بسمه تعالی

سازمان فناوری اطلاعات ایران

معاونت امنیت فضای تولید و تبادل اطلاعات

مرکز ماهر

بررسی وضعیت پیاده سازی پروتکل HTTPS در وبسایت‌های میزبانی شده در کشور

تاریخ نگارش ..... ۱۶ اردیبهشت ۱۳۹۸

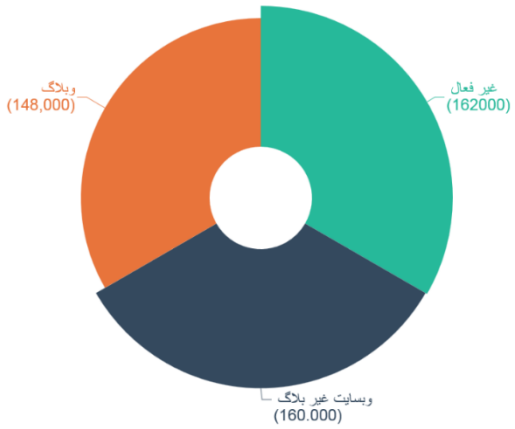
شمارهٔ نگارش ۵

فهرست مطالب

پیش‌گفتار

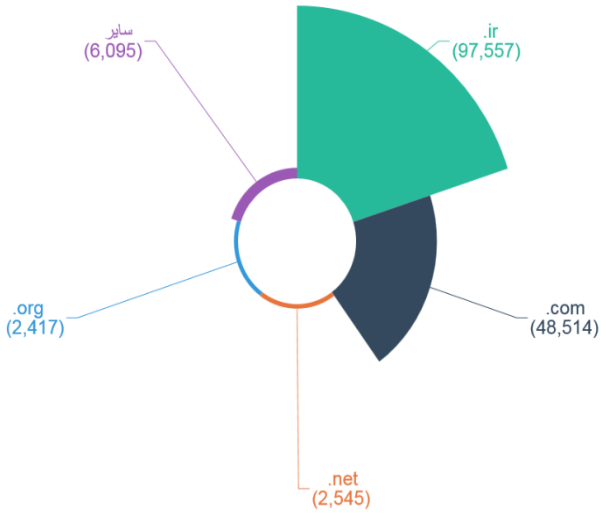
در سال‌های اخیر، پایش دائمی فضای اینترنت کشور بمنظور شناسایی تهدیدات و آسیب‌پذیری‌ها یکی از فعالیت‌های مرکز ماهر بوده است. یکی از حوزه های این پایش‌ها، وب‌سایت‌های میزبانی شده در کشور هستند. پایش فضای وب توسط سامانه جمع‌آوری و تحلیل وبسایت‌های این مرکز با استفاده از تکنیک‌های مختلف مانند Crawl، Web Scrape، Reverse DNS lookup و غیره جهت جمع‌آوری داده‌ها صورت می‌گیرد. سامانه فوق در طی مدت سه ماه زمستان ۱۳۹۷، بیش از ۴۷۰،۰۰۰ نام دامنه که در داخل کشور میزبانی می‌شوند را شناسایی کرده است. در این گزارش ارزیابی امنیت گواهی SSL این وبسایت‌ها میزان آسیب‌پذیری آن‌ها به حملات SSL مورد بررسی قرار خواهد گرفت. برای این منظور، با استفاده از ابزارهای ایجاد شده اقدام به ارزیابی امنیتی گواهی SSL کردیم. همچنین در ادامه با ارزیابی آسیب‌پذیری‌ها یا همان CVE های کشف شده برای گواهی‌های مختلف، نسبت به ارزیابی امنیتی وبسایت‌های مختلف از نگاه امنیت گواهی SSL و پیاده سازی آن، پرداخته‌ایم.

در ارزیابی‌های اولیه، مشخص شد که تقریبا ۱۶۲،۰۰۰ از این وبسایت‌ها غیرفعال می‌باشند. از این رو تمامی ارزیابی‌های بعدی تنها بر روی ۳۰۸،۰۰۰ وبسایت فعال در سطح کشور انجام گردید. از این تعداد، تقریبا ۱۴۸،۰۰۰ دامنه مربوط به وبلاگ‌های مختلف می‌باشند. از آنجایی‌که وبلاگ‌ها ذاتا دارای ماهیت نوشته‌های شخصی می‌باشند و زیرساخت و سیستم مدیریت محتوای آن‌ها نیز توسط سرویس‌دهنده تامین می‌شود، تمامی وبلاگ‌های متعلق به یک سیستم مدیریت محتوا را یک وبسایت در نظر گرفته و از بررسی جداگانه‌ی آن‌ها خودداری کردیم. لذا ارزیابی‌های مختلف تنها بر روی ۱۶۰،۰۰۰ وبسایت باقی‌مانده انجام شد.



فراوانی نام های دامنه اصلی کشور

در بین نام‌های دامنه متعلق به وبسایت‌های شناسایی شده، بیشترین فراوانی متعلق به دامنه‌های ir و com می‌باشد :



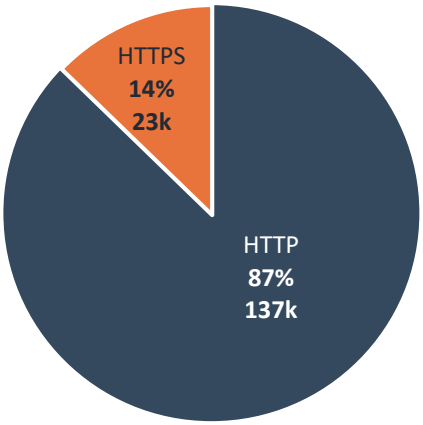
رتبه	نام‌دامنه‌ها	تعداد
۱	ir	۹۷,۵۵۷
۲	com	۴۸,۵۱۴
۳	net	۵,۲۸۹
۴	org	۲,۵۴۵
۵	سایر	۶,۰۹۵

استفاده از پروتکل ایمن HTTPS

اطلاعاتی که به طور معمول در صفحات وب رد و بدل می‌شوند در بستر پروتکل HTTP (مخفف Hyper Text Transfer Protocol) انتقال می‌یابند، این پروتکل استانداردی تعریف شده است که با آن متن و سایر اطلاعات چندرسانه‌ای در وب منتقل می‌گردد. این داده‌ها به دلیل عدم رمزگذاری برای سایرین (در صورت وجود دسترسی به ترافیک شبکه) نیز قابل خواندن هستند، لذا استفاده از پروتکل HTTP از لحاظ امنیتی برای انجام کارهایی که با اطلاعات حساس سر و کار دارند به هیچ وجه شیوه مناسبی نیست. به منظور رفع این ضعف، پروتکل دیگری به نام HTTPS (مخفف Hyper Text Transfer Protocol Secure) جهت انتقال داده های رمزگذاری شده توسط پروتکل SSL/TLS مورد استفاده قرار می گیرد.

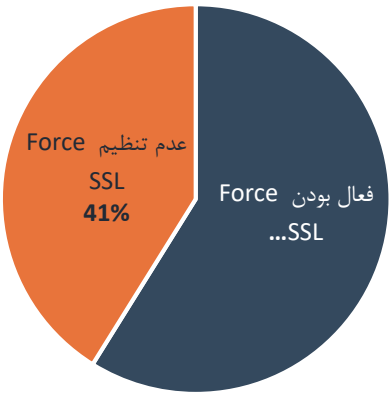
در زمان تدوین این گزارش بر اساس آمار وبسایت w3tech، تقریبا ۴۶٪ از وب‌سایت‌های جهان از این پروتکل HTTPS استفاده می‌کنند. این درحالی است که تنها ۱۴٪[۱] از وب‌سایت‌های کشور از پروتکل ایمن HTTPS استفاده می‌کنند.

[۱] البته با توجه به حذف تعداد زیادی از وبلاگ‌ها، مقایسه این دو آمار ممکن است منطقی نباشد



وضعیت وب‌سرور	تعداد
استفاده کننده از HTTP	۱۳۶,۶۰۰
استفاده کننده از HTTPS	۲۳,۳۷۶

مورد مهم قابل بررسی دیگر در ارزیابی مکانیزم HTTPS بررسی قابلیت Force SSL است. در صورتی که این قابلیت در یک وبسایت فراهم باشد، تمامی درخواست‌ها، به صورت ایمن و از طریق HTTPS پاسخ داده خواهند شد. با انجام ارزیابی اولیه بر روی وبسایت‌هایی که از HTTPS استفاده می‌کنند مشخص گردید که از این بین ۵۹٪ Force SSL را بر روی میزبان خود فعال نموده‌اند.



وضعیت وب‌سرور	تعداد
عدم تنظیم Force SSL	۹،۵۰۴
فعال بودن Force SSL	۱۳،۸۷۲

پیاده‌سازی و استفاده ایمن از این پروتکل دارای جزئیات فنی متعددی است که می‌بایست به‌درستی رعایت شود. در صورت عدم رعایت ملاحظات و نکات امنیتی در پیاده‌سازی این پروتکل، محرمانگی و یکپارچگی داده‌های مبادله شده به خطر می‌افتد.

اعتبار گواهیSSL

گواهی SSL جهت استفاده در وبسایت ها در سه دسته ارائه می‌شوند:

گواهینامه Domain Validation: در این نوع از گواهینامه SSL صادر کننده گواهینامه بر اساس نام دامنه اعتبار سنجی را انجام می‌دهد و به بررسی صحت یا اعتبار سازمان یا صاحب دامنه نمی‌پردازد.

گواهینامه Organization Validation: این نوع گواهینامه SSL علاوه بر تامین امنیت در صدد تایید اعتبار یک کسب و کار و تجارت اینترنتی است و سطح اعتبار بسیار بالاتری نسبت به گواهینامه SSL DV را دارا می باشد و بازدید کنندگان وب سایت مربوطه با مشاهده نام سازمان در بخش جزئیات گواهینامه با اطمینان از این وب سایت‌ها سرویس می‌گیرند.

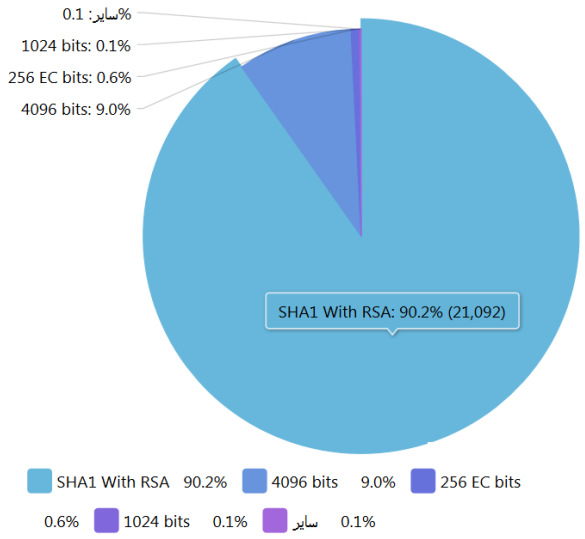
گواهینامه Extended Validation: مشخصه اصلی این نوع گواهینامه نشان سبز رنگ در مرورگر است و روند دریافت آن بسیار شبیه گواهینامه OV ولی با اعتبار و ارزشی بالاتر است. این نوع گواهی نامه SSL فقط برای سازمان های دولتی، شرکت‌ها، بانک‌ها، وزارتخانه‌ها و به طور کل اشخاص حقوقی صادر می‌گردد. در دامنه‌های بررسی شده تنها ۶۸ مورد ازآن‌ها دارای گواهی SSL EV هستند. متاسفانه پیکربندی اشتباه در این سایت‌ها نیز قابل مشاهده است.

طول کلید SSL

گواهی SSL دو کلید عمومی و اختصاصی دارد. این کلیدها برای برقراری یک ارتباط رمزگذاری شده مشترکا استفاده می‌شوند. طول کلیدها می‌تواند از ۵۱۲ تا ۴۰۹۶ بیت باشد معمولا جهت برقراری ارتباط امن از کلیدهایی با طول ۲۰۴۸ تا ۴۰۹۶ بیت استفاده می‌شود. البته امکان ساخت کلیدهای بزرگتر از ۴۰۹۶ بیت هم وجود دارد، با این وجود این نوع کلیدها به دلیل بار محاسباتی زیادی که دارند به ندرت استفاده می‌شوند.طول کلیدهای استفاده شده در وب‌سایت‌های مورد بررسی مناسب می‌باشد و تنها ۴۵ وب‌سایت از کلیدهایی با سایز کوچک استفاده می‌کنند.

فراوانی طول کلید استفاده شده در گواهی SSL

وضعیت طول کلید استفاده شده در گواهی SSL که کشف شده است. مناسب است و تنها در ۴۵ مورد امکان سواستفاده از طول کلید وجود دارد.



رتبه	طول کلید	تعداد
۱	2048 bits	۲۱،۰۹۲
۲	4096 bits	۲،۱۰۲
۳	256 EC bits	۱۳۷
۴	1024 bits	۳۰
۵	سایر	۱۵

اعتبار صادر کننده کلید

مهم‌ترین بخش گواهی SSL، امضاء الکترونیکی آن توسط یک صادرکننده معتبر گواهی است. هرکسی می‌تواند این گواهینامه را صادر کند، اما مرورگرها فقط به گواهینامه‌هایی اعتماد می‌کنند که از سوی CA های مورد تایید صادر شده باشند. برای حفظ محرمانگی امضای گواهی دیجیتال این امضا رمزگذاری می‌شود. ۲۳،۱۵۰ وب‌سایت از الگوریتم رمزگذاری SHA256 with RSA استفاده می‌کنند.

رتبه	وب‌سرور	تعداد
۱	SHA256 with RSA	۲۳،۱۵۰
۲	sha1WithRSA	۱۳۰
۳	ECDSA with SHA256	۶۹
۴	نامشخص	۱۷
۵	SHA512 with RSA	۱۱

دو راه برای دریافت گواهینامه SSL وجود دارد. راه حل اول این است که شما به عنوان یک مدیر وب‌سایت گواهینامه صادر کرده و آن را امضا کنید و کلیدهای رمزگذاری ایجاد نمایید. به چنین گواهی‌نامه‌هایی خود امضا (self-signed certificate) گفته می‌شود. وقتی کاربران می‌خواهند وارد چنین وب‌سایت‌هایی شوند توسط مرورگر هشداری در خصوص غیر قابل اعتماد بودن امضای دیجیتال را متذکر می‌شود. گواهی خود امضا با گواهی‌های دیگر SSL تفاوت چندانی از نظر میزان ایجاد امنیت ندارد. این گواهی نیز مانند گواهی‌های دیگر رمز شده و امن است. تنها تفاوت این گواهی با گواهی های صادر شده توسط CAهای معتبر این است که مرورگر یا سیستم‌عامل نمی تواند مستقلا اعتبار آنها را تایید کند.

راه حل دوم خریداری گواهینامه معتبر از یک مرکز صدور گواهی **Certificate Authority (CA)** معتبر است . در واقع کاری که این مراکز انجام می‌دهند این است که اسناد صاحب سایت و حق مالکیت دامنه را بررسی و تایید می‌کنند. البته در حال حاضر برخی شرکت‌ها اقدام به ارائه **SSL رایگان** برای سایت‌ها می‌کنند که امکان استفاده از آن ها برای اکثر دامنه‌های ir. نیز فراهم است.

دو نوع مرکز صدور گواهی ریشه (**root CA**) **و میانی (intermediate CA)** وجود دارد. برای اینکه گواهی قابل اعتماد تشخیص داده شود باید در فهرست مراکز صدور گواهی‌های مورد اعتماد سیستم‌عامل یا مرورگر قرار داشته باشد. اگر مرکز صدور گواهی در فهرست دستگاه وجود نداشته باشد، دستگاه به بررسی گواهی مرکز صدور گواهی میانی می‌پردازد. و اینکار تا زمان رسیدن به مرکز صدورگواهی ریشه یا یک گواهی قابل اعتماد برای دستگاه ادامه می‌یابد. اگر هیچ مرکز صدور گواهی قابل اعتمادی شناسایی نشود، آنگاه گواهی SSL غیر قابل اعتماد تلقی می‌شود. بیش از ۹۵٪ گواهی‌های شناسایی شده در این بررسی قابل اعتماد بوده و زنجیره معتبر است.

طی این بررسی مشخص شد ۴۳٪ از وب سایت‌های کشور گواهی خود را از مرکز صدور گواهی Let’s Encrypt تهیه کرده‌اند.

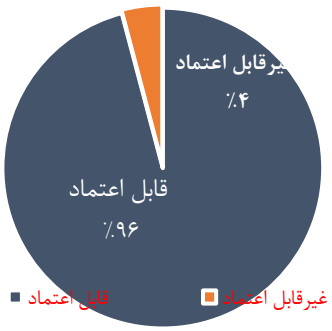
هزینه صدور گواهی SSL

استفاده از گواهی‌ها همیشه رایگان نیست و برای تهیه گواهی با کیفیت بهتر و دارای ضمانت مالی و اعتبار کافی باید هزینه پرداخت کرد. هزینه خرید یک گواهی معتبر به عوامل مختلفی بستگی دارد:

- مرکز صدور گواهی
- نوع گواهی (OV، DV و EV)
- مدت اعتبار گواهی
- چند دامنه بودن گواهی (Single Domain یا Multi Domain)

زنجیره اعتماد گواهی SSL

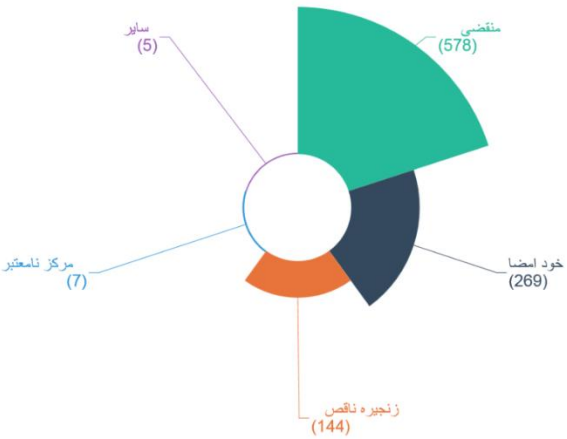
علاوه بر مرکز صدور گواهی، عواملی مانند تاریخ انقضای گواهی و زنجیره ناقص موجب غیر قابل اعتماد بودن گواهی می‌شود. در ۹۵٪ از وبسایت‌های مورد بررسی، گواهی قابل اعتماد تشخیص داده شده است.



وضعیت زنجیره گواهی	تعداد
قابل اعتماد	۲۲,۳۶۴
غیر قابل اعتماد	۱,۰۰۳

یکی از دلایل اصلی عدم اعتبار زنجیره گواهی SSL ، گذشت تاریخ انقضای گواهی SSL می‌باشد. هر گواهی SSL برای بازه زمانی مشخصی معتبر است و می‌تواند برای ایجاد ارتباط امن مورد استفاده قرار گیرد. زمانیکه این بازه زمانی مشخص به اتمام می‌رسد گواهی منقضی شده و مرورگر و برنامه‌های دیگر از پذیرش گواهی منقضی شده خودداری می‌کنند.

زمانیکه شما یک گواهی را از مراکز صدور گواهی معتبر درخواست می‌کنید. در واقع مراحلی طی می‌شود و مالکیت دامنه‌ای که برای آن درخواست گواهی دارید بررسی شده و اطمینان حاصل می‌شود که شما نتوانید گواهیSSL را برای دامنه‌ای که مالکیت آن را در اختیار ندارید تهیه کنید. در واقع مراکز صدور گواهی، در گواهی که به شما ارائه می‌دهند اعتبار وبسایت شما را تایید می‌کنند و تاریخ انقضا مدت اعتبار این اطلاعات را مشخص می‌کند. مدت اعتبار گواهی‌های مرکز LetsEncrypt معمولا سه ماه باشد. تعداد ۱۰،۴۹۳ وب‌سایت دارای مدت اعتبار گواهی ۳ ماهه هستند که این عدد به صورت مشخصی با تعداد وب‌سایت‌های که از مرکز صدور گواهی LetsEncrypt تهیه شده بودند قرابت دارد. در ۱،۰۰۳ وبسایت زنجیره گواهی غیر قابل اعتماد می‌باشدکه در بیش از ۵۰٪ دلیل عدم موفقیت زنجیره گواهی، گذشت تاریخ انقضای سایت می‌باشد.



رتبه	وضعیت زنجیره گواهی	تعداد
۱	منقضی	۵۷۸
۲	خود امضا	۲۶۹
۳	زنجیره ناقص گواهی	۱۴۴
۴	مرکز صدور گواهی غیر قابل اعتماد	۷
۵	سایر	۵

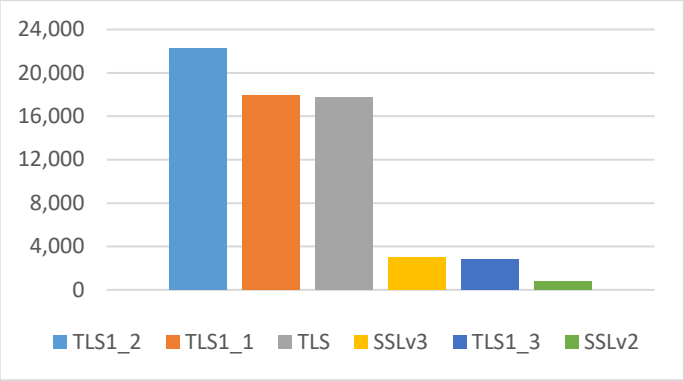
بازه زمانی اعتبار گواهی	تعداد
سه ماهه	۱۰,۴۹۳
یک ساله	۵,۹۶۲
دو سال	۳,۰۷۵
بیش از دو سال	۳,۸۳۷

بررسی میزان آسیب‌پذیری تنظیمات گواهی SSL

پروتکل SSL توسط کمپانی Netscape ابداع شد. SSLv2 وSSLv3 دو نسخه از این پروتکل هستند. بعد از SSLv3 این پروتکل به TLS تغییر نام یافت. TLS مخفف Transport Layer Security و به معنای پروتکل امنیتی لایه انتقال می‌باشد. TLS از TLSv1.0 که نسخه بروز شده SSLv3 می‌باشد، شروع شده است.

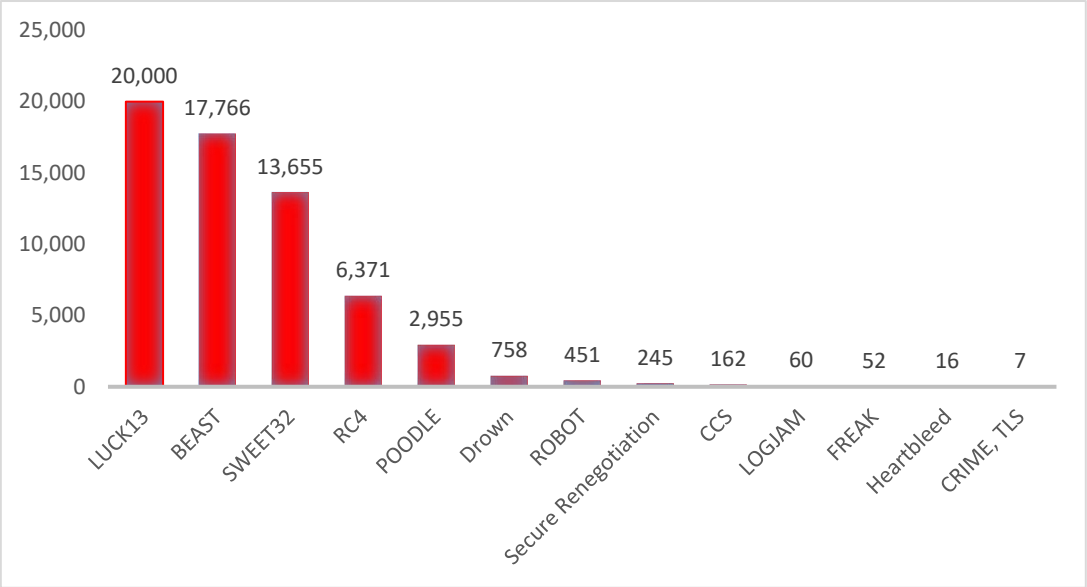
پروتکل SSLv2 آسیب‌پذیر می‌باشد و توصیه می‌گردد که این پروتکل غیرفعال گردد. همچنین پروتکل SSLv3 به دلیل وجود آسیب‌پذیری POODLE در آن ناامن است و برای جلوگیری از سواستفاده نفوذگران باید غیرفعال گردد. در حال حاضر متخصصین امنیت فقط دو پروتکل SSLv2 و SSLv3 را منسوخ شده در نظر می‌گیرند. استفاده از پروتکل TLS 1.1 نیز به دلیل آسیب‌پذیر بودن در برابر حملاتی نظیر FREAK, POODLE, BEAST و CRIME نامناسب است. تقریبا در همه‌ی وب‌سایت‌های مورد بررسی از پروتکل TLS1.2 پشتیبانی می شود، لذا در صورت غیر فعال‌سازی پروتکل‌های منسوخ شده و استفاده از دنباله رمزهای قوی در پروتکل TLS1.2، امنیت گواهی SSL وبسایت-ها به صورت چشم‌گیری افزایش خواهد یافت. در حال حاضر در ۲،۹۹۹ گواهی SSL از پروتکل‌های منسوخ شده پشتیبانی می‌کنند می‌شود. همچنین ۱۷،۹۵۳ وبسایت نیز از پروتکل TLS1.0 پشتیبانی می‌کنند که استفاده از آن موجب بروز آسیب‌پذیری در گواهی SSL می‌شود.

پروتکل	تعداد
TLS1.2	۲۲,۲۵۷
TLS1_1	۱۷,۹۵۳
TLS	۱۷,۷۸۵
SSLv3	۲,۹۹۲
TLS1_3	۲,۸۱۲
SSLv2	۷۷۳



میزان آسیب‌پذیری وب‌سایت‌های کشور در برابر حملات شناخته شده

حمله	شدت	امتیاز بر اساس CVSS	CVE	تعداد
LUCKY13	پایین	۲,۶	CVE-2013-0169	۲۰،۰۰۰
BEAST	متوسط	۴,۳	CVE-2011-3389	۱۷،۷۶۶
SWEET32	بالا	۵	CVE-2016-2183	۱۳،۶۵۵
ضعف RC4	متوسط	۴,۳	CVE-2013-2566, CVE-2015-2808	۶،۳۷۱
POODLE	متوسط	۴,۳	CVE-2014-3566	۲،۹۵۵
Drown	متوسط	۴,۳	CVE-2016-0800	۷۵۸
ROBOT	متوسط	۴,۳	CVE-2017-13099	۴۵۱
Secure Renegotiation	متوسط	۵,۸	CVE-2009-3555	۲۴۵
CCS	متوسط	۶,۸	CVE-2014-0224	۱۶۲
LOGJAM	پایین	۴,۳	CVE-2015-4000	۶۰
FREAK	متوسط	۴,۳	CVE-2015-0204	۵۲
Heartbleed	متوسط	۵	CVE-2014-0160	۱۶
CRIME, TLS	پایین	۲,۶	CVE-2012-4929	۷



مقایسه وضعیت دامنه‌های با پروتکل TLS1.2

میزان آسیب‌پذیری گواهی در هنگامی که در گواهی فقط از پروتکل TLS1.2 استفاده می‌شود به صورت چشم‌گیری کاهش می‌یابد

نام آسیب‌پذیری	تعداد وبسایت‌های آسیب‌پذیر دارای پروتکلTLS1.2	نسبت وبسایت-های آسیب‌پذیر دارای پروتکل TLS1.2	تعداد وبسایت-های آسیب‌پذیر شامل پروتکل-های دیگر	نسبت وبسایت‌های آسیب-پذیر شامل پروتکل‌های دیگر
LUCKY13	۴،۲۹۱	۰،۹۹۶	۱۹،۰۴۶	۰،۹۹۸
BEAST	۰	.	۱۷،۷۶۶	۰،۹۳۲
SWEET32	۹۵	۰،۰۲۲	۱۳،۴۷۱	۰،۷۰۶
RC4	۳۲	۰،۰۰۷	۶،۳۳۹	۰،۳۳۲
POODLE_SSL	۰	۰	۲،۹۵۵	۰،۱۵۵
DROWN	۰	۰	۷۵۸	۰،۴۰
ROBOT	۴	۰	۴۴۷	۰،۰۲۳
Secure_client renego	۷	۰،۰۰۲	۲۴۷	۰،۱۳
CCS	۰	۰	۱۶۲	۰،۰۱

بررسی وضعیت دنباله رمز

زمانیکه ارتباط HTTPS از طریق پروتکلTLS برقرار می‌شود دنباله رمزگذاری (Cipher Suite)، تعیین می‌کند که امنیت هر بخش از ارتباط سرور و مشتری چگونه تامین شود. در واقع نام هر مجموعه نشان دهنده الگوریتم‌های استفاده شده در آن است. البته برای نمایش هر کدام از الگوریتم‌ها از عبارت اختصاری همان الگوریتم استفاده می‌شود. از جمله الگوریتم‌های که در یک دنباله رمز گذاری وجود دارد عبارت است از:

Key exchange Algorithm: روشی که با آن کلیدهای متقارن تعویض می‌شوند

Authentication Algorithm: روشی که با آن نحوه اطلاعات تعین هویت سرور و (در صورت نیاز) اطلاعات تعین هویت کاربر انتقال می‌یابد

Bulk Encryption Algorithm: روشی که الگوریتم متقارنی را که برای رمزگذاری داده اصلی استفاده می‌شود مشخص می‌کند.

Message Authentication Algorithm: روشی که برای بازرسی یکپارچگی اطلاعات استفاده می‌شود

نمونه الگوریتم‌های مختلف قابل استفاده در دنباله رمز

روش	الگوریتم‌های مرسوم
Key exchange Algorithm	RSA, DH, ECDH, ECDHE SRP, PSK
Authentication Algorithm	RSA, DSA, ECDSA
Bulk Encryption Algorithm	AES, 3DES, CAMELLIA
Message Authentication Algorithm	HMAC-SHA256, HMAC-SHA1, HMAC-MD5

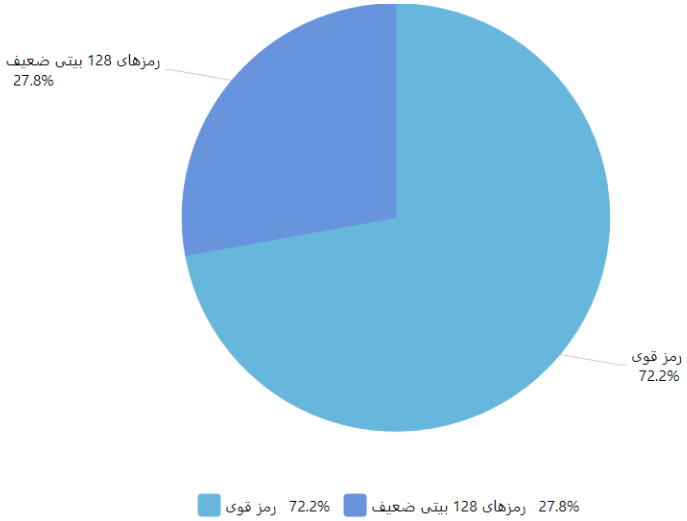
وضعیت دنباله‌های رمز استفاده شده

در فصل قبل گزارش نشان داده شد که چگونه استفاده از پروتکل‌های آسیب پذیر امنیت ارتباطات SSL/TLS را به خطر می‌اندازد. در ادامه باید بیان کرد که بسیاری از بردارهای حمله از نقص‌های خود TLS مانند Protocol downgrades، connection Renegotiation و Session resumption استفاده می‌کنند. معروف‌ترین حمله بر علیه دنباله‌های رمز Downgrade Attack می‌باشد. Downgrade در TLS زمانی رخ می‌دهد که یک مرورگر مدرن به سرور که از نسخه‌های قدیمی TLS و SSL استفاده می‌کند وصل می‌شود. هدف از ایجاد قابلیت Downgrade سازگاری با نسخه‌های قدیمی TLS بوده است. با این حال امکان سواستفاده از این ویژگی توسط نفوذگران وجود دارد به نحوی که مرورگر به صورت خودکار مجبور به استفاده از نسخه‌های پایین پروتکل‌ها شود. پروتکل‌های قدیمی‌تر از دنباله رمز

ضعیف‌تر استفاده می‌کنند و دارای آسیب‌پذیری‌های شناخته شده مانند POODLE هستند. یکی از بهترین روش‌ها برای جلوگیری از این نقص، غیر فعال سازی امکان Downgrade است.

میزان استفاده از رمزهای ۱۲۸ بیتی ضعیف

نوع رمز	تعداد
رمزهای ۱۲۸ بیتی ضعیف	۶،۵۰۷
عدم استفاده	۱۶،۸۶۰



بررسی میزان استفاده از رمزهای ضعیف 3DES

دنباله رمز 3DES که یک الگوریتم کلید متقارن بلوکی است. الگوریتم DES را سه بار به هر بلوکی داده اعمال می‌کند. در این الگوریتم به دلیل استفاده از بلوک‌ها با اندازه کوچک ۶۴ بیتی امکان تداخل و درنتیجه افشای کلید وجود دارد. در حال حاضر در بیش نیمی از دامنه‌های دارای HTTPS این الگوریتم ضعیف رمزگذاری استفاده می‌شود که این رمزگذاری موجب آسیب‌پذیری سیستم در مقابل حملات شناخته شده مانند SWEET32 می شود. در واقع حمله SWEET32 بر اساس دنباله رمز 3DES طراحی شده است و همه وبسایت‌هایی که از این رمزگذاری استفاده می‌کنند آسیب‌پذیر هستند. همچنین میزان آسیب‌پذیری به حمله BEAST نیز در زمان استفاده از این رمزگذاری به صورت قابل ملاحظه‌ای افزایش می‌یابد.

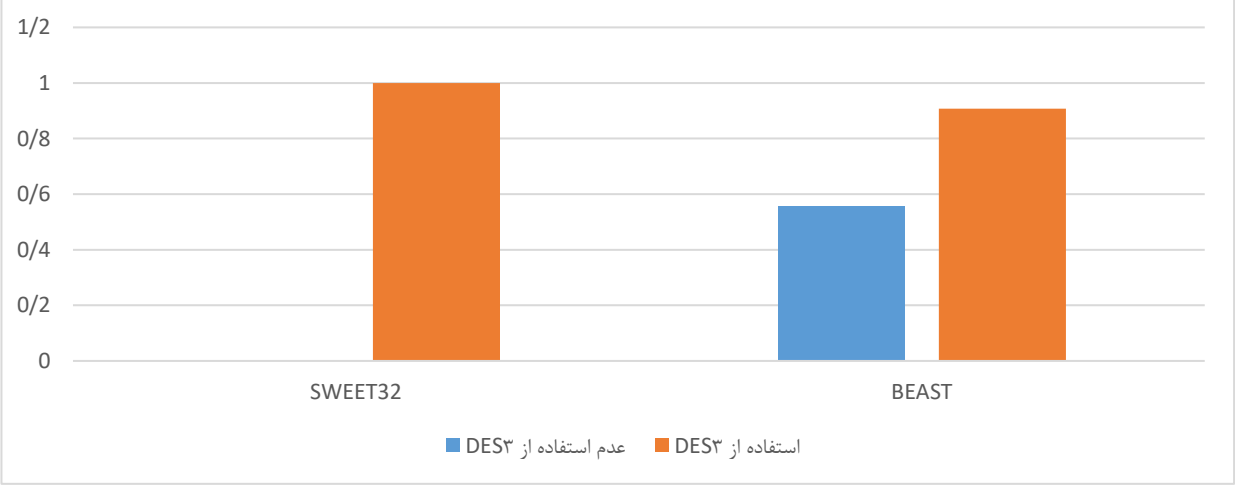
تعداد

رمزهای 3DES	۱۳,۵۶۷
عدم استفاده	۹,۸۰۰

بررسی وضعیت آسیب‌پذیری به SWEET32 و BEAST هنگام فعال بودن دنباله رمز 3DES

حمله SWEET32 بر اساس دنباله رمز 3DES طراحی شده است و همه سایت‌هایی که از این رمزگذاری استفاده می‌کنند آسیب‌پذیر هستند.

	وضعیت گواهی‌هایی با 3DES فعال
استفاده از رمز 3DES	۱۳،۵۶۷
آسیب‌پذیری به SWEET32	۱۳،۵۶۶
آسیب‌پذیری به BEAST	۱۲،۳۱۸
	وضعیت گواهی‌هایی با 3DES غیرفعال
عدم استفاده از رمز 3DES	۹،۸۰۰
آسیب‌پذیری به SWEET32	۰
آسیب‌پذیری به BEAST	۵،۴۴۸

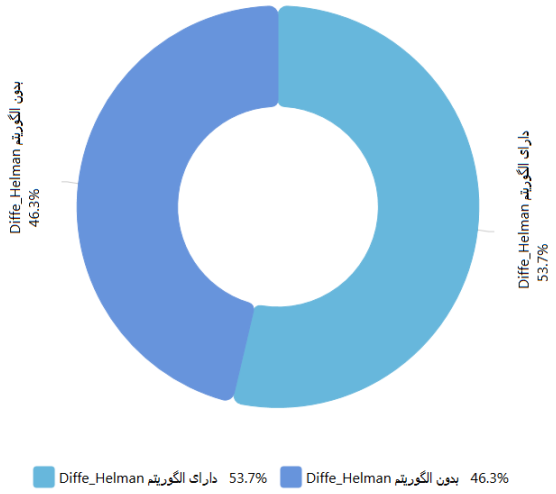


بررسی فراوانی استفاده از الگوریتم Diffe_Hellman

یکی دیگر از حمله شناخته شده LOGJAM می‌باشد که بر علیه الگوریتم Diffie-Hellman رخ می‌دهد. این حمله به مهاجم مرد میانی این اجازه را می‌دهد تا پروتکل‌های آسیب‌پذیر را وادار به برقراری ارتباط با دنباله رمز ضعیف کند. این آسیب‌پذیری به کاربران امکان مشاهده و ویرایش اطلاعات را می‌دهد. در فرمول‌های پیشنهادی این الگوریتم، عدد اول p و عملگر ضرب اعداد صحیح استفاده شده‌است. گروه‌های همنهشتی مختلف استفاده شده در این الگوریتم، قدرت آن را تحت تاثیر قرار می‌دهد. بیشتر گروه‌های استفاده شده در وبسایت‌های کشور دارای امنیت لازم هستند و احتمال حمله LOGJAM تنها در ۶۰ دامنه وجود دارد. دامنه‌های آسیب‌پذیر از گروه‌های ضعیف mod_ssl 2.2.x/1024-bit MODP group with safe prime modulus و Unknown DH group (1024 bits) استفاده می‌کنند.

Diffe_Hellman یکی از الگوریتم‌های قوی است که در زمان تعویض کلید استفاده می‌شود ولی اگر از گروه‌های ضعیف در آن استفاده شود امکان حمله LOGJAM را فراهم می‌آورد

نوع رمز	تعداد
دارای DH گروه	۱۲،۵۴۹
بدون DH گروه	۱۰،۸۲۱

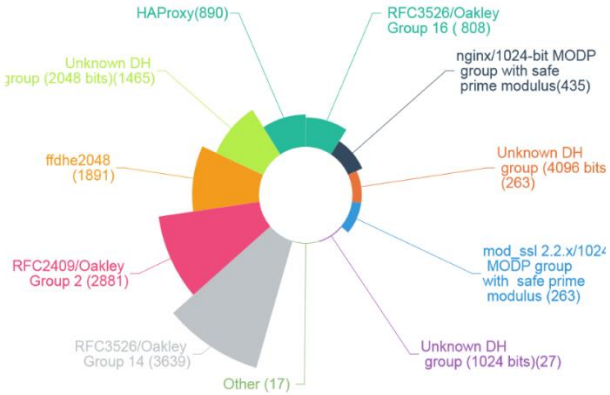


بررسی فراوانی DH گروه‌های مختلف

بسیاری از گروه‌های DH استفاده شده در وبسایت‌های کشور قدرتمند می‌باشند و در نتیجه تعداد وبسایت‌های آسیب-پذیر به حمله LOGJAM کم است.

گروهDH	تعداد
RFC3526/Oakley Group 14	۳,۶۳۹

RFC2409/Oakley Group 2	۲,۸۸۱
ffdhe2048	۱,۸۹۱
Unknown DH group (2048 bits)	۱,۴۶۵
HAProxy	۸۹۰
RFC3526/Oakley Group 16	۸۰۸
nginx/1024-bit MODP group with safe prime modulus	۴۳۵
Unknown DH group (4096 bits)	۲۶۳
mod_ssl 2.2.x/1024-bit MODP group with safe prime modulus	۲۳۳
Unknown DH group (1024 bits)	۲۷
سایر	۱۷



آسیب‌پذیری BEAST ناشی از ضعف در روش استفاده SSL/TLS از دنباله رمزگذاری بلوکی (Cipher Block Chaining) می‌باشد. دنباله رمزگذاری بلوکی یا CBC mode شامل همه انواع رمزگذاری‌های بلوکی مانند: AES و 3DES می‌باشد. این آسیب‌پذیری امکان حمله مرد میانی را فراهم می‌آورد و موجب افشای اطلاعات می‌شود. آسیب‌پذیری نسبت به حمله BEAST در پروتکل‌های نسخه TLS1.0 و SSLv3 وجود دارد. پروتکل‌هایTLS1.1 و TLS1.2 و همه دنباله رمزگذاری‌هایی که از CBC mode استفاده نمی‌کنند تحت تاثیر BEAST قرار ندارند. BEAST صرفا یک حمله سمت کاربر است و از زمانیکه به صورت عمومی منتشر شد، بسیاری از مرورگرها آن را با استفاده از روشی با نام 1/n-1 رفع کردند.

SSLv3 در ۲،۹۹۲ وب‌سایت پشتیبانی می‌شود که بیش از ٪۹۸ آنها از دنباله رمزگذاری CBC mode استفاده می‌کنند. ۴۶ دنباله رمز مختلف دارای CBC در پروتکل مشاهده شده که "DES-CBC3-SHA" با۲،۲۵۲ تکرار بیشترین فراوانی را در دنباله رمزهای آسیب‌پذیر دارد.

میزان استفاده از CBC در پروتکل SSLv3

در میان تمام دامنه که از پروتکل SSLv3 استفاده می‌کنند، تنها ۳۸ دامنه از CBC استفاده نکرده اند

وضعیت استفاده از CBC در پروتکل‌های SSLv3	
عدم استفاده از CBC	۳۸
استفاده از CBC	۲,۹۵۴

۱۷,۷۸۵ گواهی در حال حاضر از 0.TlS1 استفاده می‌کنند که بیش از ۹۹٪ آن‌ها از دنباله رمزگذاری CBC mode استفاده می‌کنند. تمام گواهی‌هایی که از دنباله رمز CBC استفاده می‌کنند و پروتکل TLS1-0 یاSSLv3 آنها فعال است نسبت به حمله BEAST آسیب‌پذیر هستند. در ۲،۹۵۰ مورد دنباله رمزگذاری ضعیف در هر دو نسخه SSLv3 و TLS1-0 مشاهده شده است.

میزان استفاده از CBC در پروتکل TLS1.0

در میان تمام دامنه که از پروتکل SSLv3 استفاده می‌کنند، تنها ۲۳ دامنه از CBC استفاده نکرده اند

وضعیت استفاده از CBC در پروتکل‌های SSLv3	
عدم استفاده از CBC	۲۳
استفاده از CBC	۱۷،۷۶۲

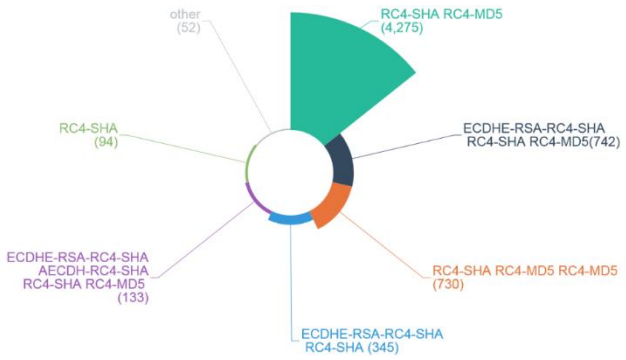
آسیب‌پذیری دیگر Lucky13 می‌باشد این آسیب‌پذیری برخلاف BEAST نیازمند اجرای کد در سمت مرورگر نیست. اما مانند BEAST ویژگی‌های CBC موجب ایجاد حمله شده است. این حمله به تمام پیاده‌سازی‌های پروتکل‌های TLS که با TLS1.1و TLS1.2 سازگار هستند اعمال می‌شود. در واقع این حمله نوع پیشرفته حمله POODLE می‌باشد و برای رفع آن نباید از mode CBC استفاده کرد یا اینکه با اعمال تغییراتی در روال رمزگشایی دنباله آسیب-پذیر مانع از وقوع این حمله شد. اما این حمله قابل اعمال به همه نسخه‌های SSL3.0 و TLS1.0 می‌باشد.

در صورت استفاده از TLS1.0 یا SSLv3 یک راه حل برای کاهش حمله BEAST استفاده از دنباله RC4 است. اما متاسفانه خود این رمز هم دارای آسیب‌پذیری می‌باشد و احتمالا به زودی منسوخ خواهد شد. ۶،۳۷۱ وبسایت دارای دنباله ضعیف RC4 هستند. در حقیقت در عمل نمی‌توان برای کاهش اثرات حمله BEAST از RC4 استفاده کرد زیرا دامنه اثر RC4 شامل همه کاربران می‌شود در حالی که BEAST فقط برخی از کاربران را شامل می‌شود.

فراوانی دنباله رمزگذاری RC4

دنباله RC4-SHA RC4-MD5 که در بیش از ۶۵٪ از دامنه‌ها استفاده شده است. بیشترین فراوانی را در دنباله‌های آسیب‌پذیر موجود در کشور دارد

دنباله RC4	تعداد
RC4-SHA RC4-MD5	۴،۲۷۵
ECDHE-RSA-RC4-SHA RC4-SHA RC4-MD5	۷۴۲
RC4-SHA RC4-MD5 RC4-MD5	۷۳۰
ECDHE-RSA-RC4-SHA RC4-SHA	۳۴۵
ECDHE-RSA-RC4-SHA AECDH-RC4-SHA RC4-SHA RC4-MD5	۱۳۳
RC4-SHA	۹۴
other	۵۲



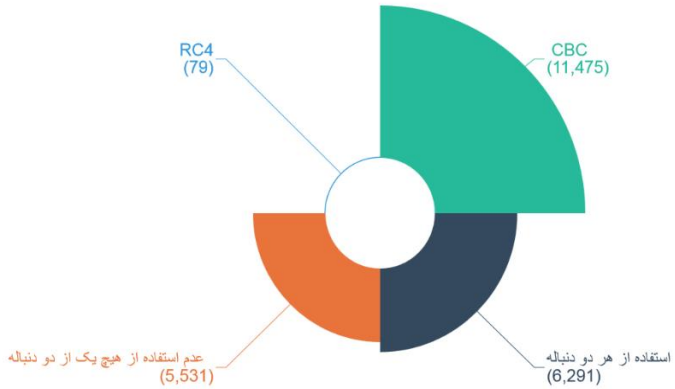
به طور خلاصه می‌توان گفت دنباله رمزگذاری RC4 که برای مدتی به عنوان جایگزینی برای دنباله‌هایCBC استفاده می‌شد، دارای آسیب‌پذیری با شدت متوسط می‌باشد که ۶،۳۷۱ دامنه را تحت تاثیر قرار می‌دهد. ۶،۲۹۱ دامنه از هر دو دنباله RC4 و CBC استفاده می‌کنند و نسبت به BEAST و RC4 آسیب‌پذیر هستند. امروزه برای افزایش امنیت از الگوریتم‌های رمزگذاری مدرن مانند: AES، modes (GCM)، ChaCha20 استفاده می‌شود.

بررسی میزان استفاده از دو دنباله CBC-mode و RC4

در ۱۱،۴۵۷ وبسایت از هر دو دنباله رمز RC4 و BEAST استفاده شده است

نوع	تعداد
استفاده از CBC و عدم استفاده از RC4	۱۱،۴۷۵
استفاده از هر دو دنباله	۶،۲۹۱

عدم استفاده از هیچ یک از رمزگذاری‌های CBC و RC4	۵،۵۳۱
عدم استفاده از CBC و استفاده از RC4	۷۹

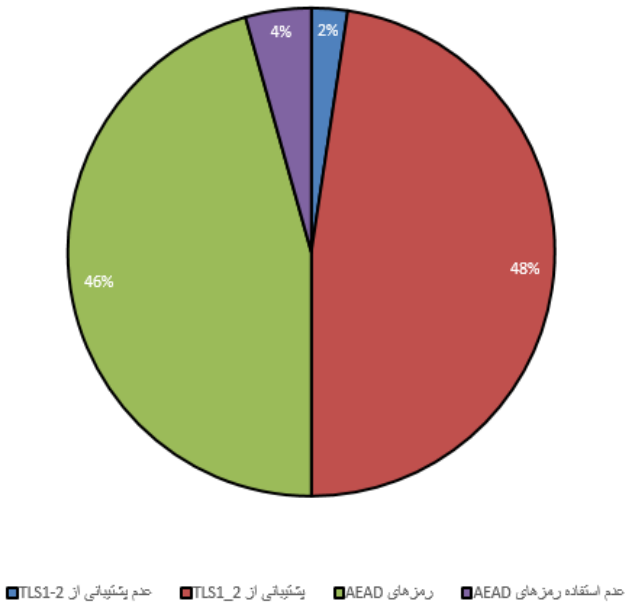


دنباله‌هایی مانند AES با Camellia، دنباله رمزگذاری قوی است که تقریبا در همه وبسایت‌های مورد بررسی ارائه شده است. همچنین دنباله رمز Authenticated Encryption with Associated Data یکی از دنباله‌های قوی است که در پروتکل TLS1.2 ارائه شده است. این دنباله جایگزین مناسبی برای CBC و RC4 می‌باشد. یکی از ویژگی‌های مهم در پروتکل‌های امنیتی قدرتمند ویژگی Perfect *Forward Secrecy* می‌باشد. این ویژگی تضمین می‌کند که حتی اگر کلید خصوصی افشا شود کلید نشست (Session) لو نخواهد رفت. این ویژگی در اکثر وبسایت‌های مورد بررسی فعال می‌باشد.

بررسی میزان استفاده از رمزهای قوی AEAD

٪۹۱ از دامنه‌های وبسایت‌ها رمزAEAD را ارائه می‌دهند.

نوع	تعداد
عدم پشتیبانی از TLS1.2	۱،۱۱۹
پشتیبانی از TLS1.2	۲۲،۲۵۷
رمزهای AEAD	۲۱،۳۳۷
عدم استفاده رمزهای AEAD	۲،۰۳۹



بررسی فراوانی استفاده از *Perfect Forward Secrecy*

این ویژگی تضمین می‌کند که حتی اگر کلید خصوصی افشا شود، کلید نشست لو نخواهد رفت.

وضعیت استفاده از Perfect *Forward Secrecy*	
غیر فعال	۲۲۲
فعال	۲۲،۱۴۵

ویژگی مهم دیگری که بهتر است در پروتکل‌های امنیتی فعال باشد HTTP Public Key Pinning می‌باشد. این ویژگی به مرورگرمی‌گوید که کلید عمومی مشخصی را به وب سرورهای معین نسبت دهد تا خطر حمله مرد میانی را کاهش دهد. متاسفانه این ویژگی در هیچ یک از وب‌سایت‌های شناسایی شده فعال نمی‌باشد.

در برخی موارد ممکن است اطلاعات ارسالی از طریق TLS رمزگذاری نشوند. در واقع آن‌ها از Cipher Suites Null استفاده می‌کنند که شامل هیچ رمزگذاری نیست. همچنین ممکن است در SSL از Anonymous Null Cipher استفاده شود و در زمان تبادل کلید، احراز هویت گواهی SSL صورت نگیرد. Anonymous Null Cipher نسبت به حمله مرد میانی آسیب‌پذیر می‌باشد و نباید از این دنباله رمز استفاده شود. خوشبختانه میزان استفاده از این دو دنباله رمز در دامنه‌های بررسی شده بسیار کم می‌باشد.

لایه SSL بر اساس سیاست تنظیمات Cipher List Order اولویت بین دنباله رمزهای خود را تعیین می‌کند. شما زمانیکه این تنظمیات را فعال می‌کنید می‌توانید ترتیب دلخواه زنجیره خود را اعمال کنید. در غیر این صورت، تنظیمات پیش‌فرض اعمال خواهد شد.

میزان تنظیم Cipher Order

Cipher order ها لیست دنباله‌هایی را که در لایه SSL استفاده می‌شود مشخص می‌کند. متاسفانه در ۴,۷۲۹ دامنه هیچ Cipher order یافت نشد.

وضعیت استفاده از CBC در پروتکل‌های SSLv3	
عدم تنظیم Cipher order	۴،۷۲۹
تنظیم Cipher order	۱۸،۶۳۸

جمع‌بندی

گواهی SSL ستون اصلی در امنیت وب است. در واقع این پروتکل از اطلاعات حساس ما در زمان انتقال در شبکه محافظت می‌کند. استفاده از SSL برای حفاظت از وبسایت‌ها ضروریست. حتی اگر اطلاعات حساسی مانند اطلاعات حساب‌های بانکی را منتقل نمی‌کنیم SSL اصالت‌سنجی وبسایت، حفاظت از حریم خصوصی و یکپارچگی داده‌های انتقالی وبسایت را فراهم می‌آورد. این در حالیست که در ایران بسیاری از وبسایت‌ها هنوز از پروتکل HTTP برای انتقال اطلاعات استفاده می کنند و تنها ۱۴٪ از وبسایت‌ها از HTTPS استفاده می‌کنند که بسیار کمتر از سطح جهانی می‌باشد.

استفاده از SSL به تنهایی نمی‌تواند تامین کننده امنیت باشد زیرا مانند هر تکنولوژی دیگری پیکربندی غلط این پروتکل‌ها یا آسیب‌پذیری‌های موجود در آن می‌تواند توسط نفوذگران مورد سواستفاده قرار گیرد. طی این بررسی مشخص شد آسیب‌پذیری وبسایت‌های کشور نسبت به حملات شناخته شده SSL در سطح بالایی است. هر چند سواستفاده از بیشتر این آسیب‌پذیری‌ها به سهولت امکان پذیر نیست. استفاده از الگوریتم‌های رمزگذاری ضعیف مانند CBC mode و RC4 باعث شده است تا ۶،۳۷۱ سایت دارای دنباله ضعف RC4 بوده و به ترتیب ۱۷،۷۶۶ و ۱۳،۶۵۵ وبسایت نسبت به حمله BEAST و SWEET32 آسیب‌پذیر باشند. همچنین استفاده از پروتکل‌های منسوخ شده SSLv3 و SSLv2 باعث شده است تا ۲،۹۵۵ وبسایت نسبت به حمله POODLE آسیب‌پذیر باشد.

دلیل اصلی این آسیب‌پذیری‌ها استفاده از پروتکل‌های ضعیف یا دنباله رمزهای نا کارآمد است که می‌توان با انجام تنظیمات ساده از وقوع بسیاری از این حملات جلوگیری کرد. در بیشتر وب‌سایت‌های مورد بررسی از پروتکل‌ها و دنباله‌های قوی نیز پشتیبانی شده اما از آنجاییکه دنباله‌ها و پروتکل‌های ضعیف نیز فعال هستند، مهاجمان با حملاتی نظیر Downgrond مرورگرها را وادار به برقراری ارتباط با پروتکل‌های ضعیف می‌کنند. برای انجام یک پیکربندی صحیح باید مواردی مختلفی در نظر گرفته شود که در سرویس دهنده‌های وب مختلف متفاوت است، اما رعایت برخی از قوانین کلی می‌تواند گام مهمی در افزایش امنیت وبسایت‌های کشور باشد، از جمله:

- غیر فعال‌سازی SSLv2 و SSLv3 برای جلوگیری از POODLE
- غیر فعال‌سازی TLS1.0 compression برای جلوگیری از CRIME
- غیر فعال‌سازی رمزهای ضعیف مانند: DES/3DES و RC4 و استفاده از رمزهای مدرن مانند AES ، modes (GCM)،ChaCha20 و پروتکل‌های TLS1.2
- بروز رسانی مرورگر به نسخه نهایی و استفاده از دنباله رمز TLS_FALLBACK_SCSV در صورت نیاز
- بروزرسانی نسخه OpenSSl و در صورت که ممکن نباشد کامپایل مجدد آن با OPENSSL_NO_HEARTBEATS