مفاهیم امنیت

سپهر مقیسه

دکتر شهریاری

۹۸۳۱۱۰۳

پاییز ۱۴۰۱

.۱

استفاده از روش two step authentication که ورود دومرحله است و در ملحه دوم کاربر حالا یا رمز عبور ارسالی به تلفن همراه یا ایمیل خود را وارد میکند و یا کد امنیتی ایجاد شده در برنامه تایید کد را وارد میکند.

روش دوم به تایید ip ورودی اشاره دارد که شرکت هایی مانند Spotify و گوگل از این کار استفاده میکنند به این صورت که اگر از ip کشوری متفاوت و مکانی متفاوت وارد شوید حتما با گزینه تایید هویت در ایمیل مواجه میشود

روش سوم: استفاده از کربروس - احراز هویت بر اساس رمز نگاری کلید مخفی(متقارن)

.۲

امنیت- اطمینان-شفافیت-مقیاس پذیری

.۳

در نسخه 5 می توان از هر الگوریتم متقارن استفاده کرد.

در نسخه 5 می توان از هر آدرس شبکه(مثلا OSI یا) IP استفاده کرد

در نسخه 5 محدودیت زمان اعتبار بلیت ها وجود ندارد

.۴

تا دو طرف ارتباط بتوانند ارتباط خود را مخفی و محرمانه نگه دارند.

هرزمان که کاربر جدیدی درخواستی به تایید کننده هویت میزند .سرور احراز هویت باید یک توکن جدید ایجاد کند و آن را میان هر دو گروه توزیع کند که به آن کلید جلسه گفته میشود.

به زبانی دیگر هنگامی که دو سیستم پایانی(میزبان، پایانهها، و غیره)تمایل به برقراری ارتباط

داشته باشند، آنها یک ارتباط منطقی برقرار میکنند(به عنوان مثال، مدار مجازی.)

.۵

در تبادل کلید اکثر سیستم ها به این صورت عمل میکنند که یک سیستم کلید را ایجاد کرده و به سیستم دیگر ارسال میکند و به اصطلاحی سیستم دوم در تولید کلید دستی نداشته است و یا حتی تبادل کلید عمومی نیز

تبادل کلید نامیده میشود. ولی در توافق کلید هردو بر سر کلید عمومی و خصوصی به توافق رسیده و کلیدی اشتراکی ایجاد میکنند.

۶.

.به طور مثال با ورود به یک سایت یک جلسه ایجاد کردیم و حال هر بار با هر وسیله ای به ان "متصل" بشویم به جلسه دست پیدا میکنیم یعنی به یک جلسه میتوان از کانکشن های متعدد استفاده کنیم. مثال سایت کورسز که یک بار جلسه ایجاد میکنیم و با هر بار بستن و باز کردن سایت بدون نیاز به ورود به آن وارد میشویم به صورت خودکار.

۷.

- Version-نسخه
- Serial number-سریال گواهی
- Signature algorithm- روش الگوریتم رمزی که صادر کننده توسط ان این گواهی را امضا میکند
- Issuer-صادر کننده
- Valid from-زمان شروع اعتبار گواهی
- Valid to- تا زمانی که گواهی اعتبار دارد
- Subject-اطلاعات کسی که این گواهی برایش صادر شده
- Public key-فیلد حاوی گواهی عمومی
- Extension-در این فیلد میتوان به تعداد دلخواه فیلد ایجاد کرد که هرکدام شناسه مشخص دارند

۸.

درtls میتواند در پیام handshake باشد اما جداسازی ان باعث اسانی فهمیدن رفتار پروتکل میشود

جواب طولانی تر به این گونه است که پروتوکل ssl از پیام هایی استفاده میشود که برای هر رکورد منحصر به فرد کدگزاری شده اند.اما چند پیام یک نوع مانند handshake ها میتواند در یک رکورد جای بگیرد .از انجایی که change cipher spec روش کدگزاری را تغییر میدهد، باید یک رکورد جدید سریعا ایجاد شود تا تغییرات لحاظ شوند برای همین وقتی یک پروتکل برای این کار ایجاد میکنیم بعد از نوع جدید رکورد استفاده کنیم، ssl چاره ای جز تغییر روش کدگزاری ندارد و از رکورد بعدی با آن روش کدگزاری را انجام میدهد.

۹.

الف)

Ssl تمامی ارتباطات را کدگزاری کرده. و این گونه فردی که ip spoofing را انجام میدهد نیاز به داشتن کلید کدگزاری کردن ssl دارد. حتی اگر این کلید را بدست اورد هر پکت اطلاعاتی در پروتکل

ssl یک هشتگ بسیار سخت برای برگشت دارد که وظیفه دارد تا پکت را بدون دست خوردن ارسال کند.اگر این هشتگ ها دست خورده شوند سریعا به دو طرف خبرداده شده و ارتباط نا امن را قطع میکنند

ب)

به این صورت که کلاینت و سرور بر سر یک کلید جلسه توافق کرده . این کلید فرستاده نمیشود بلکه اطلاعات با این کلید کدگزاری شده و ارسال میشوند و به دلیل روشی که پروتوکل ssl کلید را به اشتراک میگذارد نمیتوان رمز را پیدا کرد.

.۱۰

Session-identifier : یک دنباله بایتی که سرور انتخاب میکند تا جلسات فعال را پیدا کند.

Peer certificate: یک گواهی x.509 . این فیلد میتواند خالی باشد.

Compression method:روشی که داده را قبل از کدکردن فشرده میکند

Cipher spec: روش کدگزاری را مشخص میکند.یک کدگزاری روش هش نیز برای محاسبه مک استفاده میشود همچنین مقادیر کریپتوکرافیگی مانند اندازه هش را مشخص میکند.

Master secret: سکرت ۴۹ بایتی که میان کلاینت و سرور به اشتراک گذاشته میشود

Is resumable: پرچمی که برای مشخص سازی این که ایا میتوان از نشست برای ایجاد اتصال های جدید استفاده کرد و یا خیر

.۱۱

وقتی که میزبان A تمایل به برقرای ارتباط با میزبان B داشته باشد؛ یک بسته درخواست اتصال به KDC ارسال میکند .ارتباط بین A و KDC با استفاده از یک شاه کلید صورت میگیرد که تنها توسط A و KDC به اشتراک گذاشته شده است. اگر KDC درخواست اتصال را تأیید نماید، یک کلید جلسه منحصر بفرد را ایجاد کرده و کلید جلسه را با استفاده از کلید دائمی که با A به اشتراک گذاشته شده رمزگذاری نموده و کلید جلسه رمزگذاری شده را برای B ارسال می نماید. اکنون A و B میتوانند یک اتصال منطقی برای مبادله پیام و اطلاعات برقرار کنند . همه رمزگذاریها از کلید جلسه به طور موقت استفاده میکنند.

روش های توزیع کلید سری:

مبادله کلید با استفاده از رمز متقارن

مبادله کلید با استفاده از رمز کلید عمومی

مبادله پیام و کلید

پخش پیام و کلید

مبادله کلید دیفی-هلمن

پروتکل ایستگاه به ایستگاه

.۱۲

یک پروتکل است که توسط RFC 2408 برای ایجاد Security association (**SA**) و کلیدهای رمزنگاری در یک محیط اینترنتی تعریف شده است. در دو فاز فعالیت خود را انجام میدهد. در فاز اول که ISAKMP SA نامیده می شود ابتدا توافقات امنیتی بین دو نقطه صورت می پذیرد. در فاز اول علاوه بر توافقات امنیتی، Key Management برای بحث رمزنگاری (تبادل کلید) و Authentication نیز انجام می شود. در فاز دوم که IPSEC SA گفته می شود پروتکل Tunneling که می خواهیم استفاده نماییم از بین AH و ESP انتخاب می شود. در این فاز به صورت Optional می توانید Key Management را داشته باشید.

IKE یک پروتکل را با استفاده از بخشی از Oakley و بخشی از SKEME همراه با ISAKMP برای به دست آوردن مواد کلید دار معتبر برای استفاده با ISAKMP و سایر انجمن های امنیتی مانند AH و ESP برای IETF IPsec DOI توصیف می کند.

.۱۳

برای مدیریت خودکار کلید ها،توزیع و تنظیمات آن ها از این پروتکل استفاده میشود. و به اصطلاح پروتکلی است که دو سرور بر آن برای ایجاد ipsec توافق میکنند.

.۱۴

سایت اول:

خلاصه گزارش

B

88.8 / 100

دامنه، آدرس IP و شماره پورت
aut.ac.ir (185.211.88.131:443)
تاریخ و ساعت ارزیابی
Saturday 03 Dey 1401 14:06
مدت زمان ارزیابی
60 ثانیه

ارزیابی های انجام شده توسط "TLS1" نشان می دهد سرویس دچار آسیب پذیری است. در نتیجه رتبه سایت به B کاهش داده می شود

ارزیابی های انجام شده توسط "TLS1_1" نشان می دهد سرویس دچار آسیب پذیری است. در نتیجه رتبه سایت به B کاهش داده می شود

اطلاعات گواهی	
آیا گواهی همچنان معتبر است؟	بله
تاریخ صدور گواهی	2022-09-24 08:50
تاریخ انقضای گواهی	2023-09-24 08:50
وضعیت زنجیره اطمینان	خوب
صادر کننده گواهی	Certum Domain Validation CA SHA2 (Unizeto Technologies S.A. from PL)
آیا این گواهی برای دامنه‌ی aut.ac.ir معتبر است؟	بله

محتویات سرآیند HTTP	
کد وضعیت HTTP	('/') OK 200
پشتیبانی از Strict Transport Security	not offered
پشتیبانی از Public Key Pinning	No support for HTTP Public Key Pinning
وضعیت Server Banner	Apache
وضعیت Banner Application	No application banner found

چ

اطلاعات پروتکل	
SSLv2	سرویس از SSLv2 پشتیبانی نمی‌کند که یک مزیت است. زیرا این پروتکل ناامن به شمار می‌رود.
SSLv3	سرویس از SSLv3 پشتیبانی نمی‌کند که یک مزیت است. زیرا این پروتکل ناامن به شمار می رود.
TLS1	سرویس از TLSv1.0 پشتیبانی می‌کند. این پروتکل ضعیف است. پیشنهاد می‌شود برای افزایش امنیت، پشتیبانی از این پروتکل را غیرفعال کنید.
TLS1.1	سرویس شما از TLSv1.1 پشتیبانی می‌کند. پیشنهاد می‌شود برای افزایش امنیت، پشتیبانی از این پروتکل را غیرفعال کنید.
TLS1.2	سرویس شما از TLSv1.2 پشتیبانی می‌کند. در حال حاضر این پروتکل پایدار به شمار می‌رود، اما بهتر است پشتیبانی از TLSv1.3 را هم مد نظر داشته باشید.
TLS1.3	سرویس شما از پروتکل TLSv1.3 پشتیبانی نمی‌کند. پیشنهاد می شود امکان پشتیبانی از این پروتکل را فراهم کنید.

الگوریتم‌های رمزنگاری	
NULL	سرویس شما از رمزنگاری Null پشتیبانی نمی‌کند.
aNULL	سرویس شما از دنباله‌رمزهای aNULL پشتیبانی نمی‌کند.
EXPORT	سرویس شما از دنباله‌رمزهای EXPORT پشتیبانی نمی‌کند.
LOW	سرویس شما از دنباله‌رمزهای ضعیف (۶۴ بیتی، DES یا RC[2,4]) پشتیبانی نمی‌کند.
3DES_IDEA	سرویس شما از دنباله رمزهای 3DES پشتیبانی می‌کند که جزو دنباله‌رمزهای ناامن به شمار می‌روند.
AVERAGE	سرویس شما از دنباله‌رمزها و مدهای رمزنگاری متوسط مثل SEED یا CBC (۱۲۸ و ۲۵۶ بیتی) پشتیبانی می‌کند.
Strong	سرویس شما از روش‌های رمزنگاری قدرتمند مثل AEAD پشتیبانی می‌کند.

ارزیابی امنیت در مقابل حملات FREAK	اتصال شما در مقابل حملات FREAK مقاوم است.
ارزیابی امنیت در مقابل حملات DROWN	اتصال شما در مقابل حملات DROWN مقاوم است.
ارزیابی وجود اعداد اول مشترک در زوج کلیدهای عمومی/محرمانه.	اتصال شما در مقابل حملات LOGJAM_common_primes آسیب پذیر است.
ارزیابی امنیت در مقابل حملات LOGJAM	اتصال شما در مقابل حملات LOGJAM مقاوم است.
ارزیابی امنیت در مقابل آسیب پذیری CVE-2011-3389	اتصال شما در مقابل حملات BEAST_CBC_TLS1 آسیب پذیر است.
ارزیابی امنیت در مقابل حملات BEAST	اتصال شما در مقابل حملات BEAST آسیب پذیر است.
ارزیابی امنیت در مقابل حملات LUCK13	اتصال شما در مقابل حملات LUCKY13 آسیب پذیر است.
ارزیابی امنیت در مقابل حملات RC4	اتصال شما در مقابل حملات RC4 مقاوم است.

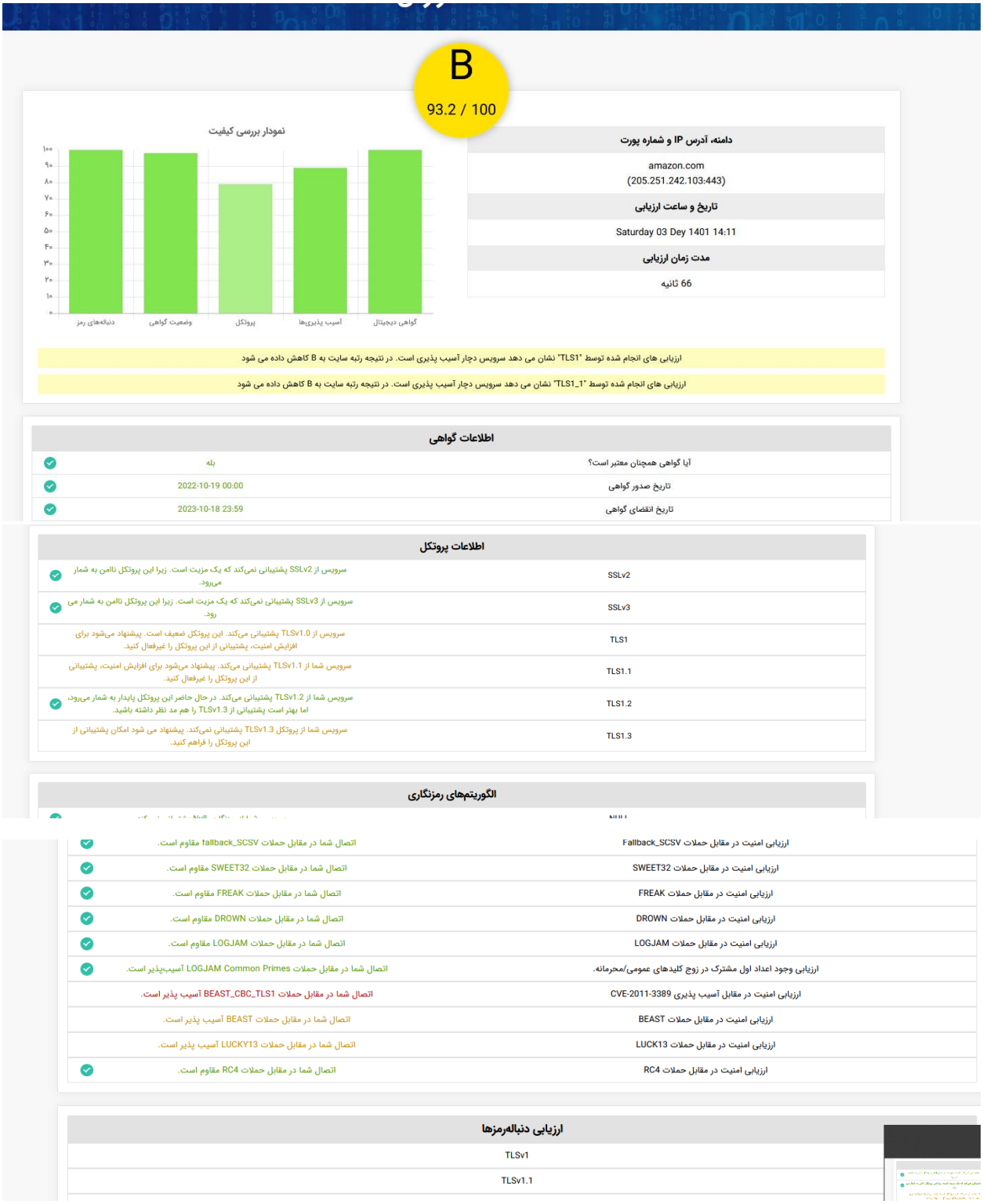
ارزیابی دنباله‌رمزها

TLSv1
TLSv1.1
TLSv1.2

شبیه سازی مرورگر

سرویس گیرنده	دنباله‌رمز	پروتکل
ANDROID-442	TLSv1.2	ECDHE-RSA-AES256-GCM-SHA384
ANDROID-500	TLSv1.2	ECDHE-RSA-AES128-GCM-SHA256
ANDROID-60	TLSv1.2	ECDHE-RSA-AES128-GCM-SHA256

سایت دوم:

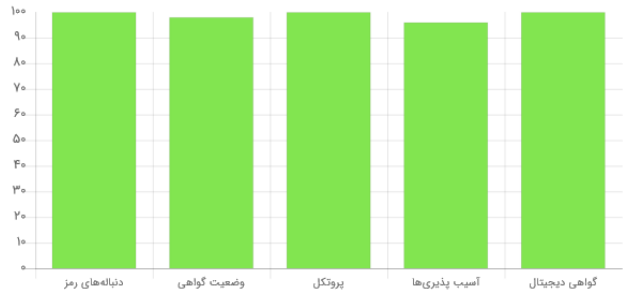

B
93.2 / 100
نمودار بررسی کیفیت
دنباله‌های رمز
وضعیت گواهی
پروتکل
آسیب پذیری‌ها
گواهی دیجیتال
دامنه، آدرس IP و شماره پورت
amazon.com
(205.251.242.103:443)
تاریخ و ساعت ارزیابی
Saturday 03 Dey 1401 14:11
مدت زمان ارزیابی
66 ثانیه
ارزیابی های انجام شده توسط "TLS1" نشان می دهد سرویس دچار آسیب پذیری است. در نتیجه رتبه سایت به B کاهش داده می شود
ارزیابی های انجام شده توسط "TLS1_1" نشان می دهد سرویس دچار آسیب پذیری است. در نتیجه رتبه سایت به B کاهش داده می شود
اطلاعات گواهی
آیا گواهی همچنان معتبر است؟
بله
تاریخ صدور گواهی
2022-10-19 00:00
تاریخ انقضای گواهی
2023-10-18 23:59
اطلاعات پروتکل
SSLv2
سرویس از SSLv2 پشتیبانی نمی‌کند که یک مزیت است. زیرا این پروتکل ناامن به شمار می‌رود.
SSLv3
سرویس از SSLv3 پشتیبانی نمی‌کند که یک مزیت است. زیرا این پروتکل ناامن به شمار می رود.
TLS1
سرویس از TLSv1.0 پشتیبانی می‌کند. این پروتکل ضعیف است. پیشنهاد می‌شود برای افزایش امنیت، پشتیبانی از این پروتکل را غیرفعال کنید.
TLS1.1
سرویس شما از TLSv1.1 پشتیبانی می‌کند. پیشنهاد می‌شود برای افزایش امنیت، پشتیبانی از این پروتکل را غیرفعال کنید.
TLS1.2
سرویس شما از TLSv1.2 پشتیبانی می‌کند. در حال حاضر این پروتکل پایدار به شمار می‌رود، اما بهتر است پشتیبانی از TLSv1.3 را هم مد نظر داشته باشید.
TLS1.3
سرویس شما از پروتکل TLSv1.3 پشتیبانی نمی‌کند. پیشنهاد می شود امکان پشتیبانی از این پروتکل را فراهم کنید.
الگوریتم‌های رمزنگاری
ارزیابی امنیت در مقابل حملات Fallback_SCSV
اتصال شما در مقابل حملات fallback_SCSV مقاوم است.
ارزیابی امنیت در مقابل حملات SWEET32
اتصال شما در مقابل حملات SWEET32 مقاوم است.
ارزیابی امنیت در مقابل حملات FREAK
اتصال شما در مقابل حملات FREAK مقاوم است.
ارزیابی امنیت در مقابل حملات DROWN
اتصال شما در مقابل حملات DROWN مقاوم است.
ارزیابی امنیت در مقابل حملات LOGJAM
اتصال شما در مقابل حملات LOGJAM مقاوم است.
ارزیابی وجود اعداد اول مشترک در زوج کلیدهای عمومی/محرمانه.
اتصال شما در مقابل حملات LOGJAM Common Primes آسیب‌پذیر است.
ارزیابی امنیت در مقابل آسیب پذیری CVE-2011-3389
اتصال شما در مقابل حملات BEAST_CBC_TLS1 آسیب پذیر است.
ارزیابی امنیت در مقابل حملات BEAST
اتصال شما در مقابل حملات BEAST آسیب پذیر است.
ارزیابی امنیت در مقابل حملات LUCK13
اتصال شما در مقابل حملات LUCKY13 آسیب پذیر است.
ارزیابی امنیت در مقابل حملات RC4
اتصال شما در مقابل حملات RC4 مقاوم است.
ارزیابی دنباله‌رمزها
TLSv1
TLSv1.1

سایت سوم:

A

98.8 / 100

نمودار بررسی کیفیت



دامنه، آدرس IP و شماره پورت
reddit.com (151.101.1.140:443)
تاریخ و ساعت ارزیابی
Saturday 03 Dey 1401 14:14
مدت زمان ارزیابی
60 ثانیه

اطلاعات گواهی

پشتیبانی از Strict Transport Security	365 days (=31536000 seconds) > 15465600 seconds
پشتیبانی HSTS از زیردامنه	includes subdomains
پشتیبانی از پیش‌بارگذاری HSTS	domain IS marked for preloading
پشتیبانی از Public Key Pinning	No support for HTTP Public Key Pinning
وضعیت Server Banner	snooserv
وضعیت Banner Application	No application banner found

اطلاعات پروتکل

ارزیابی امنیت در مقابل حملات LUCJAM	اتصال شما در مقابل حملات LUCJAM مقاوم است.
ارزیابی وجود اعداد اول مشترک در زوج کلیدهای عمومی/محرمانه.	اتصال شما در مقابل حملات LOGJAM Common Primes آسیب‌پذیر است.
ارزیابی امنیت در مقابل حملات BEAST	اتصال شما در مقابل حملات BEAST مقاوم است.
ارزیابی امنیت در مقابل حملات LUCK13	اتصال شما در مقابل حملات LUCKY13 آسیب پذیر است.
ارزیابی امنیت در مقابل حملات RC4	اتصال شما در مقابل حملات RC4 مقاوم است.