

# بررسی SSL دامنه cert.ir

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

گزارش بررسی تنظیمات SSL دامنه cert.ir

تاریخ تهیه گزارش : سه شنبه ۱۹ مرداد ۱۴۰۰ در ساعت ۱۳:۳۵

بازدید: 0

امتیاز: ★★★★★

HSTS



آسیب پذیری



سازگاری مرورگرها



معتبر



ارتباط تنها در SSL



اطلاعات هدر دامنه

Date: Tue, 10 Aug 2021 09:05:03 GMT  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
Connection: keep-alive  
Keep-Alive: timeout=65  
Set-Cookie: 1d4311f8e56c786c51a2c4f788faf7be=030t61mepm7abhe8m8vq81q9ho; path=/; secure; HttpOnly, base\_language\_id=3; expires=Thu, 09-Sep-2021 09:05:02 GMT; Max-Age=2592000; path=/, iisjalali=1  
Expires: Tue, 10 Aug 2021 09:05:03 GMT  
Cache-Control: max-age=0  
Pragma: no-cache  
Vary: Accept-Encoding  
Content-Encoding: gzip  
Strict-Transport-Security: max-age=63072000  
Server: ArvanCloud  
Content-Security-Policy: upgrade-insecure-requests  
X-XSS-Protection: 1; mode=block  
AR-PoweredBy: Arvan Cloud (arvancloud.com)  
ar-SID: 2080  
AR-ATIME: 0.630  
AR-CACHE: BYPASS  
AR-Request-ID: c7df86bd5c3b492e5083cdba06eac57c

//:http

http://cert.ir/ -&gt; 301 -&gt; https://cert.ir/ -&gt; 200

//:https

https://cert.ir/ -&gt; 200

همیشه از HTTPS استفاده کنید

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

(HTTP Strict Transport Security (HSTS)

اطلاعات بیشتر ?

days (=63072000 seconds) > 15465600 seconds 730 HTTP Strict Transport Security  
 : (TIME (HSTS  
 only for this domain HTTP Strict Transport Security  
 : (SubDomains (HSTS  
 domain is NOT marked for preloading HTTP Strict Transport Security  
 : (Preload (HSTS

اطلاعات امضای دیجیتال صادر شده

## اطلاعات امضای دیجیتال شماره # 1

cert.ir. : عنوان امضای دیجیتال  
 نام کشور : IR - جمهوری اسلامی ایران  
 عنوان های جایگزین امضا (Alternative) cert.ir , cert.ir. :  
 (Names  
 شروع اعتبار از : پنجشنبه ۳۰ آبان ۱۳۹۸ در ساعت ۲۱:۴۷  
 پایان اعتبار تا : شنبه ۲۹ آبان ۱۴۰۰ در ساعت ۲۱:۴۷ - اتمام در : 102 روز و 12 ساعت و 42 دقیقه و 24 ثانیه  
 صادر کننده مجوز : Certum Domain Validation CA SHA2  
 کشور صادر کننده مجوز : PL - لهستان  
 الگوریتم امضا : sha256 with RSA size: 2048 Bits  
 Certificate Transparency : (yes (certificate extension  
 OCSP stapling : LOW - not offered  
 OCSP URL : http://dvcasha2.ocsp-certum.com  
 CRL Distribution Points : http://crl.certum.pl/dvcasha2.crl  
 Trust  
 Android iOS Java macOS Mozilla OPENJDK Windows  
 بررسی اعتبار دامنه :

بررسی اعتبار دامنه :

نام هاست دامنه : cert.ir

انطباق دامنه با امضای دیجیتال : بلی

: 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 : =HjdYBWWVF5tsIEOfZ73yuWJo6EeCpdNv71K80zE7mvBc

=Pin : HjdYBWWVF5tsIEOfZ73yuWJo6EeCpdNv71K80zE7mvBc

Finger print : 318a601557bcfb6720dfa4e99b3dc194e0a9d7b8

عنوان : countryName=IR, commonName=.cert.ir, emailAddress=certcert.ir

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

سریال مجوز : 9.7352232312919E+36

شروع اعتبار از : 21:47:31 21-11-2019

پایان اعتبار تا : 21:47:31 20-11-2021

الگوریتم امضا : sha256

کلید عمومی : الگوریتم : RSA

کلید عمومی : نوع : 65537

کلید عمومی : اندازه : 2048

شماره 2 : =S4AbJNGvyS57nzJwv8sPMUML8VHSqH1vbiBftdPcErl

=Pin : S4AbJNGvyS57nzJwv8sPMUML8VHSqH1vbiBftdPcErl

Finger print : ff9ceb13c83f15b800e6eff987b2c72e01b4b320

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

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

سریال مجوز : 5.1662424180299E+37

شروع اعتبار از : 12:00:00 11-09-2014

پایان اعتبار تا : 10:46:39 09-06-2027

الگوریتم امضا : sha256

کلید عمومی : الگوریتم : RSA

کلید عمومی : نوع : 65537

کلید عمومی : اندازه : 2048

شماره 3 : qiYwp7YXsE0KKUureoyqpQFubb5gSDeoOoVxn6tmfrU =

=Pin : qiYwp7YXsE0KKUureoyqpQFubb5gSDeoOoVxn6tmfrU

Finger print : 07e032e020b72c3f192f0628a2593a19a70f069e

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

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

: 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 : \_\_\_

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

http/1.1 Application-Layer Protocol Negotiation  
: ((ALPN

ارائه شده است (™ **Personal Financial Specialist (PFS**

TLS\_AES\_256\_GCM\_SHA384 TLS\_CHACHA20\_POLY1305\_SHA256 ECDHE-RSA-AES256-GCM\_SHA384 ECDHE-RSA-  
AES256-SHA384 ECDHE-RSA-AES256-SHA ECDHE-RSA-CHACHA20-POLY1305 TLS\_AES\_128\_GCM\_SHA256 ECDHE-  
RSA-AES128-GCM\_SHA256 ECDHE-RSA-AES128-SHA256 ECDHE-RSA-AES128-SHA  
: PFS Ciphers

prime256v1 secp384r1 secp521r1 : PFS ECDHE curves

Default protocol TLS1.3 : Protocol Negotiated

(TLS\_AES\_256\_GCM\_SHA384, 256 bit ECDH (P-256 : Cipher Negotiated

renegotiation info/#65281 server name/#0 EC point formats/#11 session ticket/#35 next protocol/#13172  
supported versions/#43 key share/#51 max fragment length/#1 application layer protocol negotiation/#16 encrypt-  
then-mac/#22 extended master secret/#23 : TLS Extensions

(valid for 10800 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

days (=63072000 seconds) > 15465600 seconds 730 HTTP Strict Transport Security TIME

: ((HSTS

only for this domain HTTP Strict Transport Security

: (SubDomains (HSTS

domain is NOT marked for preloading HTTP Strict Transport Security

: (Preload (HSTS

ArvanCloud : Banner Server

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

/ at 3 : Cookie Count

at / marked as secure 1/3 : Cookie Secure

at / marked as HttpOnly 1/3 : Cookie HTTP Only

no heartbeat extension , آسیب پذیر نیست , : Heartbleed

آسیب پذیر نیست : (Certified Coding Specialist (CCS

آسیب پذیر نیست : Ticketbleed

CVE-2016-9244 : CVE \_|

CWE-200 : CWE \_|

no RSA key transport cipher , 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 : CWE \_|

آسیب پذیر نیست : Secure Renego

CVE-2009-3555 : CVE \_|

CWE-310 : CWE \_|

آسیب پذیر نیست : Secure Client Renego

CVE-2009-3555 : CVE \_|

CWE-310 : CWE \_|

آسیب پذیر نیست : Compression Ratio Info-leak Made

: (Easy(CRIME

CVE-2012-4929 : CVE \_|

CWE-310 : CWE \_|

[اطلاعات بیشتر ?](#)

|  |  |   |
|--|--|---|
| <p><a href="#">اطلاعات بیشتر ?</a></p> | <p>ممکن است آسیب پذیر باشد, uses gzip HTTP compression - only supplied / tested<br/>                 CVE-2013-3587<br/>                 CWE-310<br/>                 پشتیبانی می کند<br/>                 آسیب پذیر نیست<br/>                 CVE-2016-2183 CVE-2016-6329<br/>                 آسیب پذیر نیست<br/>                 CVE-327</p> | <p>: BREACH<br/>                 : CVE _ <br/>                 : CWE _ <br/>                 : Fallback SCSV<br/>                 : POODLE SSL<br/>                 : CVE _ <br/>                 : SWEET32<br/>                 : CVE _ <br/>                 : CVE _ </p> |
| <p><a href="#">اطلاعات بیشتر ?</a></p> | <p>آسیب پذیر نیست<br/>                 FREAK (Factoring RSA Export<br/>                 : (Keys</p>  | <p>: (Keys</p>  |
| <p><a href="#">اطلاعات بیشتر ?</a></p> | <p>Make sure you don t use this certificate elsewhere with SSLv2 enabled services, see<br/>                 https://censys.io/ipv4?<br/>                 q=E9C2B114C3EF2439BCD9DCA94C5C62CF929E56EF867772BCB842F1E81876A98C<br/>                 CVE-2016-0800 CVE-2016-0703<br/>                 CVE-310</p>                                  | <p>DROWN (Decrypting RSA<br/>                 with Obsolete and<br/>                 : (Weakened eNcryption<br/>                 : CVE _ <br/>                 : CVE _ </p>   |
| <p><a href="#">اطلاعات بیشتر ?</a></p> | <p>no DH key with &lt; = TLS 1.2<br/>                 CVE-2015-4000<br/>                 CVE-310</p>   | <p>: LOGJAM Common Primes<br/>                 : CVE _ <br/>                 : CVE _ </p>   |
| <p><a href="#">اطلاعات بیشتر ?</a></p> | <p>,no DH EXPORT ciphers , آسیب پذیر نیست<br/>                 CVE-2015-4000<br/>                 CVE-310</p>  | <p>: LOGJAM<br/>                 : CVE _ <br/>                 : CVE _ </p>   |
| <p><a href="#">اطلاعات بیشتر ?</a></p> | <p>ECDHE-RSA-AES256-SHA ECDHE-RSA-AES128-SHA<br/>                 CVE-2011-3389<br/>                 CVE-20</p>  | <p>: BEAST CBC TLS1<br/>                 : CVE _ <br/>                 : CVE _ </p>   |
| <p><a href="#">اطلاعات بیشتر ?</a></p> | <p>but also supports higher protocols TLSv1.1 TLSv1.2 (likely -- آسیب پذیر --<br/>                 (mitigated)</p>   | <p>: BEAST<br/>                 : CVE _ <br/>                 : CVE _ </p>  |
| <p><a href="#">اطلاعات بیشتر ?</a></p> | <p>همچنین از پروتکل های بالاتر TLSv1.1 TLSv1.2 پشتیبانی می کند<br/>                 CVE-2011-3389<br/>                 CVE-20</p>  | <p>: CVE _ <br/>                 : CVE _ </p>   |
| <p><a href="#">اطلاعات بیشتر ?</a></p> | <p>ممکن است آسیب پذیر باشد, uses TLS CBC ciphers<br/>                 CVE-2013-0169<br/>                 CVE-310</p>   | <p>: LUCKY 13<br/>                 : CVE _ <br/>                 : CVE _ </p>   |
| <p><a href="#">اطلاعات بیشتر ?</a></p> | <p>آسیب پذیر نیست<br/>                 CVE-310</p>   | <p>: RC4<br/>                 : CVE _ </p>  |



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 |



## : 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_ECDHE_RSA_WITH_AES_128_CBC_SHA | 2 |

## : Preferred Cipher Suites

| Anonymous | Connection Status | Name                               | # |
|-----------|-------------------|------------------------------------|---|
| خیر       | HTTP 200 OK       | TLS_ECDHE_RSA_WITH_AES_256_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  |
| 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 |

## : Rejected Cipher Suites

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

## : Rejected Cipher Suites

| Anonymous | Connection Status              | Name                                    | #  |
|-----------|--------------------------------|---|----|
| 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 |
| 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 / No ciphers available     | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256   | 48 |
| خیر       | TLS / No ciphers available     | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256   | 49 |
| خیر       | TLS / Alert: handshake failure | TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA     | 50 |
| خیر       | TLS / Alert: handshake failure | TLS_ECDHE_ECDSA_WITH_RC4_128_SHA        | 51 |
| خیر       | TLS / Alert: handshake failure | TLS_ECDHE_ECDSA_WITH_NULL_SHA           | 52 |
| خیر       | TLS / No ciphers available     | TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 | 53 |
| خیر       | TLS / No ciphers available     | TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 | 54 |
| خیر       | TLS / Alert: handshake failure | TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA    | 55 |
| خیر       | TLS / No ciphers available     | TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 | 56 |

## : Rejected Cipher Suites

| Anonymous | Connection Status              | Name                                    | #  |
|-----------|--------------------------------|---|----|
| خیر       | TLS / No ciphers available     | TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 | 57 |
| خیر       | TLS / Alert: handshake failure | TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA    | 58 |
| خیر       | TLS / Alert: handshake failure | TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA   | 59 |
| بلی       | TLS / Alert: handshake failure | TLS_DH_anon_WITH_SEED_CBC_SHA           | 60 |
| بلی       | TLS / Alert: handshake failure | TLS_DH_anon_WITH_RC4_128_MD5            | 61 |
| بلی       | TLS / Alert: handshake failure | TLS_DH_anon_WITH_DES_CBC_SHA            | 62 |
| بلی       | TLS / Alert: handshake failure | TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA   | 63 |
| بلی       | TLS / Alert: handshake failure | TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA   | 64 |
| بلی       | TLS / No ciphers available     | TLS_DH_anon_WITH_AES_256_GCM_SHA384     | 65 |
| بلی       | TLS / No ciphers available     | TLS_DH_anon_WITH_AES_256_CBC_SHA256     | 66 |
| بلی       | TLS / Alert: handshake failure | TLS_DH_anon_WITH_AES_256_CBC_SHA        | 67 |
| بلی       | TLS / No ciphers available     | TLS_DH_anon_WITH_AES_128_GCM_SHA256     | 68 |
| بلی       | TLS / No ciphers available     | TLS_DH_anon_WITH_AES_128_CBC_SHA256     | 69 |
| بلی       | TLS / Alert: handshake failure | TLS_DH_anon_WITH_AES_128_CBC_SHA        | 70 |
| بلی       | TLS / Alert: handshake failure | TLS_DH_anon_WITH_3DES_EDE_CBC_SHA       | 71 |
| بلی       | TLS / Alert: handshake failure | TLS_DH_anon_EXPORT_WITH_RC4_40_MD5      | 72 |
| بلی       | TLS / Alert: handshake failure | TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA   | 73 |
| خیر       | TLS / Alert: handshake failure | TLS_DH_RSA_WITH_SEED_CBC_SHA            | 74 |
| خیر       | TLS / Alert: handshake failure | TLS_DH_RSA_WITH_DES_CBC_SHA             | 75 |
| خیر       | TLS / Alert: handshake failure | TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA    | 76 |

## : Rejected Cipher Suites

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

## : Rejected Cipher Suites

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

## : Rejected Cipher Suites

| Anonymous | Connection Status              | Name                                  | #   |
|-----------|--------------------------------|---------------------------------------|-----|
| خیر       | TLS / Alert: handshake failure | TLS_DHE_DSS_WITH_AES_128_CBC_SHA      | 117 |
| خیر       | TLS / Alert: handshake failure | TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA     | 118 |
| خیر       | TLS / Alert: handshake failure | TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA | 119 |

## : 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_ECDHE_RSA_WITH_AES_128_CBC_SHA | 2 |

## : Preferred Cipher Suites

| Anonymous | Connection Status | Name                               | # |
|-----------|-------------------|------------------------------------|---|
| خیر       | HTTP 200 OK       | TLS_ECDHE_RSA_WITH_AES_256_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  |
| 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 |



## : Rejected Cipher Suites

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

## : Rejected Cipher Suites

| Anonymous | Connection Status              | Name                                    | #  |
|-----------|--------------------------------|---|----|
| 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 |
| 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 / No ciphers available     | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256   | 48 |
| خیر       | TLS / No ciphers available     | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256   | 49 |
| خیر       | TLS / Alert: handshake failure | TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA     | 50 |
| خیر       | TLS / Alert: handshake failure | TLS_ECDHE_ECDSA_WITH_RC4_128_SHA        | 51 |
| خیر       | TLS / Alert: handshake failure | TLS_ECDHE_ECDSA_WITH_NULL_SHA           | 52 |
| خیر       | TLS / No ciphers available     | TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 | 53 |
| خیر       | TLS / No ciphers available     | TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 | 54 |
| خیر       | TLS / Alert: handshake failure | TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA    | 55 |
| خیر       | TLS / No ciphers available     | TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 | 56 |

## : Rejected Cipher Suites

| Anonymous | Connection Status              | Name                                    | #  |
|-----------|--------------------------------|---|----|
| خیر       | TLS / No ciphers available     | TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 | 57 |
| خیر       | TLS / Alert: handshake failure | TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA    | 58 |
| خیر       | TLS / Alert: handshake failure | TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA   | 59 |
| بلی       | TLS / Alert: handshake failure | TLS_DH_anon_WITH_SEED_CBC_SHA           | 60 |
| بلی       | TLS / Alert: handshake failure | TLS_DH_anon_WITH_RC4_128_MD5            | 61 |
| بلی       | TLS / Alert: handshake failure | TLS_DH_anon_WITH_DES_CBC_SHA            | 62 |
| بلی       | TLS / Alert: handshake failure | TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA   | 63 |
| بلی       | TLS / Alert: handshake failure | TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA   | 64 |
| بلی       | TLS / No ciphers available     | TLS_DH_anon_WITH_AES_256_GCM_SHA384     | 65 |
| بلی       | TLS / No ciphers available     | TLS_DH_anon_WITH_AES_256_CBC_SHA256     | 66 |
| بلی       | TLS / Alert: handshake failure | TLS_DH_anon_WITH_AES_256_CBC_SHA        | 67 |
| بلی       | TLS / No ciphers available     | TLS_DH_anon_WITH_AES_128_GCM_SHA256     | 68 |
| بلی       | TLS / No ciphers available     | TLS_DH_anon_WITH_AES_128_CBC_SHA256     | 69 |
| بلی       | TLS / Alert: handshake failure | TLS_DH_anon_WITH_AES_128_CBC_SHA        | 70 |
| بلی       | TLS / Alert: handshake failure | TLS_DH_anon_WITH_3DES_EDE_CBC_SHA       | 71 |
| بلی       | TLS / Alert: handshake failure | TLS_DH_anon_EXPORT_WITH_RC4_40_MD5      | 72 |
| بلی       | TLS / Alert: handshake failure | TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA   | 73 |
| خیر       | TLS / Alert: handshake failure | TLS_DH_RSA_WITH_SEED_CBC_SHA            | 74 |
| خیر       | TLS / Alert: handshake failure | TLS_DH_RSA_WITH_DES_CBC_SHA             | 75 |
| خیر       | TLS / Alert: handshake failure | TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA    | 76 |

## : Rejected Cipher Suites

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

## : Rejected Cipher Suites

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

## : Rejected Cipher Suites

| Anonymous | Connection Status              | Name                                  | #   |
|-----------|--------------------------------|---------------------------------------|-----|
| خیر       | TLS / Alert: handshake failure | TLS_DHE_DSS_WITH_AES_128_CBC_SHA      | 117 |
| خیر       | TLS / Alert: handshake failure | TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA     | 118 |
| خیر       | TLS / Alert: handshake failure | TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA | 119 |

## : Accepted Cipher Suites

| Anonymous | Connection Status | Name  | # |
|-----------|-------------------|---|---|
| خیر       | HTTP 200 OK       | TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 | 1 |
| خیر       | HTTP 200 OK       | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384       | 2 |
| خیر       | HTTP 200 OK       | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA          | 3 |
| خیر       | HTTP 200 OK       | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384       | 4 |
| خیر       | HTTP 200 OK       | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA          | 5 |
| خیر       | HTTP 200 OK       | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256       | 6 |
| خیر       | HTTP 200 OK       | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256       | 7 |

## : Preferred Cipher Suites

| Anonymous | Connection Status | Name                                  | # |
|-----------|-------------------|---------------------------------------|---|
| خیر       | HTTP 200 OK       | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | 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 / 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_CAMELLIA_256_CBC_SHA256 | 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_SHA256 | 10 |

## : Rejected Cipher Suites

| Anonymous | Connection Status              | Name  | #  |
|-----------|--------------------------------|---|----|
| خیر       | TLS / Alert: handshake failure | TLS_RSA_WITH_AES_256_GCM_SHA384               | 12 |
| خیر       | TLS / Alert: handshake failure | TLS_RSA_WITH_AES_256_CBC_SHA256               | 13 |
| خیر       | TLS / Alert: handshake failure | TLS_RSA_WITH_AES_256_CBC_SHA                  | 14 |
| خیر       | TLS / Alert: handshake failure | TLS_RSA_WITH_AES_128_GCM_SHA256               | 15 |
| خیر       | TLS / Alert: handshake failure | TLS_RSA_WITH_AES_128_CBC_SHA256               | 16 |
| خیر       | TLS / Alert: handshake failure | TLS_RSA_WITH_AES_128_CBC_SHA                  | 17 |
| خیر       | TLS / Alert: handshake failure | TLS_RSA_WITH_3DES_EDE_CBC_SHA                 | 18 |
| بلی       | TLS / Alert: handshake failure | TLS_ECDH_anon_WITH_RC4_128_SHA                | 19 |
| بلی       | TLS / Alert: handshake failure | TLS_ECDH_anon_WITH_NULL_SHA                   | 20 |
| بلی       | TLS / Alert: handshake failure | TLS_ECDH_anon_WITH_AES_256_CBC_SHA            | 21 |
| بلی       | TLS / Alert: handshake failure | TLS_ECDH_anon_WITH_AES_128_CBC_SHA            | 22 |
| بلی       | TLS / Alert: handshake failure | TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA           | 23 |
| خیر       | TLS / Alert: handshake failure | TLS_ECDHE_RSA_WITH_RC4_128_SHA                | 24 |
| خیر       | TLS / Alert: handshake failure | TLS_ECDHE_RSA_WITH_NULL_SHA                   | 25 |
| خیر       | TLS / Alert: handshake failure | TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384    | 26 |
| خیر       | TLS / Alert: handshake failure | TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256    | 27 |
| خیر       | TLS / Alert: handshake failure | TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA           | 28 |
| خیر       | TLS / Alert: handshake failure | TLS_ECDHE_ECDSA_WITH_RC4_128_SHA              | 29 |
| خیر       | TLS / Alert: handshake failure | TLS_ECDHE_ECDSA_WITH_NULL_SHA                 | 30 |
| خیر       | TLS / Alert: handshake failure | TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 | 31 |



## : Rejected Cipher Suites

| Anonymous | Connection Status              | Name   | #  |
|-----------|--------------------------------|--|----|
| خیر       | TLS / Alert: handshake failure | TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_CBC_SHA384 | 32 |
| خیر       | TLS / Alert: handshake failure | TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_CBC_SHA256 | 33 |
| خیر       | TLS / Alert: handshake failure | TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384      | 34 |
| خیر       | TLS / Alert: handshake failure | TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384      | 35 |
| خیر       | TLS / Alert: handshake failure | TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA         | 36 |
| خیر       | TLS / Alert: handshake failure | TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256      | 37 |
| خیر       | TLS / Alert: handshake failure | TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256      | 38 |
| خیر       | TLS / Alert: handshake failure | TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA         | 39 |
| خیر       | TLS / Alert: handshake failure | TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA        | 40 |
| بلی       | TLS / Alert: handshake failure | TLS_DH_anon_WITH_SEED_CBC_SHA                | 41 |
| بلی       | TLS / Alert: handshake failure | TLS_DH_anon_WITH_RC4_128_MD5                 | 42 |
| بلی       | TLS / No ciphers available     | TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA256     | 43 |
| بلی       | TLS / Alert: handshake failure | TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA        | 44 |
| بلی       | TLS / No ciphers available     | TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA256     | 45 |
| بلی       | TLS / Alert: handshake failure | TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA        | 46 |
| بلی       | TLS / Alert: handshake failure | TLS_DH_anon_WITH_AES_256_GCM_SHA384          | 47 |
| بلی       | TLS / Alert: handshake failure | TLS_DH_anon_WITH_AES_256_CBC_SHA256          | 48 |
| بلی       | TLS / Alert: handshake failure | TLS_DH_anon_WITH_AES_256_CBC_SHA             | 49 |
| بلی       | TLS / Alert: handshake failure | TLS_DH_anon_WITH_AES_128_GCM_SHA256          | 50 |
| بلی       | TLS / Alert: handshake failure | TLS_DH_anon_WITH_AES_128_CBC_SHA256          | 51 |

## : Rejected Cipher Suites

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

## : Rejected Cipher Suites

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

## : Rejected Cipher Suites

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

: Handshake Simulation

| Cipher                                      | Type    | Name                  | #  |
|---|---------|-----------------------|----|
|   |         | (Android(2.3.7        | 1  |
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA          | tlsv1   | (Android(4.0.4        | 2  |
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA          | tlsv1   | (Android(4.1.1        | 3  |
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA          | tlsv1   | (Android(4.2.2        | 4  |
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA          | tlsv1   | (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   | (Android(5.0.0        | 7  |
| TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256       | tlsv1_2 | (Android(6.0          | 8  |
| TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 | tlsv1_2 | (Android(7.0          | 9  |
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA          | tlsv1   | (Baidu(Jan 2015       | 10 |
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA          | tlsv1   | (BingBot(Dec 2013     | 11 |
|   |         | (BingPreview(Dec 2013 | 12 |
|   |         | (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   | Chrome(27) - Win 7    | 15 |
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA          | tlsv1   | Chrome(28) - Win 7    | 16 |
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA          | tlsv1   | Chrome(29) - Win 7    | 17 |
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA          | tlsv1   | 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   | Firefox(21) - Win 7          | 38 |
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA    | tlsv1   | Firefox(10.0.12 ESR) - Win 7 | 39 |

: Handshake Simulation

| Cipher                                | Type    | Name                        | #  |
|---------------------------------------|---------|-----------------------------|----|
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA    | tlsv1   | Firefox(17.0.7 ESR) - Win 7 | 40 |
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA    | tlsv1   | 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 |
|                                       |         | Firefox(21) - Fedora 19     | 43 |
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA    | tlsv1   | Firefox(22) - Win 7         | 44 |
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA    | tlsv1   | Firefox(24) - Win 7         | 45 |
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA    | tlsv1   | 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   | (Googlebot(Oct 2013  | 65 |
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA    | tlsv1   | (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_ECDHE_RSA_WITH_AES_128_CBC_SHA    | tlsv1   | IE(7) - Vista        | 70 |
|                                       |         | IE(8) - XP           | 71 |
|                                       |         | IE(8) - XP           | 72 |
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA    | tlsv1   | IE(8) - Win 7        | 73 |
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA    | tlsv1   | IE(9) - Win 7        | 74 |
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA    | tlsv1   | IE(8-10) - Win 7     | 75 |
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA    | tlsv1   | IE(8-10) - Win 7     | 76 |
| TLS_ECDHE_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_ECDHE_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_ECDHE_RSA_WITH_AES_128_CBC_SHA    | tlsv1   | IE(10) - Win Phone 8.0        | 88 |
| TLS_ECDHE_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 |
|                                       |         | (Java(6u45                    | 97 |
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA    | tlsv1   | (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 |
|                                       |         | (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 |
|                                       |         | Opera(12.15) - Win 7        | 105 |
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA    | tlsv1   | Opera(15) - Win 7           | 106 |
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA    | tlsv1   | Opera(16) - Win 7           | 107 |
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA    | tlsv1   | 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   | 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   | 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   | Tor(17.0.9) - Win 7     | 123 |
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA    | tlsv1   | (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 |
|                                       |         | (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 |

