Qualys

SSL Labs

Home

Projects

Qualys.com

Contact

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > softeng2.alexkearns.co.uk

SSL Report: softeng2.alexkearns.co.uk (178.62.77.181)

Assessed on: Wed, 14 Mar 2018 12:28:35 UTC | [Hide](#) | [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](#).

HTTP Strict Transport Security (HSTS) with long duration deployed on this server. [MORE INFO »](#)

Certificate #1: RSA 4096 bits (SHA256withRSA)

Server Key and Certificate #1

Subject	softeng2.alexkearns.co.uk Fingerprint SHA256: 4247372f1f47dc487bb2291129494c380a519d7c3716742ee86adab95077f953 Pin SHA256: ndrVpklllZoUQ1oVg4ltGqzvBS+Tn/0sTY7OjhV/0eU=
Common names	softeng2.alexkearns.co.uk
Alternative names	softeng2.alexkearns.co.uk
Serial Number	049e09adfdfcbbb1755fb8f43689956e8365
Valid from	Sat, 10 Mar 2018 15:57:14 UTC
Valid until	Fri, 08 Jun 2018 15:57:14 UTC (expires in 2 months and 25 days)
Key	RSA 4096 bits (e 65537)
Weak key (Debian)	No
Issuer	Let's Encrypt Authority X3 AIA: http://cert.int-x3.letsencrypt.org/
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	No
OCSP Must Staple	No
Revocation information	OCSP OCSP: http://ocsp.int-x3.letsencrypt.org
Revocation status	Good (not revoked)
DNS CAA	No (more info)
Trusted	Yes Mozilla Apple Android Java Windows

Additional Certificates (if supplied)

Certificates provided	2 (2735 bytes)
Chain issues	None

#2

	Let's Encrypt Authority X3
Subject	Fingerprint SHA256: 25847d668eb4f04fdd40b12b6b0740c567da7d024308eb6c2c96fe41d9de218d Pin SHA256: YLh1dUR9y6Kja30RrAn7JKnbQG/uEtLMkBgFF2Fuihg=

https://www.ssllabs.com/ssltest/analyze.html?d=softeng2.alexkearns.co.uk

1/6

Additional Certificates (if supplied)

Valid until	Wed, 17 Mar 2021 16:40:46 UTC (expires in 3 years)
Key	RSA 2048 bits (e 65537)
Issuer	DST Root CA X3
Signature algorithm	SHA256withRSA



Certification Paths



Mozilla Apple Android Java Windows

Path #1: Trusted

1	Sent by server	softeng2.alexkearns.co.uk Fingerprint SHA256: 4247372f1f47dc487bb2291129494c380a519d7c3716742ee86adab95077f953 Pin SHA256: ndtVpkliZoUQ1oVg4ltGqzvBS+Tn/0sTY7OjhV/OeU= RSA 4096 bits (e 65537) / SHA256withRSA
2	Sent by server	Let's Encrypt Authority X3 Fingerprint SHA256: 25847d668eb4f04fdd40b12b6b0740c567da7d024308eb6c2c96fe41d9de218d Pin SHA256: YLh1dUR9y6Kja30RrAn7JKnbQG/uEILMkBgFF2Fuihg= RSA 2048 bits (e 65537) / SHA256withRSA
3	In trust store	DST Root CA X3 Self-signed Fingerprint SHA256: 0687260331a72403d909f105e69bcf0d32e1bd2493ffc6d9206d11bcd6770739 Pin SHA256: Vjs8r4z+80wjNcr1YKepWQboSIRi63WswXhIMN+eWys= RSA 2048 bits (e 65537) / SHA1withRSA Weak or insecure signature, but no impact on root certificate

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 currently support draft version 18.



Cipher Suites

TLS 1.2 (suites in server-preferred order)



TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e)	DH 2048 bits FS	128
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f)	DH 2048 bits FS	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67)	DH 2048 bits FS	128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33)	DH 2048 bits FS	128
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b)	DH 2048 bits FS	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39)	DH 2048 bits FS	256
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c)	WEAK	128
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d)	WEAK	256
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c)	WEAK	128
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d)	WEAK	256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	WEAK	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	WEAK	256
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88)	DH 2048 bits FS	256

Cipher Suites

TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x84)	WEAK	256
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x45)	DH 2048 bits FS	128
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x41)	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 4096 (SHA256)	TLS 1.0	TLS_DHE_RSA_WITH_AES_128_CBC_SHA DH 2048 FS
Android 4.0.4		RSA 4096 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Android 4.1.1		RSA 4096 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Android 4.2.2		RSA 4096 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Android 4.3		RSA 4096 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Android 4.4.2		RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Android 5.0.0		RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Android 6.0		RSA 4096 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Android 7.0		RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Baidu Jan 2015		RSA 4096 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
BingPreview Jan 2015		RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Chrome 49 / XP SP3		RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Chrome 57 / Win 7	R	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Firefox 31.3.0 ESR / Win 7		RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Firefox 47 / Win 7	R	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Firefox 49 / XP SP3		RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Firefox 53 / Win 7	R	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Googlebot Feb 2018		RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
IE 7 / Vista		RSA 4096 (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 4096 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
IE 11 / Win 7	R	RSA 4096 (SHA256)	TLS 1.2	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 DH 2048 FS
IE 11 / Win 8.1	R	RSA 4096 (SHA256)	TLS 1.2 > http/1.1	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 DH 2048 FS
IE 10 / Win Phone 8.0		RSA 4096 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
IE 11 / Win Phone 8.1	R	RSA 4096 (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 4096 (SHA256)	TLS 1.2 > http/1.1	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 DH 2048 FS
IE 11 / Win 10	R	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Edge 15 / Win 10	R	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Edge 13 / Win Phone 10	R	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Java 6u45	No SNI ²	Client does not support DH parameters > 1024 bits		
		RSA 4096 (SHA256) TLS 1.0 TLS_DHE_RSA_WITH_AES_128_CBC_SHA DH 2048		
Java 7u25		RSA 4096 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Java 8u161		RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
OpenSSL 0.9.8y		RSA 4096 (SHA256)	TLS 1.0	TLS_DHE_RSA_WITH_AES_128_CBC_SHA DH 2048 FS
OpenSSL 1.0.1j	R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
OpenSSL 1.0.2e	R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Safari 5.1.9 / OS X 10.6.8		RSA 4096 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Safari 6 / iOS 6.0.1		RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ECDH secp256r1 FS
Safari 6.0.4 / OS X 10.8.4	R	RSA 4096 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS
Safari 7 / iOS 7.1	R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ECDH secp256r1 FS
Safari 7 / OS X 10.9	R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ECDH secp256r1 FS
Safari 8 / iOS 8.4	R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ECDH secp256r1 FS
Safari 8 / OS X 10.10	R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ECDH secp256r1 FS
Safari 9 / iOS 9	R	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Safari 9 / OS X 10.11	R	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Safari 10 / iOS 10	R	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS

Handshake Simulation

Safari 10 / OS X 10.12 R	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Apple ATS 9 / iOS 9 R	RSA 4096 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Yahoo Slurp Jan 2015	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
YandexBot Jan 2015	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS

Not simulated clients (Protocol mismatch)

[IE 6 / XP](#) No FS¹ No SNI² 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

DROWN	No, server keys and hostname not seen elsewhere with SSLv2 (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
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)
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 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	No
Strict Transport Security (HSTS)	Yes max-age=15552000; 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
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://softeng2.alexkearns.co.uk/> (HTTP/1.1 302 Found)

1	Content-Type	text/html; charset=UTF-8
	Transfer-Encoding	chunked
	Connection	close
	Cache-Control	no-cache, private
	Date	Wed, 14 Mar 2018 12:26:04 GMT
	Location	https://softeng2.alexkearns.co.uk/login
	Server	Feels bad
	Content-Security-Policy	base-uri 'none'; default-src; child-src 'none'; connect-src 'none'; font-src https://fonts.gstatic.com; form-action 'self'; frame-ancestors 'none'; img-src 'self' https://zoneofnonbeing.files.wordpress.com data:; media-src 'none'; object-src 'none'; script-src 'self' https://use.fontawesome.com/releases/v5.0.6/js/all.js; style-src 'self' https://fonts.googleapis.com/ 'unsafe-inline';
	Strict-Transport-Security	max-age=15552000; preload;
	X-Content-Type-Options	nosniff
	X-Download-Options	noopen
	X-Frame-Options	sameorigin
	X-Permitted-Cross-Domain-Policies	none
	X-XSS-Protection	1; mode=block;
	Referrer-Policy	same-origin
	Set-Cookie	XSRF-TOKEN=eyJpdil6llwNnZoYjZ0OGNkbUhhUkFIVnE5QnNnPT0iLCJ2YWx1ZSI6InZSaFpvejROdVJMSys3a2JlRXFDWmE4Z2ZrY21teGZhQTZLN01zTUhZN0Vjak1nSUEwaUNGNUdGOHhWOW9BYWVsVzBSb1h5NU16SUIVMktIT21jOHpBPT0iLCJtYWMiOiI1ZmYzODk3Y2M3ZTAzMdG1ODUyYjVmMzBkMjllM2YxYWEyYjk3NmUxNGlxZWZlOWZjZWZlNjFkMGZIMTQ3YzYxIn0%3D; expires=Wed, 14-Mar-2018 14:26:04 GMT; Max-Age=7200; path=/; secure
	Set-Cookie	music_forum_session=eyJpdil6llwNnZoYjZ0OGNkbUhhUkFIVnE5QnNnPT0iLCJ2YWx1ZSI6InZSaFpvejROdVJMSys3a2JlRXFDWmE4Z2ZrY21teGZhQTZLN01zTUhZN0Vjak1nSUEwaUNGNUdGOHhWOW9BYWVsVzBSb1h5NU16SUIVMktIT21jOHpBPT0iLCJtYWMiOiI1ZmYzODk3Y2M3ZTAzMdG1ODUyYjVmMzBkMjllM2YxYWEyYjk3NmUxNGlxZWZlOWZjZWZlNjFkMGZIMTQ3YzYxIn0%3D; expires=Wed, 14-Mar-2018 14:26:04 GMT; Max-Age=7200; path=/; secure; HttpOnly

2 <https://softeng2.alexkearns.co.uk/login> (HTTP/1.1 200 OK)

2	Content-Type	text/html; charset=UTF-8
	Transfer-Encoding	chunked
	Connection	close
	Vary	Accept-Encoding
	Cache-Control	no-cache, private
	Date	Wed, 14 Mar 2018 12:26:05 GMT
	Server	Feels bad
	Content-Security-Policy	base-uri 'none'; default-src; child-src 'none'; connect-src 'none'; font-src https://fonts.gstatic.com; form-action 'self'; frame-ancestors 'none'; img-src 'self' https://zoneofnonbeing.files.wordpress.com data:; media-src 'none'; object-src 'none'; script-src 'self' https://use.fontawesome.com/releases/v5.0.6/js/all.js; style-src 'self' https://fonts.googleapis.com/ 'unsafe-inline';
	Strict-Transport-Security	max-age=15552000; preload;
	X-Content-Type-Options	nosniff
	X-Download-Options	noopen
	X-Frame-Options	sameorigin
	X-Permitted-Cross-Domain-Policies	none
	X-XSS-Protection	1; mode=block;
	Referrer-Policy	same-origin
	Set-Cookie	XSRF-TOKEN=eyJpdil6llwNnZoYjZ0OGNkbUhhUkFIVnE5QnNnPT0iLCJ2YWx1ZSI6InZSaFpvejROdVJMSys3a2JlRXFDWmE4Z2ZrY21teGZhQTZLN01zTUhZN0Vjak1nSUEwaUNGNUdGOHhWOW9BYWVsVzBSb1h5NU16SUIVMktIT21jOHpBPT0iLCJtYWMiOiI1ZmYzODk3Y2M3ZTAzMdG1ODUyYjVmMzBkMjllM2YxYWEyYjk3NmUxNGlxZWZlOWZjZWZlNjFkMGZIMTQ3YzYxIn0%3D; expires=Wed, 14-Mar-2018 14:26:05 GMT; Max-Age=7200; path=/; secure

[2](#) <https://softeng2.alexkearns.co.uk/login> (HTTP/1.1 200 OK)

Set-Cookie

music_forum_session=eyJpdil6lkNRSVZISzNxNWRuempseW9MR2JwU1E9PSIsInZhbHVlIj
oib1VEckFubUQwWUUXTVBrRDZ1VUJ2Qkl1SkxZRWlUQjhBMkhxbEdMV0w4TXRJK0RuY
UVJZTNQcXBQZ0FXc3ZjcGEV1d5ZkNRZzQ3amVobmw3aUN3NkE9PSIsIm1hYyI6IjAxNz
UxMzQ5NTc4OTMwNmUwNjY3N2UzYzY0MmU0NWZmOTIiYzRkMzA3YzRmMDFinmE2M
2RIYzAyMzQxMjVmYzYifQ%3D%3D; expires=Wed, 14-Mar-2018 14:26:05 GMT; Max-
Age=7200; path=/; secure; HttpOnly



Miscellaneous

Test date	Wed, 14 Mar 2018 12:25:57 UTC
Test duration	157.606 seconds
HTTP status code	200
HTTP server signature	Feels bad
Server hostname	-

SSL Report v1.31.0