SSL چیست؟

SSL مخفف عبارت Secure Sockets Layer است. اگر بخواهیم آن را به فارسی ترجمه کنیم می‌شود: لایه سوکت امن. این لایه امن بین مرورگر کاربر و سرور سایت برقرار می‌شود و از لو رفتن اطلاعات جلوگیری می‌کند.

SSL چگونه کار می‌کند؟

فرض کنید که داخل یک کافی‌شاپ به WIFI وصل شوید. اگر در این اتصال از پروتکل Http استفاده شده باشد و خبری از لایه امنیتی نباشد، هکرها می‌توانند با تلاش کمی اطلاعات شما را بدزدند.

در سایت هم، وقتی که از پروتکل Http استفاده می‌شود و خبری از گواهی SSL و لایه امنیتی نیست، هکرها می‌توانند خیلی راحت به اطلاعات کاربران دست پیدا کنند. چطور؟

به طور خیلی خلاصه، هکر یک برنامه کوچک را روی سرور یک وب سایت قرار می‌دهد. این برنامه به صورت پیوسته ارتباطات سرور را شنود می‌کند و منتظر می ماند بازدیدکننده اطلاعاتی را در وب سایت وارد کند. در همین زمان، برنامه هکر وارد عمل شده و خط به خط اطلاعات ورودی را شناسایی و ضبط می‌کند.

اما اگر از پروتکل Https در سایت استفاده شده باشد چه اتفاقی می‌افتد؟

در این حالت، حتی اگر هکرها اطلاعات را بدزدند، از آن سر درنمی‌آورند! چرا؟ چون این اطلاعات به لطف SSL در یک فایل رمزنگاری شده قرار گرفته‌اند و رمزگشایی از آنها کار سختی است!

همین‌جا یک پرانتز باز کنیم. ما یک گواهی مشابه SSL هم داریم که TLS نام دارد.

TLS مخفف Transport Layer Security و درست مثل SSL از پروتکل Https و یک لایه امنیتی، برای تبادل اطلاعات بین کاربر و وب سرور استفاده می‌کند.

تفاوت SSL و TLS در این است که TLS از الگوریتم های به روزتری برای رمزنگاری استفاده می‌کند. با توجه به این موضوع، به نظر می‌رسد که بهتر است از گواهی TLS استفاده کنیم؛ اما فراموش نکنید که برخی نسخه های مرورگرها هنوز از SSL پشتیبانی می‌کنند؛ به همین خاطر استفاده از گواهی SSL بیشتر رواج دارد!