بررسی SLL دامنه nashreonline.com

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

گزارش بررسی تنظیمات SSL دامنه nashreonline.com

تاریخ تهیه گزارش : یکشنبه ۰۳ فروردین ۱۳۹۹ در ساعت ۱۱:۴۴

بازدید :0

امتیاز :

ارتباط تنها در SSL	معتبر	سازگاری مرورگرها	آسیب پذیری	HSTS
				

اطلاعات هدر دامنه

```
Date: Sun, 22 Mar 2020 07:14:56 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Set-Cookie: __cfduid=daf1e5f99b75780902bcbdb7f90ac75b71584861296; expires=Tue, 21-Apr-20 07:14:56 GMT; path=/; domain=.nashreonline.com; HttpOnly; SameSite=Lax; Secure
Last-Modified: Sun, 22 Mar 2020 06:23:45 GMT
Cache-Control: public, max-age=0
Expires: Sun, 22 Mar 2020 07:14:56 GMT
Vary: Accept-Encoding,Accept-Encoding
X-Turbo-Charged-By: LiteSpeed
CF-Cache-Status: DYNAMIC
Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
Server: cloudflare
CF-RAY: 577e1e5ec9b30eb7-FRA
Content-Encoding: gzip
```

ارتباط تنها در SSL

//:http	http://nashreonline.com/ -> 301 -> https://nashreonline.com/ -> 200
//:https	https://nashreonline.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 : sni.cloudflaressl.com
نام کشور : US - ایلات متحده (آمریکا)
عنوان های جایگزین امضا (Alternative Names) : sni.cloudflaressl.com. , nashreonline.com , nashreonline.com ,
شروع اعتبار از : سه شنبه ۲۲ بهمن ۱۳۹۸ در ساعت ۰۰:۰۰
پایان اعتبار تا : جمعه ۱۸ مهر ۱۳۹۹ در ساعت ۱۲:۰۰ - **اتمام در** : 201 روز و 3 ساعت و 44 دقیقه و 59 ثانیه
صادر کننده مجوز : CloudFlare Inc ECC CA-2
کشور صادر کننده مجوز : US - ایلات متحده (آمریکا)
الگوریتم امضا : sha256 with EllipticCurve size: 256 Bits
Certificate Transparency : yes (certificate extension)
OCSP stapling : LOW - not offered
OCSP URL : http://ocsp.digicert.com
CRL Distribution Points : http://crl3.digicert.com/CloudFlareIncECCCA2.crl http://crl4.digicert.com/CloudFlareIncECCCA2.crl

Trust

Android iOS Java macOS Mozilla OPENJDK Windows

بررسی اعتبار دامنه :

بررسی اعتبار دامنه :

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

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

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 : xgudI9TToO8nZrVENlVUz5nn710TtqNLYivwaFnWnwk=

Pin : xgudI9TToO8nZrVENlVUz5nn710TtqNLYivwaFnWnwk=

Finger print : 89e566a16539661708aea5abcc72b3db4dbfe8af

عنوان : countryName=US, stateOrProvinceName=CA, localityName=San Francisco, organizationName=Cloudflare, Inc., commonName=sni.cloudflaressl.com

صادر کننده مجوز : countryName=US, stateOrProvinceName=CA, localityName=San Francisco, organizationName=CloudFlare, Inc., commonName=CloudFlare Inc ECC CA-2

سریال مجوز : 2.0957599825224E+37

شروع اعتبار از : 00:00:00 11-02-2020

پایان اعتبار تا : 12:00:00 09-10-2020

الگوریتم امضا : sha256

کلید عمومی : الگوریتم : EllipticCurve

کلید عمومی : نوع : secp256r1

کلید عمومی : اندازه : 256

شماره 2 : 3kcNJzkUJ1RqMXJzFX4Zxux5WfETK+uL6Viq9lJNn4o=

Pin : 3kcNJzkUJ1RqMXJzFX4Zxux5WfETK+uL6Viq9lJNn4o=

Finger print : 6b53c3b358cef368201f8741b9c5aedeea3861fa

عنوان : countryName=US, stateOrProvinceName=CA, localityName=San Francisco, organizationName=CloudFlare, Inc., commonName=CloudFlare Inc ECC CA-2

صادر کننده مجوز : countryName=IE, organizationName=Baltimore, organizationalUnitName=CyberTrust, commonName=Baltimore CyberTrust Root

سریال مجوز : 2.1204814788473E+37

شروع اعتبار از : 12:00:00 14-10-2015

پایان اعتبار تا : 12:00:00 09-10-2020

الگوریتم امضا : sha256

کلید عمومی : الگوریتم : EllipticCurve

کلید عمومی : نوع : secp256r1

کلید عمومی : اندازه : 256

بررسی اعتبار امضای دیجیتال

شماره 3 : Y9mvm0exBk1JoQ57f9Vm28jKo5lFm/woKcVxrYxu80o=

Pin : Y9mvm0exBk1JoQ57f9Vm28jKo5lFm/woKcVxrYxu80o=

Finger print : d4de20d05e66fc53fe1a50882c78db2852cae474

عنوان : countryName=IE, organizationName=Baltimore, organizationalUnitName=CyberTrust, commonName=Baltimore CyberTrust Root

صادر کننده مجوز : countryName=IE, organizationName=Baltimore, organizationalUnitName=CyberTrust, commonName=Baltimore CyberTrust Root

سریال مجوز : 33554617

شروع اعتبار از : 18:46:00 12-05-2000

پایان اعتبار تا : 23:59:00 12-05-2025

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 ندارد
IDs :

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-ECDSA-CHACHA20-POLY1305-OLD ECDHE-ECDSA-AES256-GCM-SHA384 ECDHE-ECDSA-AES256-SHA384 ECDHE-ECDSA-AES256-SHA ECDHE-ECDSA-CHACHA20-POLY1305 TLS_AES_128_GCM_SHA256 ECDHE-ECDSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES128-SHA256 ECDHE-ECDSA-AES128-SHA
PFS ECDHE curves :	prime256v1 secp384r1 secp521r1 X25519
Protocol Negotiated :	Default protocol TLS1.3
Cipher Negotiated :	(TLS_AES_256_GCM_SHA384, 253 bit ECDH (X25519
TLS Extensions :	server name/#0 renegotiation info/#65281 EC point formats/#11 session ticket/#35 next protocol/#13172 key share/#51 supported versions/#43 extended master secret/#23 application layer protocol negotiation/#16
TLS Session Ticket :	(valid for 64800 seconds only (< daily
SSL SessionID Support :	yes
Session Resumption Ticket :	پشتیبانی می کند
Session Resumption ID :	پشتیبانی می کند
TLS Timestamp :	off by 0 seconds from your localtime
DNS CAA Record :	--
Cert Transparency :	(yes (certificate extension
HTTP Status :	(/) OK 200
HTTP Strict Transport Security (HSTS) :	ارائه نشده است
Banner Server :	cloudflare
HTTP Public Key Pinning (HPKP) :	No support for HTTP Public Key Pinning
Cookie Count :	/ at 1
Cookie Cecure :	All (1) at / marked as secure
Cookie HTTP Only :	All (1) at / marked as HttpOnly
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 , no RSA key transport cipher
__ 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

اطلاعات بیشتر

آسیب پذیری های امضای دیجیتال

POODLE SSL :	آسیب پذیر نیست	اطلاعات بیشتر
CVE : __|	CWE-310	
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) :	no RSA certificate, can t be used with SSLv2 elsewhere	اطلاعات بیشتر
CVE : __|	CVE-2016-0800 CVE-2016-0703	
CWE : __|	CWE-310	
LOGJAM Common Primes :	no DH key with < = TLS 1.2	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 CBC TLS1 :	ECDHE-ECDSA-AES128-SHA ECDHE-ECDSA-AES256-SHA	اطلاعات بیشتر
CVE : __|	CVE-2011-3389	
CWE : __|	CWE-20	
BEAST :	آسیب پذیر -- (likely mitigated) but also supports higher protocols TLSv1.1 TLSv1.2 همچنین از پروتکل های بالاتر TLSv1.1 TLSv1.2 پشتیبانی می کند	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	TCP / Received RST	خیر
2	SSL_CK_RC4_128_EXPORT40_WITH_MD5	TCP / Received RST	خیر
3	SSL_CK_RC2_128_CBC_WITH_MD5	TCP / Received RST	خیر
4	SSL_CK_RC2_128_CBC_EXPORT40_WITH_MD5	TCP / Received RST	خیر
5	SSL_CK_IDEA_128_CBC_WITH_MD5	TCP / Received RST	خیر
6	SSL_CK_DES_64_CBC_WITH_MD5	TCP / Received RST	خیر
7	SSL_CK_DES_192_EDE3_CBC_WITH_MD5	TCP / Received RST	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 / Wrong version number	خیر
2	TLS_RSA_WITH_RC4_128_SHA	TLS / Wrong version number	خیر
3	TLS_RSA_WITH_RC4_128_MD5	TLS / Wrong version number	خیر
4	TLS_RSA_WITH_NULL_SHA256	TLS / No ciphers available	خیر
5	TLS_RSA_WITH_NULL_SHA	TLS / Wrong version number	خیر
6	TLS_RSA_WITH_NULL_MD5	TLS / Wrong version number	خیر
7	TLS_RSA_WITH_IDEA_CBC_SHA	TLS / Wrong version number	خیر
8	TLS_RSA_WITH_DES_CBC_SHA	TLS / Wrong version number	خیر
9	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	TLS / Wrong version number	خیر
10	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	TLS / Wrong version number	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 / Wrong version number	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 / Wrong version number	خیر
17	TLS_RSA_WITH_3DES_EDE_CBC_SHA	TLS / Wrong version number	خیر
18	TLS_RSA_EXPORT_WITH_RC4_40_MD5	TLS / Wrong version number	خیر

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
20	TLS_RSA_EXPORT_WITH_DES40_CBC_SHA	TLS / Wrong version number	خیر
21	TLS_ECDH_anon_WITH_RC4_128_SHA	TLS / Wrong version number	بلی
22	TLS_ECDH_anon_WITH_NULL_SHA	TLS / Wrong version number	بلی
23	TLS_ECDH_anon_WITH_AES_256_CBC_SHA	TLS / Wrong version number	بلی
24	TLS_ECDH_anon_WITH_AES_128_CBC_SHA	TLS / Wrong version number	بلی
25	TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA	TLS / Wrong version number	بلی
26	TLS_ECDH_RSA_WITH_RC4_128_SHA	TLS / Wrong version number	خیر
27	TLS_ECDH_RSA_WITH_NULL_SHA	TLS / Wrong version number	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 / Wrong version number	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 / Wrong version number	خیر
34	TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA	TLS / Wrong version number	خیر
35	TLS_ECDH_ECDSA_WITH_RC4_128_SHA	TLS / Wrong version number	خیر
36	TLS_ECDH_ECDSA_WITH_NULL_SHA	TLS / Wrong version number	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 / Wrong version number	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 / Wrong version number	خیر
43	TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA	TLS / Wrong version number	خیر
44	TLS_ECDHE_RSA_WITH_RC4_128_SHA	TLS / Wrong version number	خیر
45	TLS_ECDHE_RSA_WITH_NULL_SHA	TLS / Wrong version number	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 / Wrong version number	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 / Wrong version number	خیر
52	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	TLS / Wrong version number	خیر
53	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA	TLS / Wrong version number	خیر
54	TLS_ECDHE_ECDSA_WITH_NULL_SHA	TLS / Wrong version number	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 / Wrong version number	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 / Wrong version number	خیر
61	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	TLS / Wrong version number	خیر
62	TLS_DH_anon_WITH_SEED_CBC_SHA	TLS / Wrong version number	بلی
63	TLS_DH_anon_WITH_RC4_128_MD5	TLS / Wrong version number	بلی
64	TLS_DH_anon_WITH_DES_CBC_SHA	TLS / Wrong version number	بلی
65	TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA	TLS / Wrong version number	بلی
66	TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA	TLS / Wrong version number	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 / Wrong version number	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 / Wrong version number	بلی
73	TLS_DH_anon_WITH_3DES_EDE_CBC_SHA	TLS / Wrong version number	بلی
74	TLS_DH_anon_EXPORT_WITH_RC4_40_MD5	TLS / Wrong version number	بلی
75	TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA	TLS / Wrong version number	بلی
76	TLS_DH_RSA_WITH_SEED_CBC_SHA	TLS / Wrong version number	خیر
77	TLS_DH_RSA_WITH_DES_CBC_SHA	TLS / Wrong version number	خیر
78	TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA	TLS / Wrong version number	خیر
79	TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA	TLS / Wrong version number	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 / Wrong version number	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 / Wrong version number	خیر
86	TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA	TLS / Wrong version number	خیر
87	TLS_DH_DSS_WITH_SEED_CBC_SHA	TLS / Wrong version number	خیر
88	TLS_DH_DSS_WITH_DES_CBC_SHA	TLS / Wrong version number	خیر
89	TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA	TLS / Wrong version number	خیر
90	TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA	TLS / Wrong version number	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 / Wrong version number	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 / Wrong version number	خیر
97	TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA	TLS / Wrong version number	خیر
98	TLS_DHE_RSA_WITH_SEED_CBC_SHA	TLS / Wrong version number	خیر
99	TLS_DHE_RSA_WITH_DES_CBC_SHA	TLS / Wrong version number	خیر

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
100	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA	TLS / Wrong version number	خیر
101	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA	TLS / Wrong version number	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 / Wrong version number	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 / Wrong version number	خیر
108	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	TLS / Wrong version number	خیر
109	TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA	TLS / Wrong version number	خیر
110	TLS_DHE_DSS_WITH_SEED_CBC_SHA	TLS / Wrong version number	خیر
111	TLS_DHE_DSS_WITH_DES_CBC_SHA	TLS / Wrong version number	خیر
112	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA	TLS / Wrong version number	خیر
113	TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA	TLS / Wrong version number	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 / Wrong version number	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 / Wrong version number	خیر

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
120	TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	TLS / Wrong version number	خیر
121	TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA	TLS / Wrong version number	خیر

پشتیبانی از این پروتکل : بلی

Accepted Cipher Suites :

#	Name	Connection Status	Anonymous
1	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	HTTP 521 Origin Down	خیر
2	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	HTTP 521 Origin Down	خیر

Preferred Cipher Suites :

#	Name	Connection Status	Anonymous
1	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	HTTP 521 Origin Down	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
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

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
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
19	TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5	TLS / Alert: handshake failure	خیر
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

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
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
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

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
57	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	TLS / No ciphers available	خیر
58	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	TLS / No ciphers available	خیر
59	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	TLS / Alert: handshake failure	خیر
60	TLS_DH_anon_WITH_SEED_CBC_SHA	TLS / Alert: handshake failure	بلی
61	TLS_DH_anon_WITH_RC4_128_MD5	TLS / Alert: handshake failure	بلی
62	TLS_DH_anon_WITH_DES_CBC_SHA	TLS / Alert: handshake failure	بلی
63	TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA	TLS / Alert: handshake failure	بلی
64	TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA	TLS / Alert: handshake failure	بلی
65	TLS_DH_anon_WITH_AES_256_GCM_SHA384	TLS / No ciphers available	بلی
66	TLS_DH_anon_WITH_AES_256_CBC_SHA256	TLS / No ciphers available	بلی
67	TLS_DH_anon_WITH_AES_256_CBC_SHA	TLS / Alert: handshake failure	بلی
68	TLS_DH_anon_WITH_AES_128_GCM_SHA256	TLS / No ciphers available	بلی
69	TLS_DH_anon_WITH_AES_128_CBC_SHA256	TLS / No ciphers available	بلی
70	TLS_DH_anon_WITH_AES_128_CBC_SHA	TLS / Alert: handshake failure	بلی
71	TLS_DH_anon_WITH_3DES_EDE_CBC_SHA	TLS / Alert: handshake failure	بلی
72	TLS_DH_anon_EXPORT_WITH_RC4_40_MD5	TLS / Alert: handshake failure	بلی
73	TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA	TLS / Alert: handshake failure	بلی
74	TLS_DH_RSA_WITH_SEED_CBC_SHA	TLS / Alert: handshake failure	خیر
75	TLS_DH_RSA_WITH_DES_CBC_SHA	TLS / Alert: handshake failure	خیر
76	TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA	TLS / Alert: handshake failure	خیر

Rejected Cipher Suites :

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

Rejected Cipher Suites :

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

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
117	TLS_DHE_DSS_WITH_AES_128_CBC_SHA	TLS / Alert: handshake failure	خیر
118	TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	TLS / Alert: handshake failure	خیر
119	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_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	HTTP 521 Origin Down	خیر
2	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	HTTP 521 Origin Down	خیر

Preferred Cipher Suites :

#	Name	Connection Status	Anonymous
1	TLS_ECDHE_ECDSA_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
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

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
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
19	TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5	TLS / Alert: handshake failure	خیر
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

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
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
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

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
57	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	TLS / No ciphers available	خیر
58	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	TLS / No ciphers available	خیر
59	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	TLS / Alert: handshake failure	خیر
60	TLS_DH_anon_WITH_SEED_CBC_SHA	TLS / Alert: handshake failure	بلی
61	TLS_DH_anon_WITH_RC4_128_MD5	TLS / Alert: handshake failure	بلی
62	TLS_DH_anon_WITH_DES_CBC_SHA	TLS / Alert: handshake failure	بلی
63	TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA	TLS / Alert: handshake failure	بلی
64	TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA	TLS / Alert: handshake failure	بلی
65	TLS_DH_anon_WITH_AES_256_GCM_SHA384	TLS / No ciphers available	بلی
66	TLS_DH_anon_WITH_AES_256_CBC_SHA256	TLS / No ciphers available	بلی
67	TLS_DH_anon_WITH_AES_256_CBC_SHA	TLS / Alert: handshake failure	بلی
68	TLS_DH_anon_WITH_AES_128_GCM_SHA256	TLS / No ciphers available	بلی
69	TLS_DH_anon_WITH_AES_128_CBC_SHA256	TLS / No ciphers available	بلی
70	TLS_DH_anon_WITH_AES_128_CBC_SHA	TLS / Alert: handshake failure	بلی
71	TLS_DH_anon_WITH_3DES_EDE_CBC_SHA	TLS / Alert: handshake failure	بلی
72	TLS_DH_anon_EXPORT_WITH_RC4_40_MD5	TLS / Alert: handshake failure	بلی
73	TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA	TLS / Alert: handshake failure	بلی
74	TLS_DH_RSA_WITH_SEED_CBC_SHA	TLS / Alert: handshake failure	خیر
75	TLS_DH_RSA_WITH_DES_CBC_SHA	TLS / Alert: handshake failure	خیر
76	TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA	TLS / Alert: handshake failure	خیر

Rejected Cipher Suites :

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

Rejected Cipher Suites :

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

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
117	TLS_DHE_DSS_WITH_AES_128_CBC_SHA	TLS / Alert: handshake failure	خیر
118	TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	TLS / Alert: handshake failure	خیر
119	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_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	HTTP 200 OK	خیر
2	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	HTTP 200 OK	خیر
3	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	HTTP 525 Origin SSL Handshake Error	خیر
4	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	HTTP 521 Origin Down	خیر
5	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	HTTP 200 OK	خیر
6	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	HTTP 521 Origin Down	خیر
7	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	HTTP 521 Origin Down	خیر

Preferred Cipher Suites :

#	Name	Connection Status	Anonymous
1	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	HTTP 521 Origin Down	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 / 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_CAMELLIA_256_CBC_SHA256	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_SHA256	TLS / Alert: handshake failure	خیر

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
12	TLS_RSA_WITH_AES_256_GCM_SHA384	TLS / Alert: handshake failure	خیر
13	TLS_RSA_WITH_AES_256_CBC_SHA256	TLS / Alert: handshake failure	خیر
14	TLS_RSA_WITH_AES_256_CBC_SHA	TLS / Alert: handshake failure	خیر
15	TLS_RSA_WITH_AES_128_GCM_SHA256	TLS / Alert: handshake failure	خیر
16	TLS_RSA_WITH_AES_128_CBC_SHA256	TLS / Alert: handshake failure	خیر
17	TLS_RSA_WITH_AES_128_CBC_SHA	TLS / Alert: handshake failure	خیر
18	TLS_RSA_WITH_3DES_EDE_CBC_SHA	TLS / Alert: handshake failure	خیر
19	TLS_ECDH_anon_WITH_RC4_128_SHA	TLS / Alert: handshake failure	بلی
20	TLS_ECDH_anon_WITH_NULL_SHA	TLS / Alert: handshake failure	بلی
21	TLS_ECDH_anon_WITH_AES_256_CBC_SHA	TLS / Alert: handshake failure	بلی
22	TLS_ECDH_anon_WITH_AES_128_CBC_SHA	TLS / Alert: handshake failure	بلی
23	TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA	TLS / Alert: handshake failure	بلی
24	TLS_ECDHE_RSA_WITH_RC4_128_SHA	TLS / Alert: handshake failure	خیر
25	TLS_ECDHE_RSA_WITH_NULL_SHA	TLS / Alert: handshake failure	خیر
26	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	TLS / Alert: handshake failure	خیر
27	TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384	TLS / Alert: handshake failure	خیر
28	TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256	TLS / Alert: handshake failure	خیر
29	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	TLS / Alert: handshake failure	خیر
30	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	TLS / Alert: handshake failure	خیر
31	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	TLS / Alert: handshake failure	خیر

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
32	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	TLS / Alert: handshake failure	خیر
33	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	TLS / Alert: handshake failure	خیر
34	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	TLS / Alert: handshake failure	خیر
35	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	TLS / Alert: handshake failure	خیر
36	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA	TLS / Alert: handshake failure	خیر
37	TLS_ECDHE_ECDSA_WITH_NULL_SHA	TLS / Alert: handshake failure	خیر
38	TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_CBC_SHA384	TLS / Alert: handshake failure	خیر
39	TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_CBC_SHA256	TLS / Alert: handshake failure	خیر
40	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	TLS / Alert: handshake failure	خیر
41	TLS_DH_anon_WITH_SEED_CBC_SHA	TLS / Alert: handshake failure	بلی
42	TLS_DH_anon_WITH_RC4_128_MD5	TLS / Alert: handshake failure	بلی
43	TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA256	TLS / No ciphers available	بلی
44	TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA	TLS / Alert: handshake failure	بلی
45	TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA256	TLS / No ciphers available	بلی
46	TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA	TLS / Alert: handshake failure	بلی
47	TLS_DH_anon_WITH_AES_256_GCM_SHA384	TLS / Alert: handshake failure	بلی
48	TLS_DH_anon_WITH_AES_256_CBC_SHA256	TLS / Alert: handshake failure	بلی
49	TLS_DH_anon_WITH_AES_256_CBC_SHA	TLS / Alert: handshake failure	بلی
50	TLS_DH_anon_WITH_AES_128_GCM_SHA256	TLS / Alert: handshake failure	بلی
51	TLS_DH_anon_WITH_AES_128_CBC_SHA256	TLS / Alert: handshake failure	بلی

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
52	TLS_DH_anon_WITH_AES_128_CBC_SHA	TLS / Alert: handshake failure	بلی
53	TLS_DH_anon_WITH_3DES_EDE_CBC_SHA	TLS / Alert: handshake failure	بلی
54	TLS_DHE_RSA_WITH_SEED_CBC_SHA	TLS / Alert: handshake failure	خیر
55	TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256	TLS / Alert: handshake failure	خیر
56	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256	TLS / Alert: handshake failure	خیر
57	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA	TLS / Alert: handshake failure	خیر
58	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256	TLS / Alert: handshake failure	خیر
59	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA	TLS / Alert: handshake failure	خیر
60	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	TLS / Alert: handshake failure	خیر
61	TLS_DHE_RSA_WITH_AES_256_CCM	TLS / Alert: handshake failure	خیر
62	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	TLS / Alert: handshake failure	خیر
63	TLS_DHE_RSA_WITH_AES_256_CBC_SHA	TLS / Alert: handshake failure	خیر
64	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	TLS / Alert: handshake failure	خیر
65	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	TLS / Alert: handshake failure	خیر
66	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	TLS / Alert: handshake failure	خیر
67	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	TLS / Alert: handshake failure	خیر
68	TLS_DHE_DSS_WITH_SEED_CBC_SHA	TLS / Alert: handshake failure	خیر
69	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA256	TLS / Alert: handshake failure	خیر
70	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA	TLS / Alert: handshake failure	خیر
71	TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA256	TLS / Alert: handshake failure	خیر

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
72	TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA	TLS / Alert: handshake failure	خیر
73	TLS_DHE_DSS_WITH_AES_256_GCM_SHA384	TLS / Alert: handshake failure	خیر
74	TLS_DHE_DSS_WITH_AES_256_CBC_SHA256	TLS / Alert: handshake failure	خیر
75	TLS_DHE_DSS_WITH_AES_256_CBC_SHA	TLS / Alert: handshake failure	خیر
76	TLS_DHE_DSS_WITH_AES_128_GCM_SHA256	TLS / Alert: handshake failure	خیر
77	TLS_DHE_DSS_WITH_AES_128_CBC_SHA256	TLS / Alert: handshake failure	خیر
78	TLS_DHE_DSS_WITH_AES_128_CBC_SHA	TLS / Alert: handshake failure	خیر
79	TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	TLS / Alert: handshake failure	خیر
80	RSA_WITH_AES_256_CCM_8	TLS / Alert: handshake failure	خیر
81	RSA_WITH_AES_256_CCM	TLS / Alert: handshake failure	خیر
82	RSA_WITH_AES_128_CCM_8	TLS / Alert: handshake failure	خیر
83	RSA_WITH_AES_128_CCM	TLS / Alert: handshake failure	خیر
84	ECDHE_ECDSA_WITH_AES_256_CCM_8	TLS / Alert: handshake failure	خیر
85	ECDHE_ECDSA_WITH_AES_256_CCM	TLS / Alert: handshake failure	خیر
86	ECDHE_ECDSA_WITH_AES_128_CCM_8	TLS / Alert: handshake failure	خیر
87	ECDHE_ECDSA_WITH_AES_128_CCM	TLS / Alert: handshake failure	خیر
88	ECDHE-ECDSA-ARIA256-GCM-SHA384	TLS / Alert: handshake failure	خیر
89	ECDHE-ECDSA-ARIA128-GCM-SHA256	TLS / Alert: handshake failure	خیر
90	ECDHE-ARIA256-GCM-SHA384	TLS / Alert: handshake failure	خیر
91	ECDHE-ARIA128-GCM-SHA256	TLS / Alert: handshake failure	خیر

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
92	DHE_RSA_WITH_AES_256_CCM_8	TLS / Alert: handshake failure	خیر
93	DHE_RSA_WITH_AES_128_CCM_8	TLS / Alert: handshake failure	خیر
94	DHE_RSA_WITH_AES_128_CCM	TLS / Alert: handshake failure	خیر
95	DHE-RSA-ARIA256-GCM-SHA384	TLS / Alert: handshake failure	خیر
96	DHE-RSA-ARIA128-GCM-SHA256	TLS / Alert: handshake failure	خیر
97	DHE-DSS-ARIA256-GCM-SHA384	TLS / Alert: handshake failure	خیر
98	DHE-DSS-ARIA128-GCM-SHA256	TLS / Alert: handshake failure	خیر
99	ARIA256-GCM-SHA384	TLS / Alert: handshake failure	خیر
100	ARIA128-GCM-SHA256	TLS / Alert: handshake failure	خیر

: Handshake Simulation

#	Name	Type	Cipher
1	(Android(2.3.7		
2	(Android(4.0.4	tlsv1	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
3	(Android(4.1.1	tlsv1	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
4	(Android(4.2.2	tlsv1	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
5	(Android(4.3	tlsv1	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
6	(Android(4.4.2	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
7	(Android(5.0.0	tlsv1	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
8	(Android(6.0	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
9	(Android(7.0	tlsv1_2	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
10	(Baidu(Jan 2015	tlsv1	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
11	(BingBot(Dec 2013	tlsv1	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
12	(BingPreview(Dec 2013		
13	(BingPreview(Jun 2014		
14	(BingPreview(Jan 2015	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
15	Chrome(27) - Win 7	tlsv1	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
16	Chrome(28) - Win 7	tlsv1	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
17	Chrome(29) - Win 7	tlsv1	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
18	Chrome(30) - Win 7	tlsv1	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
19	Chrome(31) - Win 7	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

: Handshake Simulation

#	Name	Type	Cipher
20	Chrome(32) - Win 7	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
21	Chrome(33) - Win 7	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
22	Chrome(34) - OS X	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
23	Chrome(35) - Win 7	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
24	Chrome(36) - Win 7	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
25	Chrome(37) - OS X	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
26	Chrome(39) - OS X	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
27	Chrome(40) - OS X	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
28	Chrome(42) - OS X	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
29	Chrome(43) - OS X	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
30	Chrome(45) - OS X	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
31	Chrome(47) - OS X	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
32	Chrome(48) - OS X	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
33	Chrome(49) - Win 7	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
34	Chrome(49) - XP SP3		
35	Chrome(50) - Win 7	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
36	Chrome(51) - Win 7	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
37	Chrome(57) - Win 7	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
38	Firefox(21) - Win 7	tlsv1	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
39	Firefox(10.0.12 ESR) - Win 7	tlsv1	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA

: Handshake Simulation

#	Name	Type	Cipher
40	Firefox(17.0.7 ESR) - Win 7	tlsv1	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
41	Firefox(24.2.0 ESR) - Win 7	tlsv1	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
42	Firefox(31.3.0 ESR) - Win 7	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
43	Firefox(21) - Fedora 19		
44	Firefox(22) - Win 7	tlsv1	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
45	Firefox(24) - Win 7	tlsv1	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
46	Firefox(26) - Win 8	tlsv1	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
47	Firefox(27) - Win 8	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
48	Firefox(29) - OS X	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
49	Firefox(30) - OS X	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
50	Firefox(31) - OS X	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
51	Firefox(32) - OS X	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
52	Firefox(34) - OS X	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
53	Firefox(35) - OS X	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
54	Firefox(37) - OS X	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
55	Firefox(39) - OS X	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
56	Firefox(41) - OS X	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
57	Firefox(42) - OS X	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
58	Firefox(44) - OS X	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
59	Firefox(45) - Win 7	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

: Handshake Simulation

#	Name	Type	Cipher
60	Firefox(46) - Win 7	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
61	Firefox(47) - Win 7	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
62	Firefox(49) - XP SP3	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
63	Firefox(49) - Win 7	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
64	Firefox(53) - Win 7	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
65	(Googlebot(Oct 2013	tlsv1	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
66	(Googlebot(Jun 2014	tlsv1	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
67	(Googlebot(Feb 2015	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
68	IE(6) - XP		
69	IE(6) - XP		
70	IE(7) - Vista	tlsv1	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
71	IE(8) - XP		
72	IE(8) - XP		
73	IE(8) - Win 7	tlsv1	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
74	IE(9) - Win 7	tlsv1	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
75	IE(8-10) - Win 7	tlsv1	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
76	IE(8-10) - Win 7	tlsv1	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
77	IE(11) - Win 7	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
78	IE(11) - Win 7	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
79	IE(11) - Win 7	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

: Handshake Simulation

#	Name	Type	Cipher
80	IE(11) - Win 7	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
81	IE(11) - Win 7	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
82	IE(11) - Win 10 Preview	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
83	IE(11) - Win 8.1	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
84	IE(11) - Win 8.1	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
85	IE(11) - Win 8.1	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
86	IE(11) - Win 8.1	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
87	IE(11) - Win 8.1	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
88	IE(10) - Win Phone 8.0	tlsv1	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
89	IE(11) - Win Phone 8.1	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
90	IE(11) - Win Phone 8.1 Update	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
91	IE(11) - Win 10	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
92	IE(11) - Win 10	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
93	Edge(12) - Win 10	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
94	Edge(13) - Win 10	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
95	Edge(13) - Win 10	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
96	Edge(13) - Win Phone 10	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
97	(Java(6u45		
98	(Java(7u25	tlsv1	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
99	(Java(8b132	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256

: Handshake Simulation

#	Name	Type	Cipher
100	(Java(8u31	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
101	(OpenSSL(0.9.8y		
102	(OpenSSL(1.0.1h	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
103	(OpenSSL(1.0.1l	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
104	(OpenSSL(1.0.2e	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
105	Opera(12.15) - Win 7		
106	Opera(15) - Win 7	tlsv1	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
107	Opera(16) - Win 7	tlsv1	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
108	Opera(17) - Win 7	tlsv1	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
109	Safari(5) - iOS 5.1.1	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
110	Safari(5.1.9) - OS X 10.6.8	tlsv1	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
111	Safari(6) - iOS 6.0.1	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
112	Safari(6.0.4) - OS X 10.8.4	tlsv1	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
113	Safari(7) - iOS 7.1	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
114	Safari(8) - iOS 8.0 Beta	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
115	Safari(7) - OS X 10.9	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
116	Safari(8) - iOS 8.4	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
117	Safari(8) - OS X 10.10	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
118	Safari(9) - iOS 9	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
119	Safari(9) - OS X 10.11	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

: Handshake Simulation

#	Name	Type	Cipher
120	Safari(10) - iOS 10	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
121	Safari(10) - OS X 10.12	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
122	Apple ATS(9) - iOS 9	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
123	Tor(17.0.9) - Win 7	tlsv1	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
124	(Yahoo Slurp(Oct 2013	tlsv1	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
125	(Yahoo Slurp(Jun 2014	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
126	(Yahoo Slurp(Jan 2015	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
127	(YandexBot(3.0		
128	(YandexBot(May 2014		
129	(YandexBot(Sep 2014	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
130	(YandexBot(Jan 2015	tlsv1_2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384