Namatek
True Education

Secure Sockets Layer

www.namatek.com

SSL چیست؟

فهرست مطالب

www.namatek.com

این روزها تعداد سایت ها و کسب و کارهای اینترنتی هر لحظه بیشتر و بیشتر می شود و ممکن است به علت تازه کار بودن سایت ها امن بودن آن ها قابل تشخیص نباشد و به همین دلیل تمامی کاربران اینترنت باید بدانند SSL چیست و نمایشگر چه سطحی از امنیت سایت است؟

با رونق گرفتن خریدها و پرداخت های آنلاین، امنیت اطلاعات کاربران به یکی از بزرگترین چالش ها برای کاربران و فروشگاه های آنلاین تبدیل شده و به همین دلیل روش های مختلفی برای رمزنگاری و حفظ امنیت اطلاعات ساخته شدند که پروتکل SSL یکی از موفق ترین آن ها است.

اگر شما هم علاقه دارید با این پروتکل، نحوه راه اندازی و مزایای استفاده از آن آشنا شوید، با ما همراه باشید.

پروتکل SSL چیست؟

اگر در زمان جستجو در مرورگرها دقت کرده باشید برخی از آدرس وب سایت هایی که به آن ها مراجعه می کنید، با http:// و برخی دیگر با https:// شروع می شوند. وب سایت هایی که نیاز به ارائه اطلاعات حساس مانند اطلاعات بانکی دارند، آدرسشان با https:// شروع می شود؛ زیرا طبق قانون می بایست ازhttps استفاده کنند.

اما این "s" در https از کجا آمده و به چه معناست؟

این "s" به معنای اتصال امن و رمزگذاری شده بین کاربران و آن سایت است؛ یعنی هر داده ای که وارد می شود در امنیت کامل با آن وب سایت به اشتراک گذاشته می شود.

به این فناوری SSL گفته می شود که مخفف **Secure Sockets Layer** است. https با استفاده از پروتکل SSL یک نماد قدرتمند برای اطمینان خاطر از حفظ رازداری یک وب سایت در تبادل اطلاعات است.

SSL چگونه امنیت اطلاعات را تضمین می‌کند؟

SSL یک فناوری امنیتی است. زمانی که در یک وب سایت فرمی را برای ارسال پر می کنید، اطلاعاتی که وارد می کنید می تواند توسط یک هکر در یک وب سایت ناامن رهگیری شود. یکی از رایج ترین روش ها برای رهگیری و دسترسی به اطلاعات کاربران شنود اطلاعات مبادله شده با سرور میزبان وب سایت، از طریق یک برنامه است. این برنامه در پس زمینه منتظر می ماند تا اطلاعات وارد شده توسط کاربر را ضبط کرده و به هکر ارسال کند. برای جلوگیری از این حملات تنها راه حفظ امنیت اطلاعات استفاده از SSLاست. در این حالت، زمانی که شما از یک وب سایت رمزگذاری شده

با SSL دیدن می کنید و مرورگر شما اقدام به ارتباط با سرور وب سایت می کند، اطلاعات توسط پروتکل SSL رمزگذاری می شود تا هیچکس غیر از شما و وب سایت نتواند به اطلاعات شما دسترسی پیدا کند.

گواهینامه SSL چیست؟

پروتکل SSL تنها توسط وب سایت هایی که دارای گواهی SSL هستند (گواهی TLS) قابل اجرا است. یک گواهی SSL مانند یک کارت شناسایی یا نشان است که ثابت می کند وب سایت همان چیزی است که نشان می دهد. گواهی های SSL توسط سرور وب سایت یا برنامه در وب ذخیره و نمایش داده می شوند.

انواع گواهینامه پروتکل SSL

اگر برای شما هم سوال است که گواهینامه SSL چیست باید بگوییم که سایت ها بر اساس میزان اعتبارسنجی و رمزگذاری ارائه شده یا تعداد دامنه ها یا زیر دامنه های تحت گواهی طبقه بندی می شوند.

چترهایی که گواهینامه های SSL تحت آن قرار می گیرند عبارتند از:

- **رمزگذاری (encryption)**
- **اعتبارسنجی (validation)**
- **شماره دامنه (domain number)**

هر کدام از موارد بالا دارای سه طبقه بندی هستند و می توان از آن ها در وب سایت ها استفاده کرد.

این گواهینامه ها توسط یک مرجع صدور گواهینامه Certificate Authority یا CA پردازش می شوند. این مرجع به طور خاص برای اجرا و اعطای این گواهینامه ها طراحی شده است.

انواع گواهینامه SSL بر اساس اعتبار سنجی سایت

انواع گواهینامه های SSL بر اساس اعتبارسنجی سایت که قابل دریافت هستند عبارت اند از:

- **Domain Validated (DV)**

همانطور که از اسم این گواهینامه پیداست فقط بر اساس تایید شدن ثبت دامنه جدید به یک سایت داده می شود و نظارتی بر روی ثبت سازمان و... ندارد. معمولا از این گواهی برای سایت های عمومی استفاده می شود.

- **Organization Validated (OV)**

در این مدل علاوه بر مورد تایید بودن دامنه سایت، سازمان متقاضی از لحاظ ثبت رسمی شرکت هم تایید می شود.

- **Extended Validation (EV)**

این نوع گواهینامه کامل ترین و در عین حال سخت ترین نوع گواهی قابل دریافت است.

با داشتن گواهینامه EV علاوه بر مورد تایید بودن سایت و ثبت رسمی شرکت، یک نوار سبز رنگ در مرور کاربران نمایش داده می شود که نام رسمی شرکت هم در آن ذکر شده است.

انواع گواهینامه SSL بر اساس شماره دامنه سایت

گواهینامه های SSL بر اساس تعداد دامنه های مورد استفاده نیز به سه دسته زیر تقسیم می شوند.

- **SSL Wildcard**

این نوع گواهی به شما اجازه می دهد علاوه بر دامنه اصلی هر تعداد دامنه فرعی دیگری که داشته باشید هم تحت پوشش SSL قرار بگیرد.
برای مثال دامنه اصلی سایت نماتک "namatek.com" است و یکی از دامنه های فرعی این سایت "forum.namatek.com" است.

- **Multi-Domain SSL Certificates (MDC)**

مورد استفاده برای ۲ تا ۱۰۰ دامنه که روی یک IP مشابه تنظیم شده اند.

- **Cases for Multi-Domain SSL Certificates (UCC)**

ترکیبی از گواهینامه MDC و EV است که تا ۱۰۰ دامنه را پوشش داده و نوار سبز رنگ نیز در مرورگر کاربران سایت نمایش داده می شود.

شرکت های صادر کننده گواهینامهSSL

در سراسر دنیا شرکت های بسیار متنوعی وجود دارند که امکان صادر کردن انواع گواهینامه های SSL را برای یک سایت دارند.

در ادامه تعدادی از این مراکز که نسبتا معروف تر و رایج تر هستند را معرفی می کنیم.

- **Certum:** بزرگترین و قدیمی ترین مرکز ارائه گواهینامه های SSL که در لهستان واقع شده و تمامی انواع گواهینامه ها را صادر می کند.
- **Digicert:** مجموعه ارائه خدمات اینترنتی و صادرکننده هر سه نوع گواهی EV ، OVو DV که در آمریکا قرار است.
- **Positive SSL:** گواهی صادر شده توسط شرکت Comodo که مناسب سایت های تازه کار و ابتدای شروع به طراحی وب سایت است.
- **GeoTrust:** یک مجموعه ارزان قیمت برای راه اندازی SSL که برای کسب و کارهای کوچیک مناسب است.

تفاوت TLS و SSL چیست؟

می توان گفت که SSL والد مستقیم پروتکل دیگری به نام TLS مخفف Transport Layer Security است.

در سال ۱۹۹۹، گروه مهندسی اینترنت IETF به روز رسانی SSL را پیشنهاد کرد. از آن جایی که این به روز رسانی توسط IETF انجام شد و شرکت Netscapeدیگر در آن مشارکت نداشت، نام SSL به TLS تغییر پیدا کرد.
تفاوت بین نسخه نهایی SSL 3.0 و نسخه اول TLS شدید نیست.
مشخص است که این تغییر نام برای نشان دادن تغییر در مالکیت اعمال شده است. این دو اصطلاح به دلیل شباهت زیاد SSL و TLS به یکدیگر، اغلب به جای یکدیگر استفاده می شوند و گاهی اشتباه گرفته می شوند. برخی هنوز از SSL برای اشاره به TLS استفاده می کنند، برخی دیگر نیز از اصطلاح رمزگذاری SSL/TLS استفاده می کنند؛ زیرا SSL نام بسیار شناخته شده ای است.

آیا SSL همچنان به روز و قابل استفاده است؟

SSL از زمان نسخه SSL 3.0 در سال ۱۹۹۶ به روز نشده است و اکنون منسوخ در نظر گرفته می شود.

علاوه بر این چندین آسیب پذیری در پروتکل SSL شناخته شده است و کارشناسان امنیتی توصیه می کنند استفاده از آن را متوقف کنید. اما دلیل خرید و فروش SSL چیست و با وجود عدم به روز رسانی و داشتن آسیب پذیری های متعدد، چرا همچنان ادامه دارد؟

در حقیقت، اکثر مرورگرهای وب مدرن دیگر به هیچ وجه از SSL پشتیبانی نمی کنند و TLS یک پروتکل رمزگذاری به روز است که در حال حاضر به صورت آنلاین اجرا می شود؛ اما بسیاری از مردم هنوز از آن به عنوان SSL یاد می کنند. این موضوع می تواند برای کسی که برای راه حل های امنیتی اقدام به خرید گواهینامه می کند، گیج کننده باشد.

حقیقت این است که تمام فروشندگان که این روزها "SSL" ارائه می دهند. در واقع نسخه TLS را ارائه خواهند داد که بیش از ۲۰ سال است جایگزین SSLشده است؛ اما از آن جا که بسیاری از افراد هنوز SSL را جستجو می کنند، این اصطلاح هنوز در بسیاری از صفحات محصول به طور برجسته نشان داده شده است.

مزایای پروتکل SSL چیست؟

- **SSL از داده های مشتری محافظت می کند.**

در این بازار رقابتی، داده های مشتری نظیر رمز عبور و اطلاعات بانکی برای سازمان ها مانند یک الماس است؛ بنابراین از گواهینامهSSL برای رمزگذاری و حفظ اطلاعات خصوصی استفاده می کنند. SSL با تبدیل آن ها به فرمت غیر قابل رمزگشایی به محافظت از داده ها در برابر هکرها و اسکیمرها کمک می کند.

- **SSL از مواجهه با هشدار Google Warning جلوگیری می کند.**

گوگل برای تبدیل اینترنت به مکانی امن تر اقدام به نمایش Google Warning برای سایت های رمزگذاری نشده (سایت هایHTTP) کرده است. داشتن گواهینامه SSL وب سایت شما را بهHTTPS تبدیل می کند و شما را از هشدارهای Google نجات می دهد.

- **SSL رتبه سئوی وب سایت را افزایش می دهد.**

گوگل دائما در حال به روز رسانی الگوریتم های SEO است. در سال ۲۰۱٤ گوگل HTTPS را به عنوان یکی از عوامل مؤثر بر رتبه بندی وب سایت ها اعلام کرد. علاوه بر این قرار دادن یک گواهی SSL در وب سایت باعث نمایش نشانگر اعتماد (Pad Lock) در نوار آدرس مرورگر کاربران و افزایش شاخص اعتماد و ترافیک ورودی به وب سایت شما می شود که رتبه سئوی شما را بهبود می دهد.

- **SSL از حملاتی نظیر فیشینگ و سایر حملات جلوگیری می کند.**

روش پیشگیری از حملات توسط SSL چیست؟ امروزه با افزایش تعداد کاربران در اینترنت، حملاتی مانند فیشینگ و MITM افزایش می یابد. از این رو ایمن سازی وب سایت ضروری است. یک راه ساده این است که گواهی SSL را در وب سایت خود داشته باشید. به عنوان مثال، از آنجا که حمله فیشینگ شامل شبیه سازی یک وب سایت یا یک صفحه وب است، تقریبا غیرممکن است که یک وب سایت غیرقانونی دارای مجوز SSL وجود داشته باشد؛ بنابراین شناسایی این حملات برای کاربران بسیار آسان است.

معایب پروتکل SSL چیست؟

- پروتکل SSL منقضی شده است و دارای آسیب پذیری های متعدد است؛ بنابراین بهتر است از TSL به جای آن استفاده شود.
- در مقایسه با سایر روش های رمزگذاری ایمن، تأخیر بیشتری را ارائه می دهد.
- خرید و راه اندازی گواهی SSL می تواند بسیار گران باشد.
- گواهی SSL پس از مدتی نیاز به تمدید دارد. اگر هر از گاهی تمدید نشود، پیامی ظاهر می شود که نشان می دهد گواهی SSL منقضی شده است. به این معنی که سایت دیگر ایمن نیست؛ بنابراین، مشتریان می توانند اعتماد خود را در انجام معاملات از دست بدهند.
- اگر گواهی SSL به درستی روی وب سایت اجرا نشود، فایل هایی که باید از طریق HTTPS اجرا شوند از طریق HTTP اجرا می شوند؛ بنابراین، یک پیام هشدار برای بازدیدکنندگان نمایش داده می شود که نشان می دهد اطلاعات آن ها محافظت نشده است.