بررسی SLL دامنه tochal.org

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

گزارش بررسی تنظیمات SSL دامنه tochal.org

تاریخ تهیه گزارش : یکشنبه ۲۰ تیر ۱۴۰۰ در ساعت ۱۳:۱۶

بازدید :0

امتیاز :

ارتباط تنها در SSL	معتبر	سازگاری مرورگرها	آسیب پذیری	HSTS
				

اطلاعات هدر دامنه

```
Transfer-Encoding: chunked
Content-Type: text/html; charset=utf-8
Content-Encoding: gzip
Vary: Accept-Encoding
Server: Kestrel
Set-Cookie: .AspNetCore.Mvc.CookieTempDataProvider=; expires=Thu, 01 Jan 1970 00:00:00 GMT; path=/; samesite=lax
Strict-Transport-Security: max-age=2592000
X-Powered-By: ASP.NET
Date: Sun, 11 Jul 2021 08:48:09 GMT
```

ارتباط تنها در SSL

//:http	http://tochal.org/ -> 301 -> https://tochal.org// -> 200
//:https	https://tochal.org/ -> 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) TIME :	max-age too short. 30 days (=2592000 seconds) < 15465600 seconds
HTTP Strict Transport Security (HSTS) SubDomains :	only for this domain
HTTP Strict Transport Security (HSTS) Preload :	domain is NOT marked for preloading

اطلاعات امضای دیجیتال صادر شده

اطلاعات امضای دیجیتال شماره #1

عنوان امضای دیجیتال :	tochal.org.
عنوان های جایگزین امضا (Alternative Names) :	tochal.org. , tochal.org ,
شروع اعتبار از :	دوشنبه ۰۶ بهمن ۱۳۹۹ در ساعت ۱۳:۱۰
پایان اعتبار تا :	سه شنبه ۰۵ بهمن ۱۴۰۰ در ساعت ۱۳:۱۰ - **اتمام در :** 198 روز و 4 ساعت و 24 دقیقه و 6 ثانیه
صادر کننده مجوز :	Certum Domain Validation CA SHA2
کشور صادر کننده مجوز :	PL - لهستان
الگوریتم امضا :	sha256 with RSA size: 2048 Bits
Certificate Transparency :	yes (certificate extension)
OCSP stapling :	OK - offered
OCSP URL :	http://dvcasha2.ocsp-certum.com
CRL Distribution Points :	http://crl.certum.pl/dvcasha2.crl

Trust

Android iOS Java macOS Mozilla OPENJDK Windows

بررسی اعتبار دامنه :

بررسی اعتبار دامنه :

|___ **نام هاست دامنه :** tochal.org

|___ **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 : aVv5qtiixoCZsPmbPVt29VK4GjOu7eDVH+spN/c6DX4=

Pin= : aVv5qtiixoCZsPmbPVt29VK4GjOu7eDVH+spN/c6DX4

Finger print : b75e8e7b792e5c5ccb46159c62101e1dc65d8420

عنوان : commonName=.tochal.org

صادر کننده مجوز : countryName=PL, organizationName=Unizeto Technologies S.A., organizationalUnitName=Certum Certification Authority, commonName=Certum Domain Validation CA SHA2

سریال مجوز : 8.5511716100987E+37

شروع اعتبار از : 13:10:58 25-01-2021

پایان اعتبار تا : 13:10:58 25-01-2022

الگوریتم امضا : sha256

کلید عمومی : الگوریتم : RSA

کلید عمومی : نوع : 65537

کلید عمومی : اندازه : 2048

شماره 2 : S4AbJNGvyS57nzJwv8sPMUML8VHSqH1vbiBftdPcErI=

Pin= : S4AbJNGvyS57nzJwv8sPMUML8VHSqH1vbiBftdPcErI

Finger print : ff9ceb13c83f15b800e6eff987b2c72e01b4b320

عنوان : countryName=PL, organizationName=Unizeto Technologies S.A., organizationalUnitName=Certum Certification Authority, commonName=Certum Domain Validation CA SHA2

صادر کننده مجوز : countryName=PL, organizationName=Unizeto Technologies S.A., organizationalUnitName=Certum Certification Authority, commonName=Certum Trusted Network CA

سریال مجوز : 5.1662424180299E+37

شروع اعتبار از : 12:00:00 11-09-2014

پایان اعتبار تا : 10:46:39 09-06-2027

الگوریتم امضا : sha256

کلید عمومی : الگوریتم : RSA

کلید عمومی : نوع : 65537

کلید عمومی : اندازه : 2048

شماره 3 : qiYwp7YXsE0KKUureoyqpQFubb5gSDeoOoVxn6tmfrU=

Pin : qiYwp7YXsE0KKUureoyqpQFubb5gSDeoOoVxn6tmfrU=

Finger print : 07e032e020b72c3f192f0628a2593a19a70f069e

عنوان : countryName=PL, organizationName=Unizeto Technologies S.A., organizationalUnitName=Certum Certification Authority, commonName=Certum Trusted Network CA

صادر کننده مجوز : countryName=PL, organizationName=Unizeto Technologies S.A., organizationalUnitName=Certum Certification Authority, commonName=Certum Trusted Network CA

سریال مجوز : 279744

شروع اعتبار از : 12:07:37 22-10-2008

پایان اعتبار تا : 12:07:37 31-12-2029

الگوریتم امضا : sha1

کلید عمومی : الگوریتم : RSA

کلید عمومی : نوع : 65537

کلید عمومی : اندازه : 2048

OCSP Stapling :
|___ پشتیبانی از OCSP : بلی
|___ OCSP Response : بلی
|___ |___ Trusted By Mozilla بلی
CA Store :
|___ |___ Responder ID : C = PL, O = Asseco Data Systems S.A., CN = Certum Domain Validation CA SHA2 Validation Service
|___ |___ Response Status :
|___ |___ Produced At : Jul 4 21:56:02 2021 GMT
Deflate Compression : ندارد - Type : DEFLATE
Downgrade Attacks Prevention : ندارد(TLS Fallback Scsv)
Session Renegotiation :
|___ Secure Renegotiation : خیر
|___ Insecure Client-Initiated خیر
Renegotiation :
Resumption Support :
|___ Resumption With TLS ندارد
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 نشده است
Application-Layer Protocol Negotiation ((ALPN) :	http/1.1
Personal Financial Specialist (PFS™) :	ارائه شده است
PFS Ciphers :	ECDHE-RSA-AES256-GCM-SHA384 ECDHE-RSA-AES256-SHA384 ECDHE-RSA-AES256-SHA DHE-RSA-AES256-GCM-SHA384 DHE-RSA-AES256-SHA ECDHE-RSA-AES128-GCM-SHA256 ECDHE-RSA-AES128-SHA256 ECDHE-RSA-AES128-SHA DHE-RSA-AES128-GCM-SHA256 DHE-RSA-AES128-SHA
PFS ECDHE curves :	prime256v1 secp384r1 X25519
DH Groups :	ffdhe2048
Protocol Negotiated :	Default protocol TLS1.2
Cipher Negotiated :	(ECDHE-RSA-AES256-GCM-SHA384, 256 bit ECDH (P-256
TLS Extensions :	status request/#5 renegotiation info/#65281 application layer protocol negotiation/#16 extended master secret/#23
TLS Session Ticket :	No lifetime advertised
SSL SessionID Support :	yes
Session Resumption Ticket :	پشتیبانی نمی کند
Session Resumption ID :	پشتیبانی نمی کند
TLS Timestamp :	off by +84 seconds from your localtime
DNS CAA Record :	--
Cert Transparency :	(yes (certificate extension
HTTP Status :	(/) OK 200
HTTP Strict Transport Security TIME (HSTS) :	max-age too short. 30 days (=2592000 seconds) < 15465600 seconds
HTTP Strict Transport Security (SubDomains (HSTS :	only for this domain
HTTP Strict Transport Security (Preload (HSTS :	domain is NOT marked for preloading
Banner Server :	Kestrel
HTTP Public Key Pinning (HPKP) :	No support for HTTP Public Key Pinning
Cookie Count :	/ at 1
Cookie Cecure :	at / marked as secure 0/1
Cookie HTTP Only :	at / marked as HttpOnly 0/1
Heartbleed :	آسیب پذیر نیست , no heartbeat extension
Certified Coding Specialist (CCS) :	آسیب پذیر نیست
Ticketbleed :	no session ticket extension
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

اطلاعات بیشتر

Compression Ratio Info-leak (CRIME Made Easy) :	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 نمی کند	
POODLE SSL :	آسیب پذیر نیست	اطلاعات بیشتر
CVE :	CWE-310	
SWEET32 :	uses 64 bit block ciphers	
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=FF679CA86BACD80AAD872314FACA7EA2444C2C995FFB75B56A59FF2712B5C160	اطلاعات بیشتر
CVE :	CVE-2016-0800 CVE-2016-0703	
CWE :	CWE-310	
LOGJAM Common Primes :	RFC7919/ffdhe2048	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-RSA-AES256-SHA ECDHE-RSA-AES128-SHA DHE-RSA-AES256-SHA DHE-RSA-AES128-SHA AES256-SHA AES128-SHA DES-CBC3-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, Detected ciphers: RC4-SHA RC4-MD5	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	TCP / Received RST	خیر
2	TLS_RSA_WITH_RC4_128_SHA	TCP / Received RST	خیر
3	TLS_RSA_WITH_RC4_128_MD5	TCP / Received RST	خیر
4	TLS_RSA_WITH_NULL_SHA256	TLS / No ciphers available	خیر
5	TLS_RSA_WITH_NULL_SHA	TCP / Received RST	خیر
6	TLS_RSA_WITH_NULL_MD5	TCP / Received RST	خیر
7	TLS_RSA_WITH_IDEA_CBC_SHA	TCP / Received RST	خیر
8	TLS_RSA_WITH_DES_CBC_SHA	TCP / Received RST	خیر
9	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	TCP / Received RST	خیر
10	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	TCP / Received RST	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	TCP / Received RST	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	TCP / Received RST	خیر
17	TLS_RSA_WITH_3DES_EDE_CBC_SHA	TCP / Received RST	خیر
18	TLS_RSA_EXPORT_WITH_RC4_40_MD5	TCP / Received RST	خیر

Rejected Cipher Suites :

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

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
100	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA	TCP / Received RST	خیر
101	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA	TCP / Received RST	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	TCP / Received RST	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	TCP / Received RST	خیر
108	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	TCP / Received RST	خیر
109	TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA	TCP / Received RST	خیر
110	TLS_DHE_DSS_WITH_SEED_CBC_SHA	TCP / Received RST	خیر
111	TLS_DHE_DSS_WITH_DES_CBC_SHA	TCP / Received RST	خیر
112	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA	TCP / Received RST	خیر
113	TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA	TCP / Received RST	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	TCP / Received RST	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	TCP / Received RST	خیر

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
120	TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	TCP / Received RST	خیر
121	TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA	TCP / Received RST	خیر

پشتیبانی از این پروتکل : بلی

Accepted Cipher Suites :

#	Name	Connection Status	Anonymous
1	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	Timeout on HTTP GET	خیر
2	TLS_RSA_WITH_AES_256_CBC_SHA	Timeout on HTTP GET	خیر
3	TLS_DHE_RSA_WITH_AES_256_CBC_SHA	Timeout on HTTP GET	خیر
4	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Timeout on HTTP GET	خیر
5	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	Timeout on HTTP GET	خیر
6	TLS_RSA_WITH_AES_128_CBC_SHA	Timeout on HTTP GET	خیر
7	TLS_RSA_WITH_RC4_128_SHA	Timeout on HTTP GET	خیر
8	TLS_RSA_WITH_RC4_128_MD5	Timeout on HTTP GET	خیر
9	TLS_RSA_WITH_3DES_EDE_CBC_SHA	Timeout on HTTP GET	خیر

Preferred Cipher Suites :

#	Name	Connection Status	Anonymous
1	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	Timeout on HTTP GET	خیر

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
1	TLS_RSA_WITH_SEED_CBC_SHA	TCP / Received RST	خیر
2	TLS_RSA_WITH_NULL_SHA256	TLS / No ciphers available	خیر
3	TLS_RSA_WITH_NULL_SHA	TCP / Received RST	خیر
4	TLS_RSA_WITH_NULL_MD5	TCP / Received RST	خیر
5	TLS_RSA_WITH_IDEA_CBC_SHA	TCP / Received RST	خیر
6	TLS_RSA_WITH_DES_CBC_SHA	TCP / Received RST	خیر
7	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	TCP / Received RST	خیر
8	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	TCP / Received RST	خیر

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
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_EXPORT_WITH_RC4_40_MD5	TCP / Received RST	خیر
14	TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5	TCP / Received RST	خیر
15	TLS_RSA_EXPORT_WITH_DES40_CBC_SHA	TCP / Received RST	خیر
16	TLS_ECDH_anon_WITH_RC4_128_SHA	TCP / Received RST	بلی
17	TLS_ECDH_anon_WITH_NULL_SHA	TCP / Received RST	بلی
18	TLS_ECDH_anon_WITH_AES_256_CBC_SHA	TCP / Received RST	بلی
19	TLS_ECDH_anon_WITH_AES_128_CBC_SHA	TCP / Received RST	بلی
20	TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA	TCP / Received RST	بلی
21	TLS_ECDH_RSA_WITH_RC4_128_SHA	TCP / Received RST	خیر
22	TLS_ECDH_RSA_WITH_NULL_SHA	TCP / Received RST	خیر
23	TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384	TLS / No ciphers available	خیر
24	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384	TLS / No ciphers available	خیر
25	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA	TCP / Received RST	خیر
26	TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256	TLS / No ciphers available	خیر
27	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256	TLS / No ciphers available	خیر
28	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA	TCP / Received RST	خیر
29	TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA	TCP / Received RST	خیر

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
30	TLS_ECDH_ECDSA_WITH_RC4_128_SHA	TCP / Received RST	خیر
31	TLS_ECDH_ECDSA_WITH_NULL_SHA	TCP / Received RST	خیر
32	TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384	TLS / No ciphers available	خیر
33	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384	TLS / No ciphers available	خیر
34	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA	TCP / Received RST	خیر
35	TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256	TLS / No ciphers available	خیر
36	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256	TLS / No ciphers available	خیر
37	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA	TCP / Received RST	خیر
38	TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA	TCP / Received RST	خیر
39	TLS_ECDHE_RSA_WITH_RC4_128_SHA	TCP / Received RST	خیر
40	TLS_ECDHE_RSA_WITH_NULL_SHA	TCP / Received RST	خیر
41	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	TLS / No ciphers available	خیر
42	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	TLS / No ciphers available	خیر
43	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	TLS / No ciphers available	خیر
44	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	TLS / No ciphers available	خیر
45	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	TCP / Received RST	خیر
46	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA	TCP / Received RST	خیر
47	TLS_ECDHE_ECDSA_WITH_NULL_SHA	TCP / Received RST	خیر
48	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	TLS / No ciphers available	خیر
49	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	TLS / No ciphers available	خیر

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
50	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	TCP / Received RST	خیر
51	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	TLS / No ciphers available	خیر
52	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	TLS / No ciphers available	خیر
53	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	TCP / Received RST	خیر
54	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	TCP / Received RST	خیر
55	TLS_DH_anon_WITH_SEED_CBC_SHA	TCP / Received RST	بلی
56	TLS_DH_anon_WITH_RC4_128_MD5	TCP / Received RST	بلی
57	TLS_DH_anon_WITH_DES_CBC_SHA	TCP / Received RST	بلی
58	TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA	TCP / Received RST	بلی
59	TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA	TCP / Received RST	بلی
60	TLS_DH_anon_WITH_AES_256_GCM_SHA384	TLS / No ciphers available	بلی
61	TLS_DH_anon_WITH_AES_256_CBC_SHA256	TLS / No ciphers available	بلی
62	TLS_DH_anon_WITH_AES_256_CBC_SHA	TCP / Received RST	بلی
63	TLS_DH_anon_WITH_AES_128_GCM_SHA256	TLS / No ciphers available	بلی
64	TLS_DH_anon_WITH_AES_128_CBC_SHA256	TLS / No ciphers available	بلی
65	TLS_DH_anon_WITH_AES_128_CBC_SHA	TCP / Received RST	بلی
66	TLS_DH_anon_WITH_3DES_EDE_CBC_SHA	TCP / Received RST	بلی
67	TLS_DH_anon_EXPORT_WITH_RC4_40_MD5	TCP / Received RST	بلی
68	TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA	TCP / Received RST	بلی
69	TLS_DH_RSA_WITH_SEED_CBC_SHA	TCP / Received RST	خیر

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
70	TLS_DH_RSA_WITH_DES_CBC_SHA	TCP / Received RST	خیر
71	TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA	TCP / Received RST	خیر
72	TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA	TCP / Received RST	خیر
73	TLS_DH_RSA_WITH_AES_256_GCM_SHA384	TLS / No ciphers available	خیر
74	TLS_DH_RSA_WITH_AES_256_CBC_SHA256	TLS / No ciphers available	خیر
75	TLS_DH_RSA_WITH_AES_256_CBC_SHA	TCP / Received RST	خیر
76	TLS_DH_RSA_WITH_AES_128_GCM_SHA256	TLS / No ciphers available	خیر
77	TLS_DH_RSA_WITH_AES_128_CBC_SHA256	TLS / No ciphers available	خیر
78	TLS_DH_RSA_WITH_AES_128_CBC_SHA	TCP / Received RST	خیر
79	TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA	TCP / Received RST	خیر
80	TLS_DH_DSS_WITH_SEED_CBC_SHA	TCP / Received RST	خیر
81	TLS_DH_DSS_WITH_DES_CBC_SHA	TCP / Received RST	خیر
82	TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA	TCP / Received RST	خیر
83	TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA	TCP / Received RST	خیر
84	TLS_DH_DSS_WITH_AES_256_GCM_SHA384	TLS / No ciphers available	خیر
85	TLS_DH_DSS_WITH_AES_256_CBC_SHA256	TLS / No ciphers available	خیر
86	TLS_DH_DSS_WITH_AES_256_CBC_SHA	TCP / Received RST	خیر
87	TLS_DH_DSS_WITH_AES_128_GCM_SHA256	TLS / No ciphers available	خیر
88	TLS_DH_DSS_WITH_AES_128_CBC_SHA256	TLS / No ciphers available	خیر
89	TLS_DH_DSS_WITH_AES_128_CBC_SHA	TCP / Received RST	خیر

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
90	TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA	TCP / Received RST	خیر
91	TLS_DHE_RSA_WITH_SEED_CBC_SHA	TCP / Received RST	خیر
92	TLS_DHE_RSA_WITH_DES_CBC_SHA	TCP / Received RST	خیر
93	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA	TCP / Received RST	خیر
94	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA	TCP / Received RST	خیر
95	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	TLS / No ciphers available	خیر
96	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	TLS / No ciphers available	خیر
97	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	TLS / No ciphers available	خیر
98	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	TLS / No ciphers available	خیر
99	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	TCP / Received RST	خیر
100	TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA	TCP / Received RST	خیر
101	TLS_DHE_DSS_WITH_SEED_CBC_SHA	TCP / Received RST	خیر
102	TLS_DHE_DSS_WITH_DES_CBC_SHA	TCP / Received RST	خیر
103	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA	TCP / Received RST	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	TCP / Received RST	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
109	TLS_DHE_DSS_WITH_AES_128_CBC_SHA	TCP / Received RST	خیر

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
110	TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	TCP / Received RST	خیر
111	TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA	TCP / Received RST	خیر

پشتیبانی از این پروتکل : بلی

Accepted Cipher Suites :

#	Name	Connection Status	Anonymous
1	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	Timeout on HTTP GET	خیر
2	TLS_DHE_RSA_WITH_AES_256_CBC_SHA	Timeout on HTTP GET	خیر
3	TLS_RSA_WITH_AES_256_CBC_SHA	Timeout on HTTP GET	خیر
4	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Timeout on HTTP GET	خیر
5	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	Timeout on HTTP GET	خیر
6	TLS_RSA_WITH_AES_128_CBC_SHA	Timeout on HTTP GET	خیر
7	TLS_RSA_WITH_RC4_128_SHA	Timeout on HTTP GET	خیر
8	TLS_RSA_WITH_RC4_128_MD5	Timeout on HTTP GET	خیر
9	TLS_RSA_WITH_3DES_EDE_CBC_SHA	Timeout on HTTP GET	خیر

Preferred Cipher Suites :

#	Name	Connection Status	Anonymous
1	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	Timeout on HTTP GET	خیر

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
1	TLS_RSA_WITH_SEED_CBC_SHA	TCP / Received RST	خیر
2	TLS_RSA_WITH_NULL_SHA256	TLS / No ciphers available	خیر
3	TLS_RSA_WITH_NULL_SHA	TCP / Received RST	خیر
4	TLS_RSA_WITH_NULL_MD5	TCP / Received RST	خیر
5	TLS_RSA_WITH_IDEA_CBC_SHA	TCP / Received RST	خیر
6	TLS_RSA_WITH_DES_CBC_SHA	TCP / Received RST	خیر
7	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	TCP / Received RST	خیر
8	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	TCP / Received RST	خیر

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
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_EXPORT_WITH_RC4_40_MD5	TCP / Received RST	خیر
14	TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5	TCP / Received RST	خیر
15	TLS_RSA_EXPORT_WITH_DES40_CBC_SHA	TCP / Received RST	خیر
16	TLS_ECDH_anon_WITH_RC4_128_SHA	TCP / Received RST	بلی
17	TLS_ECDH_anon_WITH_NULL_SHA	TCP / Received RST	بلی
18	TLS_ECDH_anon_WITH_AES_256_CBC_SHA	TCP / Received RST	بلی
19	TLS_ECDH_anon_WITH_AES_128_CBC_SHA	TCP / Received RST	بلی
20	TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA	TCP / Received RST	بلی
21	TLS_ECDH_RSA_WITH_RC4_128_SHA	TCP / Received RST	خیر
22	TLS_ECDH_RSA_WITH_NULL_SHA	TCP / Received RST	خیر
23	TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384	TLS / No ciphers available	خیر
24	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384	TLS / No ciphers available	خیر
25	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA	TCP / Received RST	خیر
26	TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256	TLS / No ciphers available	خیر
27	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256	TLS / No ciphers available	خیر
28	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA	TCP / Received RST	خیر
29	TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA	TCP / Received RST	خیر

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
30	TLS_ECDH_ECDSA_WITH_RC4_128_SHA	TCP / Received RST	خیر
31	TLS_ECDH_ECDSA_WITH_NULL_SHA	TCP / Received RST	خیر
32	TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384	TLS / No ciphers available	خیر
33	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384	TLS / No ciphers available	خیر
34	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA	TCP / Received RST	خیر
35	TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256	TLS / No ciphers available	خیر
36	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256	TLS / No ciphers available	خیر
37	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA	TCP / Received RST	خیر
38	TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA	TCP / Received RST	خیر
39	TLS_ECDHE_RSA_WITH_RC4_128_SHA	TCP / Received RST	خیر
40	TLS_ECDHE_RSA_WITH_NULL_SHA	TCP / Received RST	خیر
41	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	TLS / No ciphers available	خیر
42	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	TLS / No ciphers available	خیر
43	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	TLS / No ciphers available	خیر
44	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	TLS / No ciphers available	خیر
45	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	TCP / Received RST	خیر
46	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA	TCP / Received RST	خیر
47	TLS_ECDHE_ECDSA_WITH_NULL_SHA	TCP / Received RST	خیر
48	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	TLS / No ciphers available	خیر
49	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	TLS / No ciphers available	خیر

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
50	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	TCP / Received RST	خیر
51	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	TLS / No ciphers available	خیر
52	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	TLS / No ciphers available	خیر
53	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	TCP / Received RST	خیر
54	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	TCP / Received RST	خیر
55	TLS_DH_anon_WITH_SEED_CBC_SHA	TCP / Received RST	بلی
56	TLS_DH_anon_WITH_RC4_128_MD5	TCP / Received RST	بلی
57	TLS_DH_anon_WITH_DES_CBC_SHA	TCP / Received RST	بلی
58	TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA	TCP / Received RST	بلی
59	TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA	TCP / Received RST	بلی
60	TLS_DH_anon_WITH_AES_256_GCM_SHA384	TLS / No ciphers available	بلی
61	TLS_DH_anon_WITH_AES_256_CBC_SHA256	TLS / No ciphers available	بلی
62	TLS_DH_anon_WITH_AES_256_CBC_SHA	TCP / Received RST	بلی
63	TLS_DH_anon_WITH_AES_128_GCM_SHA256	TLS / No ciphers available	بلی
64	TLS_DH_anon_WITH_AES_128_CBC_SHA256	TLS / No ciphers available	بلی
65	TLS_DH_anon_WITH_AES_128_CBC_SHA	TCP / Received RST	بلی
66	TLS_DH_anon_WITH_3DES_EDE_CBC_SHA	TCP / Received RST	بلی
67	TLS_DH_anon_EXPORT_WITH_RC4_40_MD5	TCP / Received RST	بلی
68	TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA	TCP / Received RST	بلی
69	TLS_DH_RSA_WITH_SEED_CBC_SHA	TCP / Received RST	خیر

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
70	TLS_DH_RSA_WITH_DES_CBC_SHA	TCP / Received RST	خیر
71	TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA	TCP / Received RST	خیر
72	TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA	TCP / Received RST	خیر
73	TLS_DH_RSA_WITH_AES_256_GCM_SHA384	TLS / No ciphers available	خیر
74	TLS_DH_RSA_WITH_AES_256_CBC_SHA256	TLS / No ciphers available	خیر
75	TLS_DH_RSA_WITH_AES_256_CBC_SHA	TCP / Received RST	خیر
76	TLS_DH_RSA_WITH_AES_128_GCM_SHA256	TLS / No ciphers available	خیر
77	TLS_DH_RSA_WITH_AES_128_CBC_SHA256	TLS / No ciphers available	خیر
78	TLS_DH_RSA_WITH_AES_128_CBC_SHA	TCP / Received RST	خیر
79	TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA	TCP / Received RST	خیر
80	TLS_DH_DSS_WITH_SEED_CBC_SHA	TCP / Received RST	خیر
81	TLS_DH_DSS_WITH_DES_CBC_SHA	TCP / Received RST	خیر
82	TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA	TCP / Received RST	خیر
83	TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA	TCP / Received RST	خیر
84	TLS_DH_DSS_WITH_AES_256_GCM_SHA384	TLS / No ciphers available	خیر
85	TLS_DH_DSS_WITH_AES_256_CBC_SHA256	TLS / No ciphers available	خیر
86	TLS_DH_DSS_WITH_AES_256_CBC_SHA	TCP / Received RST	خیر
87	TLS_DH_DSS_WITH_AES_128_GCM_SHA256	TLS / No ciphers available	خیر
88	TLS_DH_DSS_WITH_AES_128_CBC_SHA256	TLS / No ciphers available	خیر
89	TLS_DH_DSS_WITH_AES_128_CBC_SHA	TCP / Received RST	خیر

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
90	TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA	TCP / Received RST	خیر
91	TLS_DHE_RSA_WITH_SEED_CBC_SHA	TCP / Received RST	خیر
92	TLS_DHE_RSA_WITH_DES_CBC_SHA	TCP / Received RST	خیر
93	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA	TCP / Received RST	خیر
94	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA	TCP / Received RST	خیر
95	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	TLS / No ciphers available	خیر
96	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	TLS / No ciphers available	خیر
97	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	TLS / No ciphers available	خیر
98	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	TLS / No ciphers available	خیر
99	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	TCP / Received RST	خیر
100	TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA	TCP / Received RST	خیر
101	TLS_DHE_DSS_WITH_SEED_CBC_SHA	TCP / Received RST	خیر
102	TLS_DHE_DSS_WITH_DES_CBC_SHA	TCP / Received RST	خیر
103	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA	TCP / Received RST	خیر
104	TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA	TCP / Received RST	خیر
105	TLS_DHE_DSS_WITH_AES_256_GCM_SHA384	TLS / No ciphers available	خیر
106	TLS_DHE_DSS_WITH_AES_256_CBC_SHA256	TLS / No ciphers available	خیر
107	TLS_DHE_DSS_WITH_AES_256_CBC_SHA	TCP / Received RST	خیر
108	TLS_DHE_DSS_WITH_AES_128_GCM_SHA256	TLS / No ciphers available	خیر
109	TLS_DHE_DSS_WITH_AES_128_CBC_SHA256	TLS / No ciphers available	خیر

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
110	TLS_DHE_DSS_WITH_AES_128_CBC_SHA	TCP / Received RST	خیر
111	TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	TCP / Received RST	خیر
112	TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA	TCP / Received RST	خیر

پشتیبانی از این پروتکل : بلی

Accepted Cipher Suites :

#	Name	Connection Status	Anonymous
1	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	Timeout on HTTP GET	خیر
2	TLS_RSA_WITH_AES_256_CBC_SHA256	Timeout on HTTP GET	خیر
3	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	Timeout on HTTP GET	خیر
4	TLS_DHE_RSA_WITH_AES_256_CBC_SHA	Timeout on HTTP GET	خیر
5	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	Timeout on HTTP GET	خیر
6	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	Timeout on HTTP GET	خیر
7	TLS_RSA_WITH_AES_256_CBC_SHA	Timeout on HTTP GET	خیر
8	TLS_RSA_WITH_AES_256_GCM_SHA384	HTTP 200 OK	خیر
9	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Timeout on HTTP GET	خیر
10	TLS_RSA_WITH_RC4_128_MD5	Timeout on HTTP GET	خیر
11	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	Timeout on HTTP GET	خیر
12	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	Timeout on HTTP GET	خیر
13	TLS_RSA_WITH_AES_128_CBC_SHA	Timeout on HTTP GET	خیر
14	TLS_RSA_WITH_AES_128_CBC_SHA256	Timeout on HTTP GET	خیر
15	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	Timeout on HTTP GET	خیر
16	TLS_RSA_WITH_AES_128_GCM_SHA256	Timeout on HTTP GET	خیر
17	TLS_RSA_WITH_RC4_128_SHA	Timeout on HTTP GET	خیر
18	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	Timeout on HTTP GET	خیر
19	TLS_RSA_WITH_3DES_EDE_CBC_SHA	Timeout on HTTP GET	خیر

Preferred Cipher Suites :

#	Name	Connection Status	Anonymous

Preferred Cipher Suites :

#	Name	Connection Status	Anonymous
1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	HTTP 200 OK	خیر

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
1	TLS_RSA_WITH_SEED_CBC_SHA	TCP / Received RST	خیر
2	TLS_RSA_WITH_NULL_SHA256	TCP / Received RST	خیر
3	TLS_RSA_WITH_NULL_SHA	TCP / Received RST	خیر
4	TLS_RSA_WITH_NULL_MD5	TCP / Received RST	خیر
5	TLS_RSA_WITH_IDEA_CBC_SHA	TCP / Received RST	خیر
6	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256	TCP / Received RST	خیر
7	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	TCP / Received RST	خیر
8	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256	TCP / Received RST	خیر
9	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	TCP / Received RST	خیر
10	TLS_ECDH_anon_WITH_RC4_128_SHA	TCP / Received RST	بلی
11	TLS_ECDH_anon_WITH_NULL_SHA	TCP / Received RST	بلی
12	TLS_ECDH_anon_WITH_AES_256_CBC_SHA	TCP / Received RST	بلی
13	TLS_ECDH_anon_WITH_AES_128_CBC_SHA	TCP / Received RST	بلی
14	TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA	TCP / Received RST	بلی
15	TLS_ECDHE_RSA_WITH_RC4_128_SHA	TCP / Received RST	خیر
16	TLS_ECDHE_RSA_WITH_NULL_SHA	TCP / Received RST	خیر
17	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	TCP / Received RST	خیر
18	TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384	TCP / Received RST	خیر
19	TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256	TCP / Received RST	خیر

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
20	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	TCP / Received RST	خیر
21	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA	TCP / Received RST	خیر
22	TLS_ECDHE_ECDSA_WITH_NULL_SHA	TCP / Received RST	خیر
23	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	TCP / Received RST	خیر
24	TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_CBC_SHA384	TCP / Received RST	خیر
25	TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_CBC_SHA256	TCP / Received RST	خیر
26	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	TCP / Received RST	خیر
27	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	TCP / Received RST	خیر
28	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	TCP / Received RST	خیر
29	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	TCP / Received RST	خیر
30	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	TCP / Received RST	خیر
31	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	TCP / Received RST	خیر
32	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	TCP / Received RST	خیر
33	TLS_DH_anon_WITH_SEED_CBC_SHA	TCP / Received RST	بلی
34	TLS_DH_anon_WITH_RC4_128_MD5	TCP / Received RST	بلی
35	TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA256	TLS / No ciphers available	بلی
36	TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA	TCP / Received RST	بلی
37	TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA256	TLS / No ciphers available	بلی
38	TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA	TCP / Received RST	بلی
39	TLS_DH_anon_WITH_AES_256_GCM_SHA384	TCP / Received RST	بلی

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
40	TLS_DH_anon_WITH_AES_256_CBC_SHA256	TCP / Received RST	بلی
41	TLS_DH_anon_WITH_AES_256_CBC_SHA	TCP / Received RST	بلی
42	TLS_DH_anon_WITH_AES_128_GCM_SHA256	TCP / Received RST	بلی
43	TLS_DH_anon_WITH_AES_128_CBC_SHA256	TCP / Received RST	بلی
44	TLS_DH_anon_WITH_AES_128_CBC_SHA	TCP / Received RST	بلی
45	TLS_DH_anon_WITH_3DES_EDE_CBC_SHA	TCP / Received RST	بلی
46	TLS_DHE_RSA_WITH_SEED_CBC_SHA	TCP / Received RST	خیر
47	TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256	TCP / Received RST	خیر
48	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256	TCP / Received RST	خیر
49	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA	TCP / Received RST	خیر
50	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256	TCP / Received RST	خیر
51	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA	TCP / Received RST	خیر
52	TLS_DHE_RSA_WITH_AES_256_CCM	TCP / Received RST	خیر
53	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	TCP / Received RST	خیر
54	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	TCP / Received RST	خیر
55	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	TCP / Received RST	خیر
56	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA256	TCP / Received RST	خیر
57	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA	TCP / Received RST	خیر
58	TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA256	TCP / Received RST	خیر
59	TLS_DHE_DSS_WITH_AES_256_GCM_SHA384	TCP / Received RST	خیر

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
60	TLS_DHE_DSS_WITH_AES_256_CBC_SHA256	TCP / Received RST	خیر
61	TLS_DHE_DSS_WITH_AES_256_CBC_SHA	TCP / Received RST	خیر
62	TLS_DHE_DSS_WITH_AES_128_GCM_SHA256	TCP / Received RST	خیر
63	TLS_DHE_DSS_WITH_AES_128_CBC_SHA256	TCP / Received RST	خیر
64	TLS_DHE_DSS_WITH_AES_128_CBC_SHA	TCP / Received RST	خیر
65	TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	TCP / Received RST	خیر
66	RSA_WITH_AES_256_CCM_8	TCP / Received RST	خیر
67	RSA_WITH_AES_256_CCM	TCP / Received RST	خیر
68	RSA_WITH_AES_128_CCM_8	TCP / Received RST	خیر
69	RSA_WITH_AES_128_CCM	TCP / Received RST	خیر
70	ECDHE_ECDSA_WITH_AES_256_CCM_8	TCP / Received RST	خیر
71	ECDHE_ECDSA_WITH_AES_256_CCM	TCP / Received RST	خیر
72	ECDHE_ECDSA_WITH_AES_128_CCM_8	TCP / Received RST	خیر
73	ECDHE_ECDSA_WITH_AES_128_CCM	TCP / Received RST	خیر
74	ECDHE-ECDSA-ARIA256-GCM-SHA384	TCP / Received RST	خیر
75	ECDHE-ECDSA-ARIA128-GCM-SHA256	TCP / Received RST	خیر
76	ECDHE-ARIA256-GCM-SHA384	TCP / Received RST	خیر
77	ECDHE-ARIA128-GCM-SHA256	TCP / Received RST	خیر
78	DHE_RSA_WITH_AES_256_CCM_8	TCP / Received RST	خیر
79	DHE_RSA_WITH_AES_128_CCM_8	TCP / Received RST	خیر

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
80	DHE_RSA_WITH_AES_128_CCM	TCP / Received RST	خیر
81	DHE-RSA-ARIA256-GCM-SHA384	TCP / Received RST	خیر
82	DHE-RSA-ARIA128-GCM-SHA256	TCP / Received RST	خیر
83	DHE-DSS-ARIA256-GCM-SHA384	TCP / Received RST	خیر
84	DHE-DSS-ARIA128-GCM-SHA256	TCP / Received RST	خیر
85	ARIA256-GCM-SHA384	TCP / Received RST	خیر
86	ARIA128-GCM-SHA256	TCP / Received RST	خیر

: Handshake Simulation

#	Name	Type	Cipher
1	(Android(2.3.7	tlsv1	TLS_RSA_WITH_RC4_128_MD5
2	(Android(4.0.4	tlsv1	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
3	(Android(4.1.1	tlsv1	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
4	(Android(4.2.2	tlsv1	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
5	(Android(4.3	tlsv1	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	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	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
11	(BingBot(Dec 2013	tlsv1	TLS_RSA_WITH_AES_128_CBC_SHA
12	(BingPreview(Dec 2013	tlsv1	TLS_DHE_RSA_WITH_AES_256_CBC_SHA
13	(BingPreview(Jun 2014	tlsv1	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	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
16	Chrome(28) - Win 7	tlsv1	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
17	Chrome(29) - Win 7	tlsv1	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
18	Chrome(30) - Win 7	tlsv1	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	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
39	Firefox(10.0.12 ESR) - Win 7	tlsv1	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA

: Handshake Simulation

#	Name	Type	Cipher
40	Firefox(17.0.7 ESR) - Win 7	tlsv1	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
41	Firefox(24.2.0 ESR) - Win 7	tlsv1	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	TLS_DHE_RSA_WITH_AES_256_CBC_SHA
44	Firefox(22) - Win 7	tlsv1	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
45	Firefox(24) - Win 7	tlsv1	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
46	Firefox(26) - Win 8	tlsv1	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	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
66	(Googlebot(Jun 2014	tlsv1	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	tlsv1	TLS_RSA_WITH_RC4_128_MD5
69	IE(6) - XP	tlsv1	TLS_RSA_WITH_RC4_128_MD5
70	IE(7) - Vista	tlsv1	TLS_RSA_WITH_AES_128_CBC_SHA
71	IE(8) - XP	tlsv1	TLS_RSA_WITH_RC4_128_MD5
72	IE(8) - XP	tlsv1	TLS_RSA_WITH_RC4_128_MD5
73	IE(8) - Win 7	tlsv1	TLS_RSA_WITH_AES_128_CBC_SHA
74	IE(9) - Win 7	tlsv1	TLS_RSA_WITH_AES_128_CBC_SHA
75	IE(8-10) - Win 7	tlsv1	TLS_RSA_WITH_AES_128_CBC_SHA
76	IE(8-10) - Win 7	tlsv1	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	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	TLS_RSA_WITH_RC4_128_MD5
98	(Java(7u25	tlsv1	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	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_RSA_WITH_AES_256_CBC_SHA256
106	Opera(15) - Win 7	tlsv1	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
107	Opera(16) - Win 7	tlsv1	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
108	Opera(17) - Win 7	tlsv1	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	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	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	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
124	(Yahoo Slurp(Oct 2013	tlsv1	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	tlsv1	TLS_RSA_WITH_3DES_EDE_CBC_SHA
128	(YandexBot(May 2014	tlsv1	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