

بررسی SSL دامنه sobhetehran021.ir

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

تاریخ تهیه گزارش: سه شنبه ۱۸ تیر ۱۳۹۸ در ساعت ۳:۵۳:۰۰
بازدید: 0

گزارش بررسی تنظیمات SSL دامنه sobhetehran021.ir

☆ امتیاز: ★★★★★

HSTS



آسیب پذیری



سازگاری مرورگرها



معتبر



ارتباط تنها در SSL



اطلاعات هدر دامنه

Server: nginx
Date: Mon, 08 Jul 2019 23:23:27 GMT
Content-Type: text/html; charset=iso-8859-1
Transfer-Encoding: chunked
Connection: keep-alive
Vary: Accept-Encoding
Content-Encoding: gzip



Shodan اطلاعات

Shodan Information :

SSL Certificate

- Issued By:
 - Common Name:Let's Encrypt Authority X3
 - Organization:Let's Encrypt
- Issued To:
 - Common Name:server19f.axspace.com

Supported SSL Versions

TLSv1.2

pmx2.srv19.axspace.com ESMTP Exim 4.92 #5 Fri, 14 Jun 2019 18:28:58 +0430 220-We do not authorize the use of this system to-220 transport unsolicited, 220 and/or bulk e-mail. 250-pmx2.srv19.axspace.com Hello 26.163.54.29 [26.163.54.29] 250-SIZE 67108864 250-...8BITMIME 250-PIPELINING 250-AU

147.135.146.194

pmx2.srv19.axspace.com

OVH SAS

Added on 2019-06-19 06:22:04 GMT

France

SSL Certificate

:Issued By
Common Name:Let's Encrypt Authority X3 -|
Organization:Let's Encrypt -|
:Issued To
Common Name:server19f.axspace.com -|

Supported SSL Versions

TLSv1.2

//.http

http://sobhetehran021.ir/ -> 200

//.https

https://sobhetehran021.ir/ -> 200

همیشه از HTTPS استفاده کنید

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

(HTTP Strict Transport Security (HSTS

اطلاعات بیشتر ?

ارائه نشده است HTTP Strict Transport Security (HSTS):

اطلاعات امضای دیجیتال صادر شده

اطلاعات امضای دیجیتال شماره # 1

server19f.axspace.com	عنوان امضای دیجیتال :
ftp.server19f.axspace.com , mail.server19f.axspace.com , pop.server19f.axspace.com , Alternative) , server19f.axspace.com , smtp.server19f.axspace.com , www.server19f.axspace.com	عنوان های جایگزین امضا (Alternative) :
(Names)	
شروع اعتبار از : چهارشنبه ۱۲ تیر ۱۳۹۸ در ساعت ۱۰:۵۷	
پایان اعتبار تا : سه شنبه ۰۹ مهر ۱۳۹۸ در ساعت ۱۰:۵۷ - اتمام در : 84 روز و 10 ساعت و 34 دقیقه و 13 ثانیه	
صادر کننده مجوز : Lets Encrypt Authority X3	
کشور صادر کننده مجوز : US - ایلات متحده (آمریکا)	
الگوریتم امضا : sha256 with RSA size: 4096 Bits	
Certificate Transparency : (yes (certificate extension	
OCSP stapling : LOW - not offered	
OCSP URL : http://ocsp.int-x3.letsencrypt.org	
CRL Distribution Points : --	
Trust	
Android iOS Java macOS Mozilla OPENJDK Windows	
بررسی اعتبار دامنه :	

بررسی اعتبار دامنه :

نام هاست دامنه : sobhetehran021.ir

انطباق دامنه با امضای دیجیتال : خیر

: Path Validation

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

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 : =MtpCjsTtWxndZ8/+M1FLCOd050HKy07m4FxWXphLVlg

=Pin : MtpCjsTtWxndZ8/+M1FLCOd050HKy07m4FxWXphLVlg

Finger print : 78eb736a34d6572009280aaa1c397d2e6a3ad010

عنوان : commonName=server19f.axspace.com

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

سریال مجوز : 3.547000059963E+41

شروع اعتبار از : 10:57:46 03-07-2019

پایان اعتبار تا : 10:57:46 01-10-2019

الگوریتم امضا : sha256

کلید عمومی : الگوریتم : RSA

کلید عمومی : نوع : 65537

کلید عمومی : اندازه : 4096

شماره 2 : =YLh1dUR9y6Kja30RrAn7JKnbQG/uEtLMkBgFF2Fuihg

=Pin : YLh1dUR9y6Kja30RrAn7JKnbQG/uEtLMkBgFF2Fuihg

Finger print : e6a3b45b062d509b3382282d196efe97d5956ccb

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

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

سریال مجوز : 1.3298795840391E+37

شروع اعتبار از : 16:40:46 17-03-2016

پایان اعتبار تا : 16:40:46 17-03-2021

الگوریتم امضا : sha256

کلید عمومی : الگوریتم : RSA

کلید عمومی : نوع : 65537

کلید عمومی : اندازه : 2048

شماره 3 : =Vjs8r4z+80wjNcr1YKepWQboSIRi63WsWXhIMN+eWys

=Pin : Vjs8r4z+80wjNcr1YKepWQboSIRi63WsWXhIMN+eWys

Finger print : dac9024f54d8f6df94935fb1732638ca6ad77c13

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

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

سریال مجوز : 9.129973557534E+37

شروع اعتبار از : 21:12:19 30-09-2000

پایان اعتبار تا : 14:01:15 30-09-2021

الگوریتم امضا : sha1

کلید عمومی : الگوریتم : RSA

کلید عمومی : نوع : 65537

کلید عمومی : اندازه : 2048

: OCSF Stapling

خیر | پشتیبانی از OCSF : ___

خیر | OCSF Response : ___

خیر | Trusted By Mozilla : ___

: CA Store

Type : DEFLATE - ندارد | Deflate Compression

(TLS Fallback Scsv) دارد | Downgrade Attacks Prevention

: Session Renegotiation

بلی | Secure Renegotiation : ___

خیر | Insecure Client-Initiated : ___

: Renegotiation

: Resumption Support

دارد | Resumption With TLS : ___

: Tickets

دارد | Resumption With Session : ___

: IDs

5 | تعداد کل تست های انجام شده : ___

5 | تست های موفقیت آمیز : ___

0 | تست های بدون پاسخ : ___

0 | تعداد خطا ها : ___

Next Protocol Negotiation extension (with h2, http/1.1 (advertised شده است

: ((NPN

http/1.1 Application-Layer Protocol Negotiation

: ((ALPN

Personal Financial Specialist (PFS) ارائه شده است

ECDHE-RSA-AES256-GCM-SHA384 ECDHE-RSA-AES256-SHA384 ECDHE-RSA-AES256-SHA DHE-RSA-AES256-GCM-SHA384 DHE-RSA-AES256-CCM8 DHE-RSA-AES256-CCM DHE-RSA-AES256-SHA256 DHE-RSA-AES256-SHA ECDHE-RSA-CAMELLIA256-SHA384 DHE-RSA-CAMELLIA256-SHA256 DHE-RSA-CAMELLIA256-SHA ECDHE-RSA-AES128-GCM-SHA256 ECDHE-RSA-AES128-SHA256 ECDHE-RSA-AES128-SHA DHE-RSA-AES128-GCM-SHA256 DHE-RSA-AES128-CCM8 DHE-RSA-AES128-CCM DHE-RSA-AES128-SHA256 DHE-RSA-AES128-SHA ECDHE-RSA-CAMELLIA128-SHA256 DHE-RSA-CAMELLIA128-SHA256 DHE-RSA-CAMELLIA128-SHA

: PFS Ciphers

prime256v1 secp384r1 secp521r1 X25519 : PFS ECDHE curves

: DH Groups

(Unknown DH group (2048 bits

: Protocol Negotiated

Default protocol TLS1.2

: Cipher Negotiated

(ECDHE-RSA-AES128-GCM-SHA256, 256 bit ECDH (P-256

renegotiation info/#65281 server name/#0 EC point formats/#11 session ticket/#35 next protocol/#13172 encrypt-then-mac/#22 extended master secret/#23 application layer protocol negotiation/#16

: TLS Extensions

(valid for 300 seconds only (< daily

: TLS Session Ticket

yes : SSL SessionID Support

پشتیبانی می کند : Session Resumption Ticket

پشتیبانی می کند : Session Resumption ID

random : TLS Timestamp

-- : DNS CAA Record

(yes (certificate extension : Cert Transparency

(/) OK 200 : HTTP Status

ارائه نشده است (HTTP Strict Transport Security (HSTS

nginx : Banner Server

No support for HTTP Public Key Pinning : (HTTP Public Key Pinning (HPKP

/ at 0 : Cookie Count

no heartbeat extension , آسیب پذیر نیست : Heartbleed

آسیب پذیر نیست : (Certified Coding Specialist (CCS

آسیب پذیر نیست : Ticketbleed

CVE-2016-9244 : CVE _

CWE-200 : CVE _

آسیب پذیر نیست : ROBOT

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 : CVE _

CWE-203 : CVE _

آسیب پذیر نیست : Secure Renego

CVE-2009-3555 : CVE _

CWE-310 : CVE _

آسیب پذیر نیست : Secure Client Renego

CVE-2009-3555 : CVE _

CWE-310 : CVE _

آسیب پذیر نیست : Compression Ratio Info-leak Made

CVE-2012-4929 : (Easy(CRIME

CWE-310 : CVE _

ممکن است آسیب پذیر باشد, only supplied / tested uses gzip HTTP compression - : BREACH

CVE-2013-3587 : CVE _

CWE-310 : CVE _

پشتیبانی می کند : Fallback SCSV

آسیب پذیر نیست : POODLE SSL

CWE-310 : CVE _

اطلاعات بیشتر ?

اطلاعات بیشتر ?

— پشتیبانی از این پروتکل : خیر

: Accepted Cipher Suites

Anonymous	Connection Status	Name	#
-----------	-------------------	------	---

: Preferred Cipher Suites

Anonymous	Connection Status	Name	#
-----------	-------------------	------	---

: Rejected Cipher Suites

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

— پشتیبانی از این پروتکل : خیر

: Accepted Cipher Suites

Anonymous	Connection Status	Name	#
-----------	-------------------	------	---

: Preferred Cipher Suites

Anonymous	Connection Status	Name	#
-----------	-------------------	------	---

: Rejected Cipher Suites

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

: Rejected Cipher Suites

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

: Rejected Cipher Suites

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

: Rejected Cipher Suites

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

: Rejected Cipher Suites

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

: Rejected Cipher Suites

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

: Rejected Cipher Suites

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

— پشتیبانی از این پروتکل : خیر

: Accepted Cipher Suites

Anonymous	Connection Status	Name	#
-----------	-------------------	------	---

: Preferred Cipher Suites

Anonymous	Connection Status	Name	#
خیر			1

: Rejected Cipher Suites

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

: Rejected Cipher Suites

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

: Rejected Cipher Suites

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

: Rejected Cipher Suites

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

: Rejected Cipher Suites

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

: Rejected Cipher Suites

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

: Rejected Cipher Suites

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

: Accepted Cipher Suites

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

: Preferred Cipher Suites

Anonymous	Connection Status	Name	#
خیر	HTTP 200 OK	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	1

: Rejected Cipher Suites

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

: Rejected Cipher Suites

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

: Rejected Cipher Suites

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

: Rejected Cipher Suites

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

: Rejected Cipher Suites

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

: Rejected Cipher Suites

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

: Rejected Cipher Suites

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

: Accepted Cipher Suites

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

: Accepted Cipher Suites

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

: Preferred Cipher Suites

Anonymous	Connection Status	Name	#
خیر	HTTP 200 OK	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	1

: Rejected Cipher Suites

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

: Rejected Cipher Suites

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

: Rejected Cipher Suites

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

: Rejected Cipher Suites

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

: Rejected Cipher Suites

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

: Handshake Simulation

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

: Handshake Simulation

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

: Handshake Simulation

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

: Handshake Simulation

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

: Handshake Simulation

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

: Handshake Simulation

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

: Handshake Simulation

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

