بررسی SLL دامنه shahroodkala.com

تهیه شده توسط سامانه آنلاین بررسی SSL دامنه وب سایت SSLLabs.ir

گزارش بررسی تنظیمات SSL دامنه shahroodkala.com

تاریخ تهیه گزارش : یکشنبه ۰۱ دی ۱۳۹۸ در ساعت ۲۳:۲۷
بازدید :0
امتیاز :

ارتباط تنها در SSL	معتبر	سازگاری مرورگرها	آسیب پذیری	HSTS
				

اطلاعات هدر دامنه

Server: nginx
Date: Sun, 22 Dec 2019 19:57:15 GMT
Content-Type: text/html; charset=iso-8859-1
Transfer-Encoding: chunked
Connection: keep-alive
Vary: Accept-Encoding
Content-Encoding: gzip

اطلاعات Shodan

Shodan Information :

SSL Certificate

- Issued By:
  - |- Common Name:Let's Encrypt Authority X3
  - |- Organization:Let's Encrypt
- Issued To:
  - |- Common Name:server37i.irwebspace.com

Supported SSL Versions

TLSv1.2

. OK Dovecot DA ready.+OK CAPA TOP UIDL RESP-CODES PIPELINING AUTH-RESP-CODE USER SASL PLAIN+
185.147.160.12
bcx.srv37.irwebspace.com
Asiatech Data Transfer Inc PLC
Added on 2019-12-13 23:43:01 GMT
Iran, Islamic Republic of
HTTP/1.1 302 Found Server: DirectAdmin Daemon Location: https://server37i.irwebspace.com:2222 x-use-https: yes Content-type: text/html use https
Forbidden 403
185.147.160.12
bcx.srv37.irwebspace.com
Asiatech Data Transfer Inc PLC
Added on 2019-12-21 21:21:18 GMT
Iran, Islamic Republic of
HTTP/1.1 403 Forbidden Server: nginx Date: Sat, 21 Dec 2019 21:16:35 GMT Content-Type: text/html Content-Length: 548 Connection: keep-alive Vary: Accept-Encoding
185.147.160.12
bcx.srv37.irwebspace.com

ارتباط تنها در SSL

//:http	http://shahroodkala.com/ -> 301 -> https://shahroodkala.com/ -> 200
//:https	https://shahroodkala.com/ -> 200

همیشه از HTTPS استفاده کنید

تغییر همه درخواست ها با پروتکل "http" به "https".

(HTTP Strict Transport Security (HSTS

اطلاعات بیشتر

HTTP Strict Transport Security (HSTS) : ارائه نشده است

اطلاعات امضای دیجیتال صادر شده

اطلاعات امضای دیجیتال شماره #1

عنوان امضای دیجیتال :	server37i.irwebspace.com
عنوان های جایگزین امضا (Alternative Names) :	ftp.server37i.irwebspace.com , mail.server37i.irwebspace.com , pop.server37i.irwebspace.com , server37i.irwebspace.com , smtp.server37i.irwebspace.com , www.server37i.irwebspace.com
شروع اعتبار از :	جمعه ۱۵ آذر ۱۳۹۸ در ساعت ۱۸:۱۳
پایان اعتبار تا :	پنجشنبه ۱۵ اسفند ۱۳۹۸ در ساعت ۱۸:۱۳ - **اتمام در :** 73 روز و 22 ساعت و 15 دقیقه و 49 ثانیه
صادر کننده مجوز :	Lets Encrypt Authority X3
کشور صادر کننده مجوز :	US - ایلات متحده (آمریکا)
الگوریتم امضا :	sha256 with RSA size: 4096 Bits
Certificate Transparency :	(yes (certificate extension
OCSP stapling :	LOW - not offered
OCSP URL :	http://ocsp.int-x3.letsencrypt.org
CRL Distribution Points :	--

Trust

Android iOS Java macOS Mozilla OPENJDK Windows

بررسی اعتبار دامنه :

بررسی اعتبار دامنه :

|___ **نام هاست دامنه :** shahroodkala.com

|___ **انطباق دامنه با امضای دیجیتال :** خیر

Path Validation :

#	Trust Store Version	Using Trust Store	Validation Result
1	r9_9.0.0	Android	ok
2	macOS 10.14, watchOS 5, and tvOS 12 ,12	iOS	ok
3	jdk-11.0.1	Java	ok
4	macOS 10.14, watchOS 5, and tvOS 12 ,12	macOS	ok
5	2018-11-22	Mozilla	ok
6	jdk-11.0.1	OPENJDK	ok
7	2018-12-08	Windows	ok

بررسی اعتبار امضای دیجیتال

امضا های دیجیتال تایید شده :

|___ **Sha1 پشتیبانی از امضای دیجیتال (Sha1 Signed Certificate):** خیر

|___ **Successful Trust Store:** Windows

|___ **لیست امضا های تایید شده:**

شماره 1 : nOvP0Jad2XS6UIL31hWFHY3mzEQSs96wih0S+sn0jVs=

Pin= : nOvP0Jad2XS6UIL31hWFHY3mzEQSs96wih0S+sn0jVs

Finger print : 6cc2c27f885eed53de9830d099832511d14a3ed4

عنوان : commonName=server37i.irwebspace.com

صادر کننده مجوز : countryName=US, organizationName=Lets Encrypt, commonName=Lets Encrypt Authority X3

سریال مجوز : 4.2266743855614E+41

شروع اعتبار از : 18:13:10 06-12-2019

پایان اعتبار تا : 18:13:10 05-03-2020

الگوریتم امضا : sha256

کلید عمومی : الگوریتم : RSA

کلید عمومی : نوع : 65537

کلید عمومی : اندازه : 4096

شماره 2 : YLh1dUR9y6Kja30RrAn7JKnbQG/uEtLMkBgFF2Fuihg=

Pin= : YLh1dUR9y6Kja30RrAn7JKnbQG/uEtLMkBgFF2Fuihg

Finger print : e6a3b45b062d509b3382282d196efe97d5956ccb

عنوان : countryName=US, organizationName=Lets Encrypt, commonName=Lets Encrypt Authority X3

صادر کننده مجوز : organizationName=Digital Signature Trust Co., commonName=DST Root CA X3

سریال مجوز : 1.3298795840391E+37

شروع اعتبار از : 16:40:46 17-03-2016

پایان اعتبار تا : 16:40:46 17-03-2021

الگوریتم امضا : sha256

کلید عمومی : الگوریتم : RSA

کلید عمومی : نوع : 65537

کلید عمومی : اندازه : 2048

شماره 3 : Vjs8r4z+80wjNcr1YKepWQboSlRi63WsWXhlMN+eWys=

Pin : Vjs8r4z+80wjNcr1YKepWQboSlRi63WsWXhlMN+eWys=

Finger print : dac9024f54d8f6df94935fb1732638ca6ad77c13

عنوان : organizationName=Digital Signature Trust Co., commonName=DST Root CA X3

صادر کننده مجوز : organizationName=Digital Signature Trust Co., commonName=DST Root CA X3

سریال مجوز : 9.129973557534E+37

شروع اعتبار از : 21:12:19 30-09-2000

پایان اعتبار تا : 14:01:15 30-09-2021

الگوریتم امضا : sha1

کلید عمومی : الگوریتم : RSA

کلید عمومی : نوع : 65537

کلید عمومی : اندازه : 2048

OCSP Stapling :
|___ پشتیبانی از OCSP : خیر
|___ OCSP Response : خیر
|___ |___ Trusted By Mozilla خیر
CA Store :
Deflate Compression : ندارد - Type : DEFLATE
Downgrade Attacks Prevention : دارد(TLS Fallback Scsv)
Session Renegotiation :
|___ Secure Renegotiation : بلی
|___ Insecure Client-Initiated خیر
Renegotiation :
Resumption Support :
|___ Resumption With TLS دارد
Tickets :
|___Resumption With Session دارد
IDs :
|___ تعداد کل تست های انجام شده : 5
|___ تست های موفقیت آمیز : 5
|___ تست های بدون پاسخ : 0
|___ تعداد خطا ها : 0

آسیب پذیری های امضای دیجیتال

Next Protocol Negotiation extension ((NPN) :	ارائه شده است (with h2, http/1.1 (advertised
Application-Layer Protocol Negotiation ((ALPN) :	http/1.1
Personal Financial Specialist (PFS™) : ارائه شده است	
PFS Ciphers :	TLS_AES_256_GCM_SHA384 TLS_CHACHA20_POLY1305_SHA256 ECDHE-RSA-AES256-GCM-SHA384 ECDHE-RSA-AES256-SHA384 ECDHE-RSA-AES256-SHA DHE-RSA-AES256-GCM-SHA384 DHE-RSA-AES256-CCM8 DHE-RSA-AES256-CCM DHE-RSA-AES256-SHA256 DHE-RSA-AES256-SHA ECDHE-RSA-CAMELLIA256-SHA384 DHE-RSA-CAMELLIA256-SHA256 DHE-RSA-CAMELLIA256-SHA TLS_AES_128_GCM_SHA256 ECDHE-RSA-AES128-GCM-SHA256 ECDHE-RSA-AES128-SHA256 ECDHE-RSA-AES128-SHA DHE-RSA-AES128-GCM-SHA256 DHE-RSA-AES128-CCM8 DHE-RSA-AES128-CCM DHE-RSA-AES128-SHA256 DHE-RSA-AES128-SHA ECDHE-RSA-CAMELLIA128-SHA256 DHE-RSA-CAMELLIA128-SHA256 DHE-RSA-CAMELLIA128-SHA
PFS ECDHE curves :	prime256v1 secp384r1 secp521r1 X25519 X448
DH Groups :	(Unknown DH group (2048 bits
Protocol Negotiated :	Default protocol TLS1.3
Cipher Negotiated :	(TLS_AES_256_GCM_SHA384, 253 bit ECDH (X25519
TLS Extensions :	renegotiation info/#65281 server name/#0 EC point formats/#11 session ticket/#35 next protocol/#13172 supported versions/#43 key share/#51 supported_groups/#10 max fragment length/#1 application layer protocol negotiation/#16 encrypt-then-mac/#22 extended master secret/#23
TLS Session Ticket :	(valid for 300 seconds only (< daily
SSL SessionID Support :	yes
Session Resumption Ticket :	پشتیبانی می کند
Session Resumption ID :	پشتیبانی می کند
TLS Timestamp :	random
DNS CAA Record :	--
Cert Transparency :	(yes (certificate extension
HTTP Status :	(/) OK 200
HTTP Strict Transport Security (HSTS) :	ارائه نشده است
Banner Server :	nginx
HTTP Public Key Pinning (HPKP) :	No support for HTTP Public Key Pinning
Cookie Count :	/ at 0
Heartbleed :	آسیب پذیر نیست , no heartbeat extension
Certified Coding Specialist (CCS) :	آسیب پذیر نیست
Ticketbleed :	آسیب پذیر نیست
CVE :	CVE-2016-9244
CWE :	CWE-200
ROBOT :	آسیب پذیر نیست
CVE :	CVE-2017-17382 CVE-2017-17427 CVE-2017-17428 CVE-2017-13098 CVE-2017-1000385 CVE-2017-13099 CVE-2016-6883 CVE-2012-5081 CVE-2017-6168
CWE :	CWE-203
Secure Renego :	آسیب پذیر نیست
CVE :	CVE-2009-3555
CWE :	CWE-310
Secure Client Renego :	آسیب پذیر نیست
CVE :	CVE-2009-3555
CWE :	CWE-310
Compression Ratio Info-leak Made Easy(CRIME) :	آسیب پذیر نیست
CVE :	CVE-2012-4929
CWE :	CWE-310
BREACH :	ممکن است آسیب پذیر باشد, uses gzip HTTP compression - only supplied / tested
CVE :	CVE-2013-3587
CWE :	CWE-310
Fallback SCSV :	پشتیبانی می کند
POODLE SSL :	آسیب پذیر نیست
CVE :	CWE-310

اطلاعات بیشتر

اطلاعات بیشتر

SWEET32 :	آسیب پذیر نیست
CVE : __|	CVE-2016-2183 CVE-2016-6329
CWE : __|	CWE-327
FREAK (Factoring RSA Export Keys) :	آسیب پذیر نیست اطلاعات بیشتر
DROWN (Decrypting RSA with Obsolete and Weakened eNcryption) :	Make sure you don t use this certificate elsewhere with SSLv2 enabled services, see https://censys.io/ipv4?q=D83DAAB5666F87B49DD80E6425238ED52019A4CB3A10561F293D4A370CCE9320 اطلاعات بیشتر
CVE : __|	CVE-2016-0800 CVE-2016-0703
CWE : __|	CWE-310
LOGJAM Common Primes :	-- اطلاعات بیشتر
CVE : __|	CVE-2015-4000
CWE : __|	CWE-310
LOGJAM :	آسیب پذیر نیست , no DH EXPORT ciphers, اطلاعات بیشتر
CVE : __|	CVE-2015-4000
CWE : __|	CWE-310
BEAST :	آسیب پذیر نیست , no SSL3 or TLS1 اطلاعات بیشتر
CVE : __|	CVE-2011-3389
CWE : __|	CWE-20
LUCKY 13 :	ممکن است آسیب پذیر باشد, uses TLS CBC ciphers
CVE : __|	CVE-2013-0169
CWE : __|	CWE-310
RC4 :	آسیب پذیر نیست اطلاعات بیشتر
CVE : __|	CWE-310

پشتیبانی از این پروتکل : خیر

Accepted Cipher Suites :

#	Name	Connection Status	Anonymous

Preferred Cipher Suites :

#	Name	Connection Status	Anonymous

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
1	SSL_CK_RC4_128_WITH_MD5	TLS / Unexpected EOF	خیر
2	SSL_CK_RC4_128_EXPORT40_WITH_MD5	TLS / Unexpected EOF	خیر
3	SSL_CK_RC2_128_CBC_WITH_MD5	TLS / Unexpected EOF	خیر
4	SSL_CK_RC2_128_CBC_EXPORT40_WITH_MD5	TLS / Unexpected EOF	خیر
5	SSL_CK_IDEA_128_CBC_WITH_MD5	TLS / Unexpected EOF	خیر
6	SSL_CK_DES_64_CBC_WITH_MD5	TLS / Unexpected EOF	خیر
7	SSL_CK_DES_192_EDE3_CBC_WITH_MD5	TLS / Unexpected EOF	خیر

پشتیبانی از این پروتکل : خیر

Accepted Cipher Suites :

#	Name	Connection Status	Anonymous

Preferred Cipher Suites :

#	Name	Connection Status	Anonymous

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
1	TLS_RSA_WITH_SEED_CBC_SHA	TLS / Alert: handshake failure	خیر
2	TLS_RSA_WITH_RC4_128_SHA	TLS / Alert: handshake failure	خیر
3	TLS_RSA_WITH_RC4_128_MD5	TLS / Alert: handshake failure	خیر
4	TLS_RSA_WITH_NULL_SHA256	TLS / No ciphers available	خیر
5	TLS_RSA_WITH_NULL_SHA	TLS / Alert: handshake failure	خیر
6	TLS_RSA_WITH_NULL_MD5	TLS / Alert: handshake failure	خیر
7	TLS_RSA_WITH_IDEA_CBC_SHA	TLS / Alert: handshake failure	خیر
8	TLS_RSA_WITH_DES_CBC_SHA	TLS / Alert: handshake failure	خیر
9	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	TLS / Alert: handshake failure	خیر
10	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	TLS / Alert: handshake failure	خیر
11	TLS_RSA_WITH_AES_256_GCM_SHA384	TLS / No ciphers available	خیر
12	TLS_RSA_WITH_AES_256_CBC_SHA256	TLS / No ciphers available	خیر
13	TLS_RSA_WITH_AES_256_CBC_SHA	TLS / Alert: handshake failure	خیر
14	TLS_RSA_WITH_AES_128_GCM_SHA256	TLS / No ciphers available	خیر
15	TLS_RSA_WITH_AES_128_CBC_SHA256	TLS / No ciphers available	خیر
16	TLS_RSA_WITH_AES_128_CBC_SHA	TLS / Alert: handshake failure	خیر
17	TLS_RSA_WITH_3DES_EDE_CBC_SHA	TLS / Alert: handshake failure	خیر
18	TLS_RSA_EXPORT_WITH_RC4_40_MD5	TLS / Alert: handshake failure	خیر

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
20	TLS_RSA_EXPORT_WITH_DES40_CBC_SHA	TLS / Alert: handshake failure	خیر
21	TLS_ECDH_anon_WITH_RC4_128_SHA	TLS / Alert: handshake failure	بلی
22	TLS_ECDH_anon_WITH_NULL_SHA	TLS / Alert: handshake failure	بلی
23	TLS_ECDH_anon_WITH_AES_256_CBC_SHA	TLS / Alert: handshake failure	بلی
24	TLS_ECDH_anon_WITH_AES_128_CBC_SHA	TLS / Alert: handshake failure	بلی
25	TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA	TLS / Alert: handshake failure	بلی
26	TLS_ECDH_RSA_WITH_RC4_128_SHA	TLS / Alert: handshake failure	خیر
27	TLS_ECDH_RSA_WITH_NULL_SHA	TLS / Alert: handshake failure	خیر
28	TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384	TLS / No ciphers available	خیر
29	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384	TLS / No ciphers available	خیر
30	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA	TLS / Alert: handshake failure	خیر
31	TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256	TLS / No ciphers available	خیر
32	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256	TLS / No ciphers available	خیر
33	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA	TLS / Alert: handshake failure	خیر
34	TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA	TLS / Alert: handshake failure	خیر
35	TLS_ECDH_ECDSA_WITH_RC4_128_SHA	TLS / Alert: handshake failure	خیر
36	TLS_ECDH_ECDSA_WITH_NULL_SHA	TLS / Alert: handshake failure	خیر
37	TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384	TLS / No ciphers available	خیر
38	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384	TLS / No ciphers available	خیر
39	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA	TLS / Alert: handshake failure	خیر

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
40	TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256	TLS / No ciphers available	خیر
41	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256	TLS / No ciphers available	خیر
42	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA	TLS / Alert: handshake failure	خیر
43	TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA	TLS / Alert: handshake failure	خیر
44	TLS_ECDHE_RSA_WITH_RC4_128_SHA	TLS / Alert: handshake failure	خیر
45	TLS_ECDHE_RSA_WITH_NULL_SHA	TLS / Alert: handshake failure	خیر
46	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	TLS / No ciphers available	خیر
47	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	TLS / No ciphers available	خیر
48	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	TLS / Alert: handshake failure	خیر
49	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	TLS / No ciphers available	خیر
50	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	TLS / No ciphers available	خیر
51	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	TLS / Alert: handshake failure	خیر
52	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	TLS / Alert: handshake failure	خیر
53	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA	TLS / Alert: handshake failure	خیر
54	TLS_ECDHE_ECDSA_WITH_NULL_SHA	TLS / Alert: handshake failure	خیر
55	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	TLS / No ciphers available	خیر
56	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	TLS / No ciphers available	خیر
57	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	TLS / Alert: handshake failure	خیر
58	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	TLS / No ciphers available	خیر
59	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	TLS / No ciphers available	خیر

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
60	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	TLS / Alert: handshake failure	خیر
61	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	TLS / Alert: handshake failure	خیر
62	TLS_DH_anon_WITH_SEED_CBC_SHA	TLS / Alert: handshake failure	بلی
63	TLS_DH_anon_WITH_RC4_128_MD5	TLS / Alert: handshake failure	بلی
64	TLS_DH_anon_WITH_DES_CBC_SHA	TLS / Alert: handshake failure	بلی
65	TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA	TLS / Alert: handshake failure	بلی
66	TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA	TLS / Alert: handshake failure	بلی
67	TLS_DH_anon_WITH_AES_256_GCM_SHA384	TLS / No ciphers available	بلی
68	TLS_DH_anon_WITH_AES_256_CBC_SHA256	TLS / No ciphers available	بلی
69	TLS_DH_anon_WITH_AES_256_CBC_SHA	TLS / Alert: handshake failure	بلی
70	TLS_DH_anon_WITH_AES_128_GCM_SHA256	TLS / No ciphers available	بلی
71	TLS_DH_anon_WITH_AES_128_CBC_SHA256	TLS / No ciphers available	بلی
72	TLS_DH_anon_WITH_AES_128_CBC_SHA	TLS / Alert: handshake failure	بلی
73	TLS_DH_anon_WITH_3DES_EDE_CBC_SHA	TLS / Alert: handshake failure	بلی
74	TLS_DH_anon_EXPORT_WITH_RC4_40_MD5	TLS / Alert: handshake failure	بلی
75	TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA	TLS / Alert: handshake failure	بلی
76	TLS_DH_RSA_WITH_SEED_CBC_SHA	TLS / Alert: handshake failure	خیر
77	TLS_DH_RSA_WITH_DES_CBC_SHA	TLS / Alert: handshake failure	خیر
78	TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA	TLS / Alert: handshake failure	خیر
79	TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA	TLS / Alert: handshake failure	خیر

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
80	TLS_DH_RSA_WITH_AES_256_GCM_SHA384	TLS / No ciphers available	خیر
81	TLS_DH_RSA_WITH_AES_256_CBC_SHA256	TLS / No ciphers available	خیر
82	TLS_DH_RSA_WITH_AES_256_CBC_SHA	TLS / Alert: handshake failure	خیر
83	TLS_DH_RSA_WITH_AES_128_GCM_SHA256	TLS / No ciphers available	خیر
84	TLS_DH_RSA_WITH_AES_128_CBC_SHA256	TLS / No ciphers available	خیر
85	TLS_DH_RSA_WITH_AES_128_CBC_SHA	TLS / Alert: handshake failure	خیر
86	TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA	TLS / Alert: handshake failure	خیر
87	TLS_DH_DSS_WITH_SEED_CBC_SHA	TLS / Alert: handshake failure	خیر
88	TLS_DH_DSS_WITH_DES_CBC_SHA	TLS / Alert: handshake failure	خیر
89	TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA	TLS / Alert: handshake failure	خیر
90	TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA	TLS / Alert: handshake failure	خیر
91	TLS_DH_DSS_WITH_AES_256_GCM_SHA384	TLS / No ciphers available	خیر
92	TLS_DH_DSS_WITH_AES_256_CBC_SHA256	TLS / No ciphers available	خیر
93	TLS_DH_DSS_WITH_AES_256_CBC_SHA	TLS / Alert: handshake failure	خیر
94	TLS_DH_DSS_WITH_AES_128_GCM_SHA256	TLS / No ciphers available	خیر
95	TLS_DH_DSS_WITH_AES_128_CBC_SHA256	TLS / No ciphers available	خیر
96	TLS_DH_DSS_WITH_AES_128_CBC_SHA	TLS / Alert: handshake failure	خیر
97	TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA	TLS / Alert: handshake failure	خیر
98	TLS_DHE_RSA_WITH_SEED_CBC_SHA	TLS / Alert: handshake failure	خیر
99	TLS_DHE_RSA_WITH_DES_CBC_SHA	TLS / Alert: handshake failure	خیر

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
100	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA	TLS / Alert: handshake failure	خیر
101	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA	TLS / Alert: handshake failure	خیر
102	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	TLS / No ciphers available	خیر
103	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	TLS / No ciphers available	خیر
104	TLS_DHE_RSA_WITH_AES_256_CBC_SHA	TLS / Alert: handshake failure	خیر
105	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	TLS / No ciphers available	خیر
106	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	TLS / No ciphers available	خیر
107	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	TLS / Alert: handshake failure	خیر
108	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	TLS / Alert: handshake failure	خیر
109	TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA	TLS / Alert: handshake failure	خیر
110	TLS_DHE_DSS_WITH_SEED_CBC_SHA	TLS / Alert: handshake failure	خیر
111	TLS_DHE_DSS_WITH_DES_CBC_SHA	TLS / Alert: handshake failure	خیر
112	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA	TLS / Alert: handshake failure	خیر
113	TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA	TLS / Alert: handshake failure	خیر
114	TLS_DHE_DSS_WITH_AES_256_GCM_SHA384	TLS / No ciphers available	خیر
115	TLS_DHE_DSS_WITH_AES_256_CBC_SHA256	TLS / No ciphers available	خیر
116	TLS_DHE_DSS_WITH_AES_256_CBC_SHA	TLS / Alert: handshake failure	خیر
117	TLS_DHE_DSS_WITH_AES_128_GCM_SHA256	TLS / No ciphers available	خیر
118	TLS_DHE_DSS_WITH_AES_128_CBC_SHA256	TLS / No ciphers available	خیر
119	TLS_DHE_DSS_WITH_AES_128_CBC_SHA	TLS / Alert: handshake failure	خیر

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
120	TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	TLS / Alert: handshake failure	خیر
121	TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA	TLS / Alert: handshake failure	خیر

پشتیبانی از این پروتکل : خیر

Accepted Cipher Suites :

#	Name	Connection Status	Anonymous

Preferred Cipher Suites :

#	Name	Connection Status	Anonymous
1			خیر

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
1	TLS_RSA_WITH_SEED_CBC_SHA	TLS / Alert: protocol version	خیر
2	TLS_RSA_WITH_RC4_128_SHA	TLS / Alert: protocol version	خیر
3	TLS_RSA_WITH_RC4_128_MD5	TLS / Alert: protocol version	خیر
4	TLS_RSA_WITH_NULL_SHA256	TLS / No ciphers available	خیر
5	TLS_RSA_WITH_NULL_SHA	TLS / Alert: protocol version	خیر
6	TLS_RSA_WITH_NULL_MD5	TLS / Alert: protocol version	خیر
7	TLS_RSA_WITH_IDEA_CBC_SHA	TLS / Alert: protocol version	خیر
8	TLS_RSA_WITH_DES_CBC_SHA	TLS / Alert: protocol version	خیر
9	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	TLS / Alert: protocol version	خیر
10	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	TLS / Alert: protocol version	خیر
11	TLS_RSA_WITH_AES_256_GCM_SHA384	TLS / No ciphers available	خیر
12	TLS_RSA_WITH_AES_256_CBC_SHA256	TLS / No ciphers available	خیر
13	TLS_RSA_WITH_AES_256_CBC_SHA	TLS / Alert: protocol version	خیر
14	TLS_RSA_WITH_AES_128_GCM_SHA256	TLS / No ciphers available	خیر
15	TLS_RSA_WITH_AES_128_CBC_SHA256	TLS / No ciphers available	خیر
16	TLS_RSA_WITH_AES_128_CBC_SHA	TLS / Alert: protocol version	خیر
17	TLS_RSA_WITH_3DES_EDE_CBC_SHA	TLS / Alert: protocol version	خیر

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
19	TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5	TLS / Alert: protocol version	خیر
20	TLS_RSA_EXPORT_WITH_DES40_CBC_SHA	TLS / Alert: protocol version	خیر
21	TLS_ECDH_anon_WITH_RC4_128_SHA	TLS / Alert: protocol version	بلی
22	TLS_ECDH_anon_WITH_NULL_SHA	TLS / Alert: protocol version	بلی
23	TLS_ECDH_anon_WITH_AES_256_CBC_SHA	TLS / Alert: protocol version	بلی
24	TLS_ECDH_anon_WITH_AES_128_CBC_SHA	TLS / Alert: protocol version	بلی
25	TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA	TLS / Alert: protocol version	بلی
26	TLS_ECDH_RSA_WITH_RC4_128_SHA	TLS / Alert: protocol version	خیر
27	TLS_ECDH_RSA_WITH_NULL_SHA	TLS / Alert: protocol version	خیر
28	TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384	TLS / No ciphers available	خیر
29	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384	TLS / No ciphers available	خیر
30	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA	TLS / Alert: protocol version	خیر
31	TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256	TLS / No ciphers available	خیر
32	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256	TLS / No ciphers available	خیر
33	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA	TLS / Alert: protocol version	خیر
34	TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA	TLS / Alert: protocol version	خیر
35	TLS_ECDH_ECDSA_WITH_RC4_128_SHA	TLS / Alert: protocol version	خیر
36	TLS_ECDH_ECDSA_WITH_NULL_SHA	TLS / Alert: protocol version	خیر
37	TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384	TLS / No ciphers available	خیر
38	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384	TLS / No ciphers available	خیر

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
39	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA	TLS / Alert: protocol version	خیر
40	TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256	TLS / No ciphers available	خیر
41	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256	TLS / No ciphers available	خیر
42	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA	TLS / Alert: protocol version	خیر
43	TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA	TLS / Alert: protocol version	خیر
44	TLS_ECDHE_RSA_WITH_RC4_128_SHA	TLS / Alert: protocol version	خیر
45	TLS_ECDHE_RSA_WITH_NULL_SHA	TLS / Alert: protocol version	خیر
46	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	TLS / No ciphers available	خیر
47	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	TLS / No ciphers available	خیر
48	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	TLS / Alert: protocol version	خیر
49	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	TLS / No ciphers available	خیر
50	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	TLS / No ciphers available	خیر
51	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	TLS / Alert: protocol version	خیر
52	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	TLS / Alert: protocol version	خیر
53	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA	TLS / Alert: protocol version	خیر
54	TLS_ECDHE_ECDSA_WITH_NULL_SHA	TLS / Alert: protocol version	خیر
55	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	TLS / No ciphers available	خیر
56	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	TLS / No ciphers available	خیر
57	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	TLS / Alert: protocol version	خیر
58	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	TLS / No ciphers available	خیر

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
59	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	TLS / No ciphers available	خیر
60	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	TLS / Alert: protocol version	خیر
61	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	TLS / Alert: protocol version	خیر
62	TLS_DH_anon_WITH_SEED_CBC_SHA	TLS / Alert: protocol version	بلی
63	TLS_DH_anon_WITH_RC4_128_MD5	TLS / Alert: protocol version	بلی
64	TLS_DH_anon_WITH_DES_CBC_SHA	TLS / Alert: protocol version	بلی
65	TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA	TLS / Alert: protocol version	بلی
66	TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA	TLS / Alert: protocol version	بلی
67	TLS_DH_anon_WITH_AES_256_GCM_SHA384	TLS / No ciphers available	بلی
68	TLS_DH_anon_WITH_AES_256_CBC_SHA256	TLS / No ciphers available	بلی
69	TLS_DH_anon_WITH_AES_256_CBC_SHA	TLS / Alert: protocol version	بلی
70	TLS_DH_anon_WITH_AES_128_GCM_SHA256	TLS / No ciphers available	بلی
71	TLS_DH_anon_WITH_AES_128_CBC_SHA256	TLS / No ciphers available	بلی
72	TLS_DH_anon_WITH_AES_128_CBC_SHA	TLS / Alert: protocol version	بلی
73	TLS_DH_anon_WITH_3DES_EDE_CBC_SHA	TLS / Alert: protocol version	بلی
74	TLS_DH_anon_EXPORT_WITH_RC4_40_MD5	TLS / Alert: protocol version	بلی
75	TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA	TLS / Alert: protocol version	بلی
76	TLS_DH_RSA_WITH_SEED_CBC_SHA	TLS / Alert: protocol version	خیر
77	TLS_DH_RSA_WITH_DES_CBC_SHA	TLS / Alert: protocol version	خیر
78	TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA	TLS / Alert: protocol version	خیر

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
79	TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA	TLS / Alert: protocol version	خیر
80	TLS_DH_RSA_WITH_AES_256_GCM_SHA384	TLS / No ciphers available	خیر
81	TLS_DH_RSA_WITH_AES_256_CBC_SHA256	TLS / No ciphers available	خیر
82	TLS_DH_RSA_WITH_AES_256_CBC_SHA	TLS / Alert: protocol version	خیر
83	TLS_DH_RSA_WITH_AES_128_GCM_SHA256	TLS / No ciphers available	خیر
84	TLS_DH_RSA_WITH_AES_128_CBC_SHA256	TLS / No ciphers available	خیر
85	TLS_DH_RSA_WITH_AES_128_CBC_SHA	TLS / Alert: protocol version	خیر
86	TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA	TLS / Alert: protocol version	خیر
87	TLS_DH_DSS_WITH_SEED_CBC_SHA	TLS / Alert: protocol version	خیر
88	TLS_DH_DSS_WITH_DES_CBC_SHA	TLS / Alert: protocol version	خیر
89	TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA	TLS / Alert: protocol version	خیر
90	TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA	TLS / Alert: protocol version	خیر
91	TLS_DH_DSS_WITH_AES_256_GCM_SHA384	TLS / No ciphers available	خیر
92	TLS_DH_DSS_WITH_AES_256_CBC_SHA256	TLS / No ciphers available	خیر
93	TLS_DH_DSS_WITH_AES_256_CBC_SHA	TLS / Alert: protocol version	خیر
94	TLS_DH_DSS_WITH_AES_128_GCM_SHA256	TLS / No ciphers available	خیر
95	TLS_DH_DSS_WITH_AES_128_CBC_SHA256	TLS / No ciphers available	خیر
96	TLS_DH_DSS_WITH_AES_128_CBC_SHA	TLS / Alert: protocol version	خیر
97	TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA	TLS / Alert: protocol version	خیر
98	TLS_DHE_RSA_WITH_SEED_CBC_SHA	TLS / Alert: protocol version	خیر

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
99	TLS_DHE_RSA_WITH_DES_CBC_SHA	TLS / Alert: protocol version	خیر
100	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA	TLS / Alert: protocol version	خیر
101	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA	TLS / Alert: protocol version	خیر
102	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	TLS / No ciphers available	خیر
103	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	TLS / No ciphers available	خیر
104	TLS_DHE_RSA_WITH_AES_256_CBC_SHA	TLS / Alert: protocol version	خیر
105	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	TLS / No ciphers available	خیر
106	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	TLS / No ciphers available	خیر
107	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	TLS / Alert: protocol version	خیر
108	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	TLS / Alert: protocol version	خیر
109	TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA	TLS / Alert: protocol version	خیر
110	TLS_DHE_DSS_WITH_SEED_CBC_SHA	TLS / Alert: protocol version	خیر
111	TLS_DHE_DSS_WITH_DES_CBC_SHA	TLS / Alert: protocol version	خیر
112	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA	TLS / Alert: protocol version	خیر
113	TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA	TLS / Alert: protocol version	خیر
114	TLS_DHE_DSS_WITH_AES_256_GCM_SHA384	TLS / No ciphers available	خیر
115	TLS_DHE_DSS_WITH_AES_256_CBC_SHA256	TLS / No ciphers available	خیر
116	TLS_DHE_DSS_WITH_AES_256_CBC_SHA	TLS / Alert: protocol version	خیر
117	TLS_DHE_DSS_WITH_AES_128_GCM_SHA256	TLS / No ciphers available	خیر
118	TLS_DHE_DSS_WITH_AES_128_CBC_SHA256	TLS / No ciphers available	خیر

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
119	TLS_DHE_DSS_WITH_AES_128_CBC_SHA	TLS / Alert: protocol version	خیر
120	TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	TLS / Alert: protocol version	خیر
121	TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA	TLS / Alert: protocol version	خیر

پشتیبانی از این پروتکل : بلی

Accepted Cipher Suites :

#	Name	Connection Status	Anonymous
1	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	HTTP 200 OK	خیر
2	TLS_RSA_WITH_AES_256_CBC_SHA	HTTP 200 OK	خیر
3	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	HTTP 200 OK	خیر
4	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA	HTTP 200 OK	خیر
5	TLS_DHE_RSA_WITH_AES_256_CBC_SHA	HTTP 200 OK	خیر
6	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	HTTP 200 OK	خیر
7	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	HTTP 200 OK	خیر
8	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA	HTTP 200 OK	خیر
9	TLS_RSA_WITH_AES_128_CBC_SHA	HTTP 200 OK	خیر
10	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	HTTP 200 OK	خیر

Preferred Cipher Suites :

#	Name	Connection Status	Anonymous
1	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	HTTP 200 OK	خیر

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
1	TLS_RSA_WITH_SEED_CBC_SHA	TLS / Alert: handshake failure	خیر
2	TLS_RSA_WITH_RC4_128_SHA	TLS / Alert: handshake failure	خیر
3	TLS_RSA_WITH_RC4_128_MD5	TLS / Alert: handshake failure	خیر
4	TLS_RSA_WITH_NULL_SHA256	TLS / No ciphers available	خیر
5	TLS_RSA_WITH_NULL_SHA	TLS / Alert: handshake failure	خیر
6	TLS_RSA_WITH_NULL_MD5	TLS / Alert: handshake failure	خیر
7	TLS_RSA_WITH_IDEA_CBC_SHA	TLS / Alert: handshake failure	خیر

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
9	TLS_RSA_WITH_AES_256_GCM_SHA384	TLS / No ciphers available	خیر
10	TLS_RSA_WITH_AES_256_CBC_SHA256	TLS / No ciphers available	خیر
11	TLS_RSA_WITH_AES_128_GCM_SHA256	TLS / No ciphers available	خیر
12	TLS_RSA_WITH_AES_128_CBC_SHA256	TLS / No ciphers available	خیر
13	TLS_RSA_WITH_3DES_EDE_CBC_SHA	TLS / Alert: handshake failure	خیر
14	TLS_RSA_EXPORT_WITH_RC4_40_MD5	TLS / Alert: handshake failure	خیر
15	TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5	TLS / Alert: handshake failure	خیر
16	TLS_RSA_EXPORT_WITH_DES40_CBC_SHA	TLS / Alert: handshake failure	خیر
17	TLS_ECDH_anon_WITH_RC4_128_SHA	TLS / Alert: handshake failure	بلی
18	TLS_ECDH_anon_WITH_NULL_SHA	TLS / Alert: handshake failure	بلی
19	TLS_ECDH_anon_WITH_AES_256_CBC_SHA	TLS / Alert: handshake failure	بلی
20	TLS_ECDH_anon_WITH_AES_128_CBC_SHA	TLS / Alert: handshake failure	بلی
21	TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA	TLS / Alert: handshake failure	بلی
22	TLS_ECDH_RSA_WITH_RC4_128_SHA	TLS / Alert: handshake failure	خیر
23	TLS_ECDH_RSA_WITH_NULL_SHA	TLS / Alert: handshake failure	خیر
24	TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384	TLS / No ciphers available	خیر
25	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384	TLS / No ciphers available	خیر
26	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA	TLS / Alert: handshake failure	خیر
27	TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256	TLS / No ciphers available	خیر
28	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256	TLS / No ciphers available	خیر

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
29	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA	TLS / Alert: handshake failure	خیر
30	TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA	TLS / Alert: handshake failure	خیر
31	TLS_ECDH_ECDSA_WITH_RC4_128_SHA	TLS / Alert: handshake failure	خیر
32	TLS_ECDH_ECDSA_WITH_NULL_SHA	TLS / Alert: handshake failure	خیر
33	TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384	TLS / No ciphers available	خیر
34	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384	TLS / No ciphers available	خیر
35	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA	TLS / Alert: handshake failure	خیر
36	TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256	TLS / No ciphers available	خیر
37	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256	TLS / No ciphers available	خیر
38	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA	TLS / Alert: handshake failure	خیر
39	TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA	TLS / Alert: handshake failure	خیر
40	TLS_ECDHE_RSA_WITH_RC4_128_SHA	TLS / Alert: handshake failure	خیر
41	TLS_ECDHE_RSA_WITH_NULL_SHA	TLS / Alert: handshake failure	خیر
42	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	TLS / No ciphers available	خیر
43	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	TLS / No ciphers available	خیر
44	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	TLS / No ciphers available	خیر
45	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	TLS / No ciphers available	خیر
46	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	TLS / Alert: handshake failure	خیر
47	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA	TLS / Alert: handshake failure	خیر
48	TLS_ECDHE_ECDSA_WITH_NULL_SHA	TLS / Alert: handshake failure	خیر

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
49	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	TLS / No ciphers available	خیر
50	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	TLS / No ciphers available	خیر
51	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	TLS / Alert: handshake failure	خیر
52	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	TLS / No ciphers available	خیر
53	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	TLS / No ciphers available	خیر
54	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	TLS / Alert: handshake failure	خیر
55	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	TLS / Alert: handshake failure	خیر
56	TLS_DH_anon_WITH_SEED_CBC_SHA	TLS / Alert: handshake failure	بلی
57	TLS_DH_anon_WITH_RC4_128_MD5	TLS / Alert: handshake failure	بلی
58	TLS_DH_anon_WITH_DES_CBC_SHA	TLS / Alert: handshake failure	بلی
59	TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA	TLS / Alert: handshake failure	بلی
60	TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA	TLS / Alert: handshake failure	بلی
61	TLS_DH_anon_WITH_AES_256_GCM_SHA384	TLS / No ciphers available	بلی
62	TLS_DH_anon_WITH_AES_256_CBC_SHA256	TLS / No ciphers available	بلی
63	TLS_DH_anon_WITH_AES_256_CBC_SHA	TLS / Alert: handshake failure	بلی
64	TLS_DH_anon_WITH_AES_128_GCM_SHA256	TLS / No ciphers available	بلی
65	TLS_DH_anon_WITH_AES_128_CBC_SHA256	TLS / No ciphers available	بلی
66	TLS_DH_anon_WITH_AES_128_CBC_SHA	TLS / Alert: handshake failure	بلی
67	TLS_DH_anon_WITH_3DES_EDE_CBC_SHA	TLS / Alert: handshake failure	بلی
68	TLS_DH_anon_EXPORT_WITH_RC4_40_MD5	TLS / Alert: handshake failure	بلی

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
69	TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA	TLS / Alert: handshake failure	بلی
70	TLS_DH_RSA_WITH_SEED_CBC_SHA	TLS / Alert: handshake failure	خیر
71	TLS_DH_RSA_WITH_DES_CBC_SHA	TLS / Alert: handshake failure	خیر
72	TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA	TLS / Alert: handshake failure	خیر
73	TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA	TLS / Alert: handshake failure	خیر
74	TLS_DH_RSA_WITH_AES_256_GCM_SHA384	TLS / No ciphers available	خیر
75	TLS_DH_RSA_WITH_AES_256_CBC_SHA256	TLS / No ciphers available	خیر
76	TLS_DH_RSA_WITH_AES_256_CBC_SHA	TLS / Alert: handshake failure	خیر
77	TLS_DH_RSA_WITH_AES_128_GCM_SHA256	TLS / No ciphers available	خیر
78	TLS_DH_RSA_WITH_AES_128_CBC_SHA256	TLS / No ciphers available	خیر
79	TLS_DH_RSA_WITH_AES_128_CBC_SHA	TLS / Alert: handshake failure	خیر
80	TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA	TLS / Alert: handshake failure	خیر
81	TLS_DH_DSS_WITH_SEED_CBC_SHA	TLS / Alert: handshake failure	خیر
82	TLS_DH_DSS_WITH_DES_CBC_SHA	TLS / Alert: handshake failure	خیر
83	TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA	TLS / Alert: handshake failure	خیر
84	TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA	TLS / Alert: handshake failure	خیر
85	TLS_DH_DSS_WITH_AES_256_GCM_SHA384	TLS / No ciphers available	خیر
86	TLS_DH_DSS_WITH_AES_256_CBC_SHA256	TLS / No ciphers available	خیر
87	TLS_DH_DSS_WITH_AES_256_CBC_SHA	TLS / Alert: handshake failure	خیر
88	TLS_DH_DSS_WITH_AES_128_GCM_SHA256	TLS / No ciphers available	خیر

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
89	TLS_DH_DSS_WITH_AES_128_CBC_SHA256	TLS / No ciphers available	خیر
90	TLS_DH_DSS_WITH_AES_128_CBC_SHA	TLS / Alert: handshake failure	خیر
91	TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA	TLS / Alert: handshake failure	خیر
92	TLS_DHE_RSA_WITH_SEED_CBC_SHA	TLS / Alert: handshake failure	خیر
93	TLS_DHE_RSA_WITH_DES_CBC_SHA	TLS / Alert: handshake failure	خیر
94	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	TLS / No ciphers available	خیر
95	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	TLS / No ciphers available	خیر
96	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	TLS / No ciphers available	خیر
97	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	TLS / No ciphers available	خیر
98	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	TLS / Alert: handshake failure	خیر
99	TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA	TLS / Alert: handshake failure	خیر
100	TLS_DHE_DSS_WITH_SEED_CBC_SHA	TLS / Alert: handshake failure	خیر
101	TLS_DHE_DSS_WITH_DES_CBC_SHA	TLS / Alert: handshake failure	خیر
102	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA	TLS / Alert: handshake failure	خیر
103	TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA	TLS / Alert: handshake failure	خیر
104	TLS_DHE_DSS_WITH_AES_256_GCM_SHA384	TLS / No ciphers available	خیر
105	TLS_DHE_DSS_WITH_AES_256_CBC_SHA256	TLS / No ciphers available	خیر
106	TLS_DHE_DSS_WITH_AES_256_CBC_SHA	TLS / Alert: handshake failure	خیر
107	TLS_DHE_DSS_WITH_AES_128_GCM_SHA256	TLS / No ciphers available	خیر
108	TLS_DHE_DSS_WITH_AES_128_CBC_SHA256	TLS / No ciphers available	خیر

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
109	TLS_DHE_DSS_WITH_AES_128_CBC_SHA	TLS / Alert: handshake failure	خیر
110	TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	TLS / Alert: handshake failure	خیر
111	TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA	TLS / Alert: handshake failure	خیر

پشتیبانی از این پروتکل : بلی

Accepted Cipher Suites :

#	Name	Connection Status	Anonymous
1	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA	HTTP 200 OK	خیر
2	RSA_WITH_AES_256_CCM	HTTP 200 OK	خیر
3	TLS_RSA_WITH_AES_256_CBC_SHA256	HTTP 200 OK	خیر
4	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	HTTP 200 OK	خیر
5	TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384	HTTP 200 OK	خیر
6	RSA_WITH_AES_256_CCM_8	HTTP 200 OK	خیر
7	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256	HTTP 200 OK	خیر
8	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	HTTP 200 OK	خیر
9	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256	HTTP 200 OK	خیر
10	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	HTTP 200 OK	خیر
11	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	HTTP 200 OK	خیر
12	TLS_DHE_RSA_WITH_AES_256_CBC_SHA	HTTP 200 OK	خیر
13	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	HTTP 200 OK	خیر
14	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	HTTP 200 OK	خیر
15	DHE_RSA_WITH_AES_256_CCM_8	HTTP 200 OK	خیر
16	TLS_RSA_WITH_AES_256_CBC_SHA	HTTP 200 OK	خیر
17	TLS_RSA_WITH_AES_256_GCM_SHA384	HTTP 200 OK	خیر
18	TLS_DHE_RSA_WITH_AES_256_CCM	HTTP 200 OK	خیر
19	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256	HTTP 200 OK	خیر

Accepted Cipher Suites :

#	Name	Connection Status	Anonymous
20	RSA_WITH_AES_128_CCM_8	HTTP 200 OK	خیر
21	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA	HTTP 200 OK	خیر
22	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	HTTP 200 OK	خیر
23	RSA_WITH_AES_128_CCM	HTTP 200 OK	خیر
24	DHE_RSA_WITH_AES_128_CCM_8	HTTP 200 OK	خیر
25	DHE_RSA_WITH_AES_128_CCM	HTTP 200 OK	خیر
26	TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256	HTTP 200 OK	خیر
27	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	HTTP 200 OK	خیر
28	TLS_RSA_WITH_AES_128_CBC_SHA256	HTTP 200 OK	خیر
29	TLS_RSA_WITH_AES_128_CBC_SHA	HTTP 200 OK	خیر
30	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	HTTP 200 OK	خیر
31	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256	HTTP 200 OK	خیر
32	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	HTTP 200 OK	خیر
33	TLS_RSA_WITH_AES_128_GCM_SHA256	HTTP 200 OK	خیر
34	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	HTTP 200 OK	خیر
35	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	HTTP 200 OK	خیر
36	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	HTTP 200 OK	خیر

Preferred Cipher Suites :

#	Name	Connection Status	Anonymous
1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	HTTP 200 OK	خیر

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
1	TLS_RSA_WITH_SEED_CBC_SHA	TLS / Alert: handshake failure	خیر

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
3	TLS_RSA_WITH_RC4_128_MD5	TLS / Alert: handshake failure	خیر
4	TLS_RSA_WITH_NULL_SHA256	TLS / Alert: handshake failure	خیر
5	TLS_RSA_WITH_NULL_SHA	TLS / Alert: handshake failure	خیر
6	TLS_RSA_WITH_NULL_MD5	TLS / Alert: handshake failure	خیر
7	TLS_RSA_WITH_IDEA_CBC_SHA	TLS / Alert: handshake failure	خیر
8	TLS_RSA_WITH_3DES_EDE_CBC_SHA	TLS / Alert: handshake failure	خیر
9	TLS_ECDH_anon_WITH_RC4_128_SHA	TLS / Alert: handshake failure	بلی
10	TLS_ECDH_anon_WITH_NULL_SHA	TLS / Alert: handshake failure	بلی
11	TLS_ECDH_anon_WITH_AES_256_CBC_SHA	TLS / Alert: handshake failure	بلی
12	TLS_ECDH_anon_WITH_AES_128_CBC_SHA	TLS / Alert: handshake failure	بلی
13	TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA	TLS / Alert: handshake failure	بلی
14	TLS_ECDHE_RSA_WITH_RC4_128_SHA	TLS / Alert: handshake failure	خیر
15	TLS_ECDHE_RSA_WITH_NULL_SHA	TLS / Alert: handshake failure	خیر
16	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	TLS / Alert: handshake failure	خیر
17	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	TLS / Alert: handshake failure	خیر
18	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA	TLS / Alert: handshake failure	خیر
19	TLS_ECDHE_ECDSA_WITH_NULL_SHA	TLS / Alert: handshake failure	خیر
20	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	TLS / Alert: handshake failure	خیر
21	TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_CBC_SHA384	TLS / Alert: handshake failure	خیر
22	TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_CBC_SHA256	TLS / Alert: handshake failure	خیر

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
23	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	TLS / Alert: handshake failure	خیر
24	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	TLS / Alert: handshake failure	خیر
25	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	TLS / Alert: handshake failure	خیر
26	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	TLS / Alert: handshake failure	خیر
27	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	TLS / Alert: handshake failure	خیر
28	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	TLS / Alert: handshake failure	خیر
29	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	TLS / Alert: handshake failure	خیر
30	TLS_DH_anon_WITH_SEED_CBC_SHA	TLS / Alert: handshake failure	بلی
31	TLS_DH_anon_WITH_RC4_128_MD5	TLS / Alert: handshake failure	بلی
32	TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA256	TLS / No ciphers available	بلی
33	TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA	TLS / Alert: handshake failure	بلی
34	TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA256	TLS / No ciphers available	بلی
35	TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA	TLS / Alert: handshake failure	بلی
36	TLS_DH_anon_WITH_AES_256_GCM_SHA384	TLS / Alert: handshake failure	بلی
37	TLS_DH_anon_WITH_AES_256_CBC_SHA256	TLS / Alert: handshake failure	بلی
38	TLS_DH_anon_WITH_AES_256_CBC_SHA	TLS / Alert: handshake failure	بلی
39	TLS_DH_anon_WITH_AES_128_GCM_SHA256	TLS / Alert: handshake failure	بلی
40	TLS_DH_anon_WITH_AES_128_CBC_SHA256	TLS / Alert: handshake failure	بلی
41	TLS_DH_anon_WITH_AES_128_CBC_SHA	TLS / Alert: handshake failure	بلی
42	TLS_DH_anon_WITH_3DES_EDE_CBC_SHA	TLS / Alert: handshake failure	بلی

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
43	TLS_DHE_RSA_WITH_SEED_CBC_SHA	TLS / Alert: handshake failure	خیر
44	TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256	TLS / Alert: handshake failure	خیر
45	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	TLS / Alert: handshake failure	خیر
46	TLS_DHE_DSS_WITH_SEED_CBC_SHA	TLS / Alert: handshake failure	خیر
47	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA256	TLS / Alert: handshake failure	خیر
48	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA	TLS / Alert: handshake failure	خیر
49	TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA256	TLS / Alert: handshake failure	خیر
50	TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA	TLS / Alert: handshake failure	خیر
51	TLS_DHE_DSS_WITH_AES_256_GCM_SHA384	TLS / Alert: handshake failure	خیر
52	TLS_DHE_DSS_WITH_AES_256_CBC_SHA256	TLS / Alert: handshake failure	خیر
53	TLS_DHE_DSS_WITH_AES_256_CBC_SHA	TLS / Alert: handshake failure	خیر
54	TLS_DHE_DSS_WITH_AES_128_GCM_SHA256	TLS / Alert: handshake failure	خیر
55	TLS_DHE_DSS_WITH_AES_128_CBC_SHA256	TLS / Alert: handshake failure	خیر
56	TLS_DHE_DSS_WITH_AES_128_CBC_SHA	TLS / Alert: handshake failure	خیر
57	TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	TLS / Alert: handshake failure	خیر
58	ECDHE_ECDSA_WITH_AES_256_CCM_8	TLS / Alert: handshake failure	خیر
59	ECDHE_ECDSA_WITH_AES_256_CCM	TLS / Alert: handshake failure	خیر
60	ECDHE_ECDSA_WITH_AES_128_CCM_8	TLS / Alert: handshake failure	خیر
61	ECDHE_ECDSA_WITH_AES_128_CCM	TLS / Alert: handshake failure	خیر
62	ECDHE-ECDSA-ARIA256-GCM-SHA384	TLS / Alert: handshake failure	خیر

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
63	ECDHE-ECDSA-ARIA128-GCM-SHA256	TLS / Alert: handshake failure	خیر
64	ECDHE-ARIA256-GCM-SHA384	TLS / Alert: handshake failure	خیر
65	ECDHE-ARIA128-GCM-SHA256	TLS / Alert: handshake failure	خیر
66	DHE-RSA-ARIA256-GCM-SHA384	TLS / Alert: handshake failure	خیر
67	DHE-RSA-ARIA128-GCM-SHA256	TLS / Alert: handshake failure	خیر
68	DHE-DSS-ARIA256-GCM-SHA384	TLS / Alert: handshake failure	خیر
69	DHE-DSS-ARIA128-GCM-SHA256	TLS / Alert: handshake failure	خیر
70	ARIA256-GCM-SHA384	TLS / Alert: handshake failure	خیر
71	ARIA128-GCM-SHA256	TLS / Alert: handshake failure	خیر

: Handshake Simulation

#	Name	Type	Cipher
1	(Android(2.3.7	tlsv1_2	TLS_RSA_WITH_AES_128_CBC_SHA
2	(Android(4.0.4	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
3	(Android(4.1.1	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
4	(Android(4.2.2	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
5	(Android(4.3	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
6	(Android(4.4.2	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
7	(Android(5.0.0	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
8	(Android(6.0	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
9	(Android(7.0	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
10	(Baidu(Jan 2015	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
11	(BingBot(Dec 2013	tlsv1_2	TLS_RSA_WITH_AES_128_CBC_SHA
12	(BingPreview(Dec 2013	tlsv1_2	TLS_DHE_RSA_WITH_AES_256_CBC_SHA
13	(BingPreview(Jun 2014	tlsv1_2	TLS_DHE_RSA_WITH_AES_256_CBC_SHA
14	(BingPreview(Jan 2015	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
15	Chrome(27) - Win 7	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
16	Chrome(28) - Win 7	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
17	Chrome(29) - Win 7	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
18	Chrome(30) - Win 7	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
19	Chrome(31) - Win 7	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

: Handshake Simulation

#	Name	Type	Cipher
20	Chrome(32) - Win 7	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
21	Chrome(33) - Win 7	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
22	Chrome(34) - OS X	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
23	Chrome(35) - Win 7	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
24	Chrome(36) - Win 7	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
25	Chrome(37) - OS X	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
26	Chrome(39) - OS X	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
27	Chrome(40) - OS X	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
28	Chrome(42) - OS X	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
29	Chrome(43) - OS X	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
30	Chrome(45) - OS X	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
31	Chrome(47) - OS X	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
32	Chrome(48) - OS X	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
33	Chrome(49) - Win 7	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
34	Chrome(49) - XP SP3	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
35	Chrome(50) - Win 7	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
36	Chrome(51) - Win 7	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
37	Chrome(57) - Win 7	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
38	Firefox(21) - Win 7	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
39	Firefox(10.0.12 ESR) - Win 7	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA

: Handshake Simulation

#	Name	Type	Cipher
40	Firefox(17.0.7 ESR) - Win 7	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
41	Firefox(24.2.0 ESR) - Win 7	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
42	Firefox(31.3.0 ESR) - Win 7	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
43	Firefox(21) - Fedora 19	tlsv1_2	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
44	Firefox(22) - Win 7	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
45	Firefox(24) - Win 7	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
46	Firefox(26) - Win 8	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
47	Firefox(27) - Win 8	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
48	Firefox(29) - OS X	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
49	Firefox(30) - OS X	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
50	Firefox(31) - OS X	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
51	Firefox(32) - OS X	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
52	Firefox(34) - OS X	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
53	Firefox(35) - OS X	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
54	Firefox(37) - OS X	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
55	Firefox(39) - OS X	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
56	Firefox(41) - OS X	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
57	Firefox(42) - OS X	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
58	Firefox(44) - OS X	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
59	Firefox(45) - Win 7	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

: Handshake Simulation

#	Name	Type	Cipher
60	Firefox(46) - Win 7	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
61	Firefox(47) - Win 7	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
62	Firefox(49) - XP SP3	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
63	Firefox(49) - Win 7	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
64	Firefox(53) - Win 7	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
65	(Googlebot(Oct 2013	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
66	(Googlebot(Jun 2014	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
67	(Googlebot(Feb 2015	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
68	IE(6) - XP		
69	IE(6) - XP		
70	IE(7) - Vista	tlsv1_2	TLS_RSA_WITH_AES_128_CBC_SHA
71	IE(8) - XP		
72	IE(8) - XP		
73	IE(8) - Win 7	tlsv1_2	TLS_RSA_WITH_AES_128_CBC_SHA
74	IE(9) - Win 7	tlsv1_2	TLS_RSA_WITH_AES_128_CBC_SHA
75	IE(8-10) - Win 7	tlsv1_2	TLS_RSA_WITH_AES_128_CBC_SHA
76	IE(8-10) - Win 7	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
77	IE(11) - Win 7	tlsv1_2	TLS_RSA_WITH_AES_128_CBC_SHA256
78	IE(11) - Win 7	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
79	IE(11) - Win 7	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

: Handshake Simulation

#	Name	Type	Cipher
80	IE(11) - Win 7	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
81	IE(11) - Win 7	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
82	IE(11) - Win 10 Preview	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
83	IE(11) - Win 8.1	tlsv1_2	TLS_RSA_WITH_AES_128_CBC_SHA256
84	IE(11) - Win 8.1	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
85	IE(11) - Win 8.1	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
86	IE(11) - Win 8.1	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
87	IE(11) - Win 8.1	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
88	IE(10) - Win Phone 8.0	tlsv1_2	TLS_RSA_WITH_AES_128_CBC_SHA
89	IE(11) - Win Phone 8.1	tlsv1_2	TLS_RSA_WITH_AES_128_CBC_SHA256
90	IE(11) - Win Phone 8.1 Update	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
91	IE(11) - Win 10	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
92	IE(11) - Win 10	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
93	Edge(12) - Win 10	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
94	Edge(13) - Win 10	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
95	Edge(13) - Win 10	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
96	Edge(13) - Win Phone 10	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
97	(Java(6u45	tlsv1_2	TLS_RSA_WITH_AES_128_CBC_SHA
98	(Java(7u25	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
99	(Java(8b132	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

: Handshake Simulation

#	Name	Type	Cipher
100	(Java(8u31	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
101	(OpenSSL(0.9.8y	tlsv1_2	TLS_DHE_RSA_WITH_AES_256_CBC_SHA
102	(OpenSSL(1.0.1h	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
103	(OpenSSL(1.0.1l	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
104	(OpenSSL(1.0.2e	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
105	Opera(12.15) - Win 7	tlsv1_2	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
106	Opera(15) - Win 7	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
107	Opera(16) - Win 7	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
108	Opera(17) - Win 7	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
109	Safari(5) - iOS 5.1.1	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
110	Safari(5.1.9) - OS X 10.6.8	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
111	Safari(6) - iOS 6.0.1	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
112	Safari(6.0.4) - OS X 10.8.4	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
113	Safari(7) - iOS 7.1	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
114	Safari(8) - iOS 8.0 Beta	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
115	Safari(7) - OS X 10.9	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
116	Safari(8) - iOS 8.4	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
117	Safari(8) - OS X 10.10	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
118	Safari(9) - iOS 9	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
119	Safari(9) - OS X 10.11	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

: Handshake Simulation

#	Name	Type	Cipher
120	Safari(10) - iOS 10	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
121	Safari(10) - OS X 10.12	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
122	Apple ATS(9) - iOS 9	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
123	Tor(17.0.9) - Win 7	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
124	(Yahoo Slurp(Oct 2013	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
125	(Yahoo Slurp(Jun 2014	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
126	(Yahoo Slurp(Jan 2015	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
127	(YandexBot(3.0		
128	(YandexBot(May 2014	tlsv1_2	TLS_DHE_RSA_WITH_AES_256_CBC_SHA
129	(YandexBot(Sep 2014	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
130	(YandexBot(Jan 2015	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384