

HomeProjectsQualys.comContact

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > [web.mit.edu](#) > 2600:1408:10:184:0:0:0:255e

# SSL Report: [web.mit.edu](#) (2600:1408:10:184:0:0:0:255e)

Assessed on: Thu, 22 Feb 2018 22:06:57 UTC | [Hide](#) | [Clear cache](#)

[Scan Another »](#)

## Summary

Overall Rating

A

Certificate

Protocol Support


Key Exchange

Cipher Strength

020406080100


Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

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



Server Key and Certificate #1

Subject	web.mit.edu Fingerprint SHA256: 45dadd06f6a807587e424ad27f144ed4ef01d8b068da64b029d4f44bcf013c08 Pin SHA256: vuDij8ANZW9IDHqY5aTbsi/88t5sq71JxWmltnFd1ww=
Common names	web.mit.edu
Alternative names	web.mit.edu img.mit.edu alum-dev.mit.edu mit.edu betterworld.mit.edu giving.mit.edu news.mit.edu emergency.mit.net w3.mit.edu w.mit.edu www.mit.edu web-forms.mit.edu www.web.mit.edu newsoffice.mit.edu alum.mit.edu www.mit.edu emergency-dev.mit.edu www.newsoffice.mit.edu emergency.mit.edu www-mit.mit.edu swartz-report.mit.edu swartz-documents.mit.edu events-static.mit.edu mit.mit.edu
Serial Number	0e1bf1286b6c9a8c012586d7a80c404f
Valid from	Wed, 21 Feb 2018 00:00:00 UTC
Valid until	Mon, 30 Jul 2018 12:00:00 UTC (expires in 5 months and 7 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	GeoTrust RSA CA 2018 AIA: http://cacerts.geotrust.com/GeoTrustRSACA2018.crt
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	CRL, OCSP CRL: http://cdp.geotrust.com/GeoTrustRSACA2018.crl OCSP: http://status.geotrust.com
Revocation status	Good (not revoked)
DNS CAA	No (more info)
Trusted	Yes Mozilla Apple Android Java Windows



Additional Certificates (if supplied)

Certificates provided	2 (3123 bytes)
Chain issues	None

#2

https://www.ssllabs.com/ssltest/analyze.html?d=web.mit.edu&s=2600%3a1408%3a10%3a184%3a0%3a0%3a0%3a255e

1/4

Additional Certificates (if supplied)

GeoTrust RSA CA 2018	
Subject	Fingerprint SHA256: 8cc34e11c167045824ade61c4907a6440edb2c4398e99c112a859d661f8e2bc7 Pin SHA256: zUlrARNo+4JoAYA7ROeWjARtIoN4rIEbCpfCRQT6N6A=
Valid until	Sat, 06 Nov 2027 12:23:45 UTC (expires in 9 years and 8 months)
Key	RSA 2048 bits (e 65537)
Issuer	DigiCert Global Root CA
Signature algorithm	SHA256withRSA



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 currently support draft version 18.



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_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256 <sup>P</sup>	
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_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)			

(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 SNI <sup>2</sup>	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA No 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

Handshake Simulation

<a href="#">Android 7.0</a>	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	ECDH secp256r1	FS
<a href="#">Baidu Jan 2015</a>	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS
<a href="#">BingPreview Jan 2015</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
<a href="#">Chrome 49 / XP SP3</a>	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Chrome 57 / Win 7</a> R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
<a href="#">Firefox 31.3.0 ESR / Win 7</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Firefox 47 / Win 7</a> R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">Firefox 49 / XP SP3</a>	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
<a href="#">Firefox 53 / Win 7</a> R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
<a href="#">Googlebot Feb 2015</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">IE 7 / Vista</a>	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS
<a href="#">IE 8 / XP</a> No FS <sup>1</sup> No SNI <sup>2</sup>	Server sent fatal alert: handshake_failure				
<a href="#">IE 8-10 / Win 7</a> R	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS
<a href="#">IE 11 / Win 7</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS
<a href="#">IE 11 / Win 8.1</a> R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS
<a href="#">IE 10 / Win Phone 8.0</a>	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS
<a href="#">IE 11 / Win Phone 8.1</a> R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDH secp256r1	FS
<a href="#">IE 11 / Win Phone 8.1 Update</a> R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS
<a href="#">IE 11 / Win 10</a> R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
<a href="#">Edge 13 / Win 10</a> R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
<a href="#">Edge 13 / Win Phone 10</a> R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
<a href="#">Java 6u45</a> No SNI <sup>2</sup>	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA	No FS	
<a href="#">Java 7u25</a>	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1	FS
<a href="#">Java 8u31</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
<a href="#">OpenSSL 0.9.8y</a>	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA	No FS	
<a href="#">OpenSSL 1.0.1l</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
<a href="#">OpenSSL 1.0.2e</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
<a href="#">Safari 5.1.9 / OS X 10.6.8</a>	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS
<a href="#">Safari 6 / iOS 6.0.1</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS
<a href="#">Safari 6.0.4 / OS X 10.8.4</a> R	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS
<a href="#">Safari 7 / iOS 7.1</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS
<a href="#">Safari 7 / OS X 10.9</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS
<a href="#">Safari 8 / iOS 8.4</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS
<a href="#">Safari 8 / OS X 10.10</a> R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS
<a href="#">Safari 9 / iOS 9</a> R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
<a href="#">Safari 9 / OS X 10.11</a> R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
<a href="#">Safari 10 / iOS 10</a> R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
<a href="#">Safari 10 / OS X 10.12</a> R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
<a href="#">Apple ATS 9 / iOS 9</a> R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
<a href="#">Yahoo Slurp Jan 2015</a>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDH secp256r1	FS
<a href="#">YandexBot Jan 2015</a>	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<sup>1</sup> No SNI<sup>2</sup> 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 <a href="#">this longer explanation</a> (2) Key usage data kindly provided by the <a href="#">Censys</a> network search engine; original DROWN website <a href="#">here</a> (3) Censys data is only indicative of possible key and certificate reuse; possibly out-of-date and not complete
Secure Renegotiation	Supported

Protocol Details	
Secure Client-Initiated Renegotiation	Yes
Insecure Client-Initiated Renegotiation	No
BEAST attack	Not mitigated server-side ( <a href="#">more info</a> ) TLS 1.0: 0xc014
POODLE (SSLv3)	No, SSL 3 not supported ( <a href="#">more info</a> )
POODLE (TLS)	No ( <a href="#">more info</a> )
Downgrade attack prevention	Yes, TLS_FALLBACK_SCSV supported ( <a href="#">more info</a> )
SSL/TLS compression	No
RC4	No
Heartbeat (extension)	No
Heartbleed (vulnerability)	No ( <a href="#">more info</a> )
Ticketbleed (vulnerability)	No ( <a href="#">more info</a> )
OpenSSL CCS vuln. (CVE-2014-0224)	No ( <a href="#">more info</a> )
OpenSSL Padding Oracle vuln. (CVE-2016-2107)	No ( <a href="#">more info</a> )
ROBOT (vulnerability)	No ( <a href="#">more info</a> )
Forward Secrecy	With modern browsers ( <a href="#">more info</a> )
ALPN	Yes http/1.1
NPN	Yes http/1.1 http/1.0
Session resumption (caching)	Yes
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 ( <a href="#">more info</a> )
Public Key Pinning Report-Only	No
Public Key Pinning (Static)	No ( <a href="#">more info</a> )
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	secp256r1, x25519 (server preferred order)
SSL 2 handshake compatibility	Yes



HTTP Requests		<a href="#">+</a>
1	<a href="https://web.mit.edu/">https://web.mit.edu/</a> (HTTP/1.1 200 OK)	



Miscellaneous	
Test date	Thu, 22 Feb 2018 22:03:08 UTC
Test duration	108.837 seconds
HTTP status code	200
HTTP server signature	Apache/1.3.41 (Unix) mod_ssl/2.8.31 OpenSSL/0.9.8j
Server hostname	-