHA384)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Android 5.0.0	EC 256 (SHA384)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Android 6.0	EC 256 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Android 7.0	EC 256 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 ECDH x25519 FS
Android 8.0	EC 256 (SHA384)	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
BingPreview Jan 2015	EC 256 (SHA384)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Chrome 49 / XP SP3	Server sent fatal	alert: handshake_failu	ıre
Chrome 69 / Win 7 R	EC 256 (SHA384)	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 (SHA384)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Firefox 47 / Win 7 R	EC 256 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Firefox 49 / XP SP3	EC 256 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Firefox 62 / Win 7 R	EC 256 (SHA384)	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 (SHA384)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS
<u>IE 11 / Win 7</u> R	EC 256 (SHA384)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
<u>IE 11 / Win 8.1</u> R	EC 256 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
IE 11 / Win Phone 8.1 R	EC 256 (SHA384)	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 (SHA384)	TLS 1.2 > http/1.1	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
<u>IE 11 / Win 10</u> R	EC 256 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Edge 15 / Win 10 R	EC 256 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS
Edge 16 / Win 10 R	EC 256 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS
Edge 18 / Win 10 R	EC 256 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS
Edge 13 / Win Phone 10 R	EC 256 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
<u>Java 8u161</u>	EC 256 (SHA384)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
<u>Java 11.0.3</u>	-	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 1.0.1I R	EC 256 (SHA384)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
OpenSSL 1.0.2s R	EC 256 (SHA384)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
OpenSSL 1.1.0k R	EC 256 (SHA384)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_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	EC 256 (SHA384)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Safari 7 / iOS 7.1 R	EC 256 (SHA384)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
<u>Safari 7 / OS X 10.9</u> R	EC 256 (SHA384)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Safari 8 / iOS 8.4 R	EC 256 (SHA384)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Safari 8 / OS X 10.10 R	EC 256 (SHA384)	TLS 1.2	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Safari 9 / iOS 9 R	EC 256 (SHA384)	TLS 1,2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
<u>Safari 9 / OS X 10.11</u> R	EC 256 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Safari 10 / iOS 10 R	EC 256 (SHA384)	TLS 1.2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
<u>Safari 10 / OS X 10,12</u> R	EC 256 (SHA384)	TLS 1,2 > h2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS

**Handshake Simulation** 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 (SHA384) TLS 1.2 > h2 TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256 ECDH secp256r1 FS Yahoo Slurp Jan 2015 EC 256 (SHA384) TLS 1.2 TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256 ECDH secp256r1 FS YandexBot Jan 2015 EC 256 (SHA384) TLS 1.2 TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256 ECDH secp256r1 FS + # Not simulated clients (Protocol mismatch)

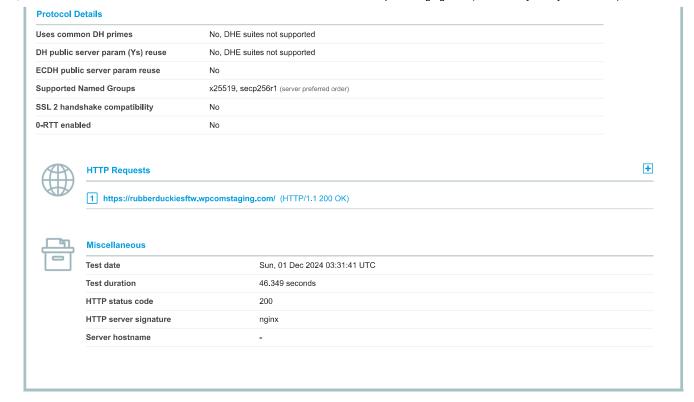
Click here to expand

- (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

Protocol Details				
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: 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 ( <u>more info</u> )			
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=31536000; includeSubDomains; preload			
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			



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.