بررسی SLL دامنه www.palayesazan.com

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

گزارش بررسی تنظیمات SSL دامنه www.palayesazan.com

تاریخ تهیه گزارش : سه شنبه ۰۸ تیر ۱۴۰۰ در ساعت ۱۵:۴۸

بازدید :0

امتیاز :

ارتباط تنها در SSL	معتبر	سازگاری مرورگرها	آسیب پذیری	HSTS
				

اطلاعات هدر دامنه

```
Server: nginx
Date: Tue, 29 Jun 2021 11:18:14 GMT
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Connection: keep-alive
P3P: CP="NOI ADM DEV PSAi COM NAV OUR OTRo STP IND DEM", CP="NOI ADM DEV PSAi COM NAV OUR OTRo STP IND DEM"
Expires: Wed, 17 Aug 2005 00:00:00 GMT
Pragma: no-cache, no-cache
Content-Encoding: gzip
Vary: Accept-Encoding,User-Agent
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0, no-cache, no-store, no-cache, must-revalidate, max-age=0
Set-Cookie: fad4bda4a6173f69040f42cae79600e3=h4p7d4r76bna3mk0koaohokmh4; path=/; domain=palayesazan.com; HttpOnly; HTTPOnly; Secure
X-Frame-Options: sameorigin
Content-Security-Policy: frame-src 'self' *.google-analytics.com *.raychat.io *.google.com
Last-Modified: Tue, 29 Jun 2021 03:25:28 GMT
ETag: "3ed38364dd3df30024e6d3ed72f2f799"
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
X-Download-Options: noopen
Referrer-Policy: strict-origin-when-cross-origin
Strict-Transport-Security: max-age=16416000; includeSubdomains
```

ارتباط تنها در SSL

//:http
//:https

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 :	190 seconds > 15465600 seconds (=16416000 seconds) days
HTTP Strict Transport Security (HSTS) SubDomains :	includes subdomains
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 :	palayesazan.com
نام کشور :	IR - جمهوری اسلامی ایران
عنوان های جایگزین امضا (Alternative Names) :	www.palayesazan.com , palayesazan.com ,
شروع اعتبار از :	چهارشنبه ۲۹ مرداد ۱۳۹۹ در ساعت ۱۲:۴۵
پایان اعتبار تا :	چهارشنبه ۲۷ مرداد ۱۴۰۰ در ساعت ۱۲:۴۵ - **اتمام در :** 50 روز و 27 دقیقه و 31 ثانیه
صادر کننده مجوز :	Certum Organization Validation CA SHA2
کشور صادر کننده مجوز :	PL - لهستان
الگوریتم امضا :	sha256 with RSA size: 2048 Bits
Certificate Transparency :	yes (certificate extension)
OCSP stapling :	LOW - not offered
OCSP URL :	http://ovcasha2.ocsp-certum.com
CRL Distribution Points :	http://crl.certum.pl/ovcasha2.crl

Trust

Android iOS Java macOS Mozilla OPENJDK Windows

بررسی اعتبار دامنه :

بررسی اعتبار دامنه :

|___ **نام هاست دامنه :** www.palayesazan.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 : mte8FUD6XmUhzarOASe+g5+N7O05zjQPCdrreXKLzms=

Pin= : mte8FUD6XmUhzarOASe+g5+N7O05zjQPCdrreXKLzms

Finger print : dbd3b868eb26d31b9092aef0a84976937834dc7d

عنوان : countryName=IR, stateOrProvinceName=Khorasan Razavi, localityName=Mashhad, organizationalUnitName=Palaye Sazan Farayand Toos Co., organizationName=Palaye Sazan Farayand Toos Co., commonName=palayesazan.com

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

سریال مجوز : 1.2795479056779E+38

شروع اعتبار از : 12:45:50 19-08-2020

پایان اعتبار تا : 12:45:50 18-08-2021

الگوریتم امضا : sha256

کلید عمومی : الگوریتم : RSA

کلید عمومی : نوع : 65537

کلید عمومی : اندازه : 2048

شماره 2 : 51GveKNrpJjtGpXY5QDx03s3YTQwaQic6dWBqo3zX6s=

Pin= : 51GveKNrpJjtGpXY5QDx03s3YTQwaQic6dWBqo3zX6s

Finger print : fa5f98e8022e8105dbdf2448656ae576c131cb28

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

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

سریال مجوز : 2.4148884671458E+38

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

Next Protocol Negotiation extension ((NPN) :	ارائه شده است (with h2, http/1.1 (advertised
Application-Layer Protocol Negotiation ((ALPN) :	ارائه نشده است
Personal Financial Specialist (PFS™) :	ارائه شده است
PFS Ciphers :	ECDHE-RSA-AES256-GCM-SHA384 DHE-RSA-AES256-GCM-SHA384 ECDHE-RSA-AES128-GCM-SHA256 DHE-RSA-AES128-GCM-SHA256
PFS ECDHE curves :	prime256v1
DH Groups :	ffdhe4096
Protocol Negotiated :	Default protocol TLS1.2
Cipher Negotiated :	(ECDHE-RSA-AES128-GCM-SHA256, 256 bit ECDH (P-256
TLS Extensions :	server name/#0 renegotiation info/#65281 EC point formats/#11 session ticket/#35 heartbeat/#15 next protocol/#13172
TLS Session Ticket :	(valid for 300 seconds only (< daily
SSL SessionID Support :	yes
Session Resumption Ticket :	پشتیبانی می کند
Session Resumption ID :	پشتیبانی می کند
TLS Timestamp :	off by -1 seconds from your localtime
DNS CAA Record :	--
Cert Transparency :	(yes (certificate extension
HTTP Status :	(/) OK 200
HTTP Strict Transport Security TIME (HSTS) :	days (=16416000 seconds) > 15465600 seconds 190
HTTP Strict Transport Security (SubDomains (HSTS :	includes subdomains
HTTP Strict Transport Security (Preload (HSTS :	domain is NOT marked for preloading
Banner Server :	nginx
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 , timed out
Certified Coding Specialist (CCS) :	آسیب پذیر نیست
Ticketbleed :	آسیب پذیر نیست , returned potential memory fragments do not differ
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

اطلاعات بیشتر

آسیب پذیری های امضای دیجیتال

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 :	no protocol below TLS 1.2 offered	
POODLE SSL :	آسیب پذیر نیست	اطلاعات بیشتر
CVE :	CWE-310	
SWEET32 :	آسیب پذیر نیست	
CVE :	CVE-2016-6329 CVE-2016-2183	
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=2E9D7E3760A619DB9DA99DD87D8BD30A091808C9C7D759F99D20841DB5607956	اطلاعات بیشتر
CVE :	CVE-2016-0703 CVE-2016-0800	
CWE :	CWE-310	
LOGJAM Common Primes :	RFC7919/ffdhe4096	اطلاعات بیشتر
CVE :	CVE-2015-4000	
CWE :	CWE-310	
LOGJAM :	آسیب پذیر نیست , no DH EXPORT ciphers,	اطلاعات بیشتر
CVE :	CVE-2015-4000	
CWE :	CWE-310	
BEAST :	آسیب پذیر نیست , no SSL3 or TLS1	اطلاعات بیشتر
CVE :	CVE-2011-3389	
CWE :	CWE-20	
LUCKY 13 :	آسیب پذیر نیست	
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	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 : خیر

Accepted Cipher Suites :

#	Name	Connection Status	Anonymous

Preferred Cipher Suites :

#	Name	Connection Status	Anonymous
1			خیر

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
1	TLS_RSA_WITH_SEED_CBC_SHA	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

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
19	TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5	TCP / Received RST	خیر
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_128_CBC_SHA	TCP / Received RST	بلی
24	TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA	TCP / Received RST	بلی
25	TLS_ECDH_RSA_WITH_RC4_128_SHA	TCP / Received RST	خیر
26	TLS_ECDH_RSA_WITH_NULL_SHA	TCP / Received RST	خیر
27	TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384	TLS / No ciphers available	خیر
28	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384	TLS / No ciphers available	خیر
29	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA	TCP / Received RST	خیر
30	TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256	TLS / No ciphers available	خیر
31	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256	TLS / No ciphers available	خیر
32	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA	TCP / Received RST	خیر
33	TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA	TCP / Received RST	خیر
34	TLS_ECDH_ECDSA_WITH_RC4_128_SHA	TCP / Received RST	خیر
35	TLS_ECDH_ECDSA_WITH_NULL_SHA	TCP / Received RST	خیر
36	TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384	TLS / No ciphers available	خیر
37	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384	TLS / No ciphers available	خیر
38	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA	TCP / Received RST	خیر

Rejected Cipher Suites :

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

Rejected Cipher Suites :

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

Rejected Cipher Suites :

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

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
99	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA	TCP / Received RST	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	TCP / Received RST	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	TCP / Received RST	خیر
106	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	TCP / Received RST	خیر
107	TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA	TCP / Received RST	خیر
108	TLS_DHE_DSS_WITH_SEED_CBC_SHA	TCP / Received RST	خیر
109	TLS_DHE_DSS_WITH_DES_CBC_SHA	TCP / Received RST	خیر
110	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA	TCP / Received RST	خیر
111	TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA	TCP / Received RST	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	TCP / Received RST	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
117	TLS_DHE_DSS_WITH_AES_128_CBC_SHA	TCP / Received RST	خیر
118	TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	TCP / Received RST	خیر

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
119	TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA	TCP / Received RST	خیر

پشتیبانی از این پروتکل : خیر

Accepted Cipher Suites :

#	Name	Connection Status	Anonymous

Preferred Cipher Suites :

#	Name	Connection Status	Anonymous
1			خیر

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
1	TLS_RSA_WITH_SEED_CBC_SHA	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

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
19	TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5	TCP / Received RST	خیر
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

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
39	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA	TCP / Received RST	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	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

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
59	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	TLS / No ciphers available	خیر
60	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	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

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
79	TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA	TCP / Received RST	خیر
80	TLS_DH_RSA_WITH_AES_256_GCM_SHA384	TLS / No ciphers available	خیر
81	TLS_DH_RSA_WITH_AES_256_CBC_SHA256	TLS / No ciphers available	خیر
82	TLS_DH_RSA_WITH_AES_256_CBC_SHA	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

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
99	TLS_DHE_RSA_WITH_DES_CBC_SHA	TCP / Received RST	خیر
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

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
119	TLS_DHE_DSS_WITH_AES_128_CBC_SHA	TCP / Received RST	خیر
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_GCM_SHA384	HTTP 200 OK	خیر
2	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	HTTP 200 OK	خیر
3	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	HTTP 200 OK	خیر
4	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	HTTP 200 OK	خیر

Preferred Cipher Suites :

#	Name	Connection Status	Anonymous
1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	HTTP 200 OK	خیر

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
1	TLS_RSA_WITH_SEED_CBC_SHA	TLS / Alert: handshake failure	خیر
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
11	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	TLS / Alert: handshake failure	خیر
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

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
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_CBC_SHA384	TLS / Alert: handshake failure	خیر
30	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	TLS / Alert: handshake failure	خیر
31	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	TLS / Alert: handshake failure	خیر
32	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	TLS / Alert: handshake failure	خیر
33	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	TLS / Alert: handshake failure	خیر
34	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA	TLS / Alert: handshake failure	خیر

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
35	TLS_ECDHE_ECDSA_WITH_NULL_SHA	TLS / Alert: handshake failure	خیر
36	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	TLS / Alert: handshake failure	خیر
37	TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_CBC_SHA384	TLS / Alert: handshake failure	خیر
38	TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_CBC_SHA256	TLS / Alert: handshake failure	خیر
39	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	TLS / Alert: handshake failure	خیر
40	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	TLS / Alert: handshake failure	خیر
41	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	TLS / Alert: handshake failure	خیر
42	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	TLS / Alert: handshake failure	خیر
43	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	TLS / Alert: handshake failure	خیر
44	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	TLS / Alert: handshake failure	خیر
45	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	TLS / Alert: handshake failure	خیر
46	TLS_DH_anon_WITH_SEED_CBC_SHA	TLS / Alert: handshake failure	بلی
47	TLS_DH_anon_WITH_RC4_128_MD5	TLS / Alert: handshake failure	بلی
48	TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA256	TLS / No ciphers available	بلی
49	TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA	TLS / Alert: handshake failure	بلی
50	TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA256	TLS / No ciphers available	بلی
51	TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA	TLS / Alert: handshake failure	بلی
52	TLS_DH_anon_WITH_AES_256_GCM_SHA384	TLS / Alert: handshake failure	بلی
53	TLS_DH_anon_WITH_AES_256_CBC_SHA256	TLS / Alert: handshake failure	بلی
54	TLS_DH_anon_WITH_AES_256_CBC_SHA	TLS / Alert: handshake failure	بلی

Rejected Cipher Suites :

#	Name	Connection Status	Anonymous
55	TLS_DH_anon_WITH_AES_128_GCM_SHA256	TLS / Alert: handshake failure	بلی
56	TLS_DH_anon_WITH_AES_128_CBC_SHA256	TLS / Alert: handshake failure	بلی
57	TLS_DH_anon_WITH_AES_128_CBC_SHA	TLS / Alert: handshake failure	بلی
58	TLS_DH_anon_WITH_3DES_EDE_CBC_SHA	TLS / Alert: handshake failure	بلی
59	TLS_DHE_RSA_WITH_SEED_CBC_SHA	TLS / Alert: handshake failure	خیر
60	TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256	TLS / Alert: handshake failure	خیر
61	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256	TLS / Alert: handshake failure	خیر
62	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA	TLS / Alert: handshake failure	خیر
63	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256	TLS / Alert: handshake failure	خیر
64	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA	TLS / Alert: handshake failure	خیر
65	TLS_DHE_RSA_WITH_AES_256_CCM	TLS / Alert: handshake failure	خیر
66	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	TLS / Alert: handshake failure	خیر
67	TLS_DHE_RSA_WITH_AES_256_CBC_SHA	TLS / Alert: handshake failure	خیر
68	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	TLS / Alert: handshake failure	خیر
69	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	TLS / Alert: handshake failure	خیر
70	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	TLS / Alert: handshake failure	خیر
71	TLS_DHE_DSS_WITH_SEED_CBC_SHA	TLS / Alert: handshake failure	خیر
72	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA256	TLS / Alert: handshake failure	خیر
73	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA	TLS / Alert: handshake failure	خیر
74	TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA256	TLS / Alert: handshake failure	خیر

Rejected Cipher Suites :

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

Rejected Cipher Suites :

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

: Handshake Simulation

#	Name	Type	Cipher
1	(Android(2.3.7		
2	(Android(4.0.4		
3	(Android(4.1.1		
4	(Android(4.2.2		
5	(Android(4.3		
6	(Android(4.4.2	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
7	(Android(5.0.0	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
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		
11	(BingBot(Dec 2013		
12	(BingPreview(Dec 2013		
13	(BingPreview(Jun 2014		
14	(BingPreview(Jan 2015	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
15	Chrome(27) - Win 7		
16	Chrome(28) - Win 7		
17	Chrome(29) - Win 7		
18	Chrome(30) - Win 7		
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		
39	Firefox(10.0.12 ESR) - Win 7		

: Handshake Simulation

#	Name	Type	Cipher
40	Firefox(17.0.7 ESR) - Win 7		
41	Firefox(24.2.0 ESR) - Win 7		
42	Firefox(31.3.0 ESR) - Win 7	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
43	Firefox(21) - Fedora 19		
44	Firefox(22) - Win 7		
45	Firefox(24) - Win 7		
46	Firefox(26) - Win 8		
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		
66	(Googlebot(Jun 2014		
67	(Googlebot(Feb 2015	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
68	IE(6) - XP		
69	IE(6) - XP		
70	IE(7) - Vista		
71	IE(8) - XP		
72	IE(8) - XP		
73	IE(8) - Win 7		
74	IE(9) - Win 7		
75	IE(8-10) - Win 7		
76	IE(8-10) - Win 7		
77	IE(11) - Win 7		
78	IE(11) - Win 7	tlsv1_2	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
79	IE(11) - Win 7	tlsv1_2	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

: Handshake Simulation

#	Name	Type	Cipher
80	IE(11) - Win 7	tlsv1_2	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
81	IE(11) - Win 7	tlsv1_2	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
82	IE(11) - Win 10 Preview	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
83	IE(11) - Win 8.1		
84	IE(11) - Win 8.1	tlsv1_2	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
85	IE(11) - Win 8.1	tlsv1_2	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
86	IE(11) - Win 8.1	tlsv1_2	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
87	IE(11) - Win 8.1	tlsv1_2	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
88	IE(10) - Win Phone 8.0		
89	IE(11) - Win Phone 8.1		
90	IE(11) - Win Phone 8.1 Update	tlsv1_2	TLS_DHE_RSA_WITH_AES_256_GCM_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		
98	(Java(7u25		
99	(Java(8b132	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

: Handshake Simulation

#	Name	Type	Cipher
100	(Java(8u31	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
101	(OpenSSL(0.9.8y		
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		
106	Opera(15) - Win 7		
107	Opera(16) - Win 7		
108	Opera(17) - Win 7		
109	Safari(5) - iOS 5.1.1		
110	Safari(5.1.9) - OS X 10.6.8		
111	Safari(6) - iOS 6.0.1		
112	Safari(6.0.4) - OS X 10.8.4		
113	Safari(7) - iOS 7.1		
114	Safari(8) - iOS 8.0 Beta		
115	Safari(7) - OS X 10.9		
116	Safari(8) - iOS 8.4		
117	Safari(8) - OS X 10.10		
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		
124	(Yahoo Slurp(Oct 2013		
125	(Yahoo Slurp(Jun 2014	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
126	(Yahoo Slurp(Jan 2015	tlsv1_2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
127	(YandexBot(3.0		
128	(YandexBot(May 2014		
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