مهندسین مشاور سازه پردازی ایران (سهامی خاص)

SAZEH PARDAZI IRAN
Consulting Eng. Co

تفاوت HTTP و HTTPS

HTTPچیست؟

- **HTTP**مخفف Hypertext Transfer Protocol است HTTP .مجموعه ای از قوانین و استانداردها را ارائه می دهد که نحوه انتقال هرگونه اطلاعات در شبکه جهانی وب را تعیین می کند HTTP .برای ارتباط با مرورگرها و سرورهای وب، قوانین استانداردی را ارائه می دهد.
- HTTPیک پروتکل شبکه در لایه اپلیکیشن یا کاربرد است که در بالاترین لایه TCP قرار گرفته است HTTP .از متن ساختار یافته Hypertext استفاده می کند که پیوند منطقی بین گره های حاوی متن را برقرار می کند.
همچنین به عنوان "stateless protocol" شناخته می شود زیرا هر دستور بدون استفاده از مرجع فرمان قبلی اجرا می شود.

مزایای HTTP

- HTTPرا می توان با پروتکل دیگر در اینترنت یا سایر شبکه ها پیاده سازی کرد.
- صفحات HTTP در حافظه های رایانه ای و اینترنتی ذخیره می شوند، بنابراین به سرعت قابل دسترسی می باشند.
- بستر مستقل که امکان حمل و نقل متقابل پلتفرم را فراهم می کند.
- به پشتیبانی Runtime احتیاج ندارد.
- قابل استفاده از طریق فایروال ها و برنامه های جهانی است.
- ارتباط اتصال گرا نیست؛ بنابراین هیچ سرباری برای شبکه در ایجاد و نگهداری سشن و اطلاعات وجود ندارد.

محدودیت های HTTP

- حریم خصوصی وجود ندارد زیرا هر کسی می تواند محتوا را ببیند.
- یکپارچگی داده ها مسئله بزرگی است زیرا می توان محتوا را تغییر داد. به همین دلیل پروتکل HTTP یک روش ناامن است زیرا از هیچ روش رمزگذاری استفاده نمی شود.
- هنوز مشخص نیست که در مورد چه کسی صحبت می کنید. هرکسی که درخواست را رهگیری کند می تواند نام کاربری و رمز عبور را بدست آورد.

HTTPSچیست؟

- HTTPSمخفف عبارت Hyper Text Transfer Protocol Secure است. این نسخه بسیار پیشرفته و امنتر از HTTPاست. از پورت ۴۴۳ برای ارتباط داده استفاده می کند. این امکان را فراهم می کند که با رمزگذاری ارتباطات باSSL ، معاملات امن انجام شود. این ترکیبی از پروتکل SSL / TLS و HTTP است. یک سرور شبکه ایمن و رمزگذاری شده را ارائه می دهد.
- HTTPهمچنین به شما امکان ایجاد ارتباط رمزگذاری شده ایمن بین سرور و مرورگر را می دهد. با این کار امنیت هر دو طرف حفظ می شود و به شما کمک می کند تا از سرقت اطلاعات مهم محافظت کنید.
- در پروتکل HTTPS انتقال اطلاعاتSSL ، با کمک الگوریتم key-based encryption انجام می شود. این کلید به طور کلی ۴۰ یا ۱۲۸ بیت طول دارد.

مزایایHTTPS

در بیشتر موارد، سایت هایی که از طریق HTTPS در حال اجرا هستند یک تغییر مسیر یا ریدایرکت در آدرس خواهند داشت. بنابراین حتی اگر HTTP را تایپ کنید به یک اتصال امن به https:// هدایت می شود که اجازه می دهد کاربران معاملات تجارت الکترونیکی امن، مانند بانکداری آنلاین داشته باشند.

فناوری SSL از هر کاربر محافظت می کند و مطمئن می باشد.

سازمانی معتبر گواهی SSL را تأیید می کند. بنابراین هر گواهی SSL شامل اطلاعات منحصر به فرد و معتبر در مورد صاحب گواهی است.

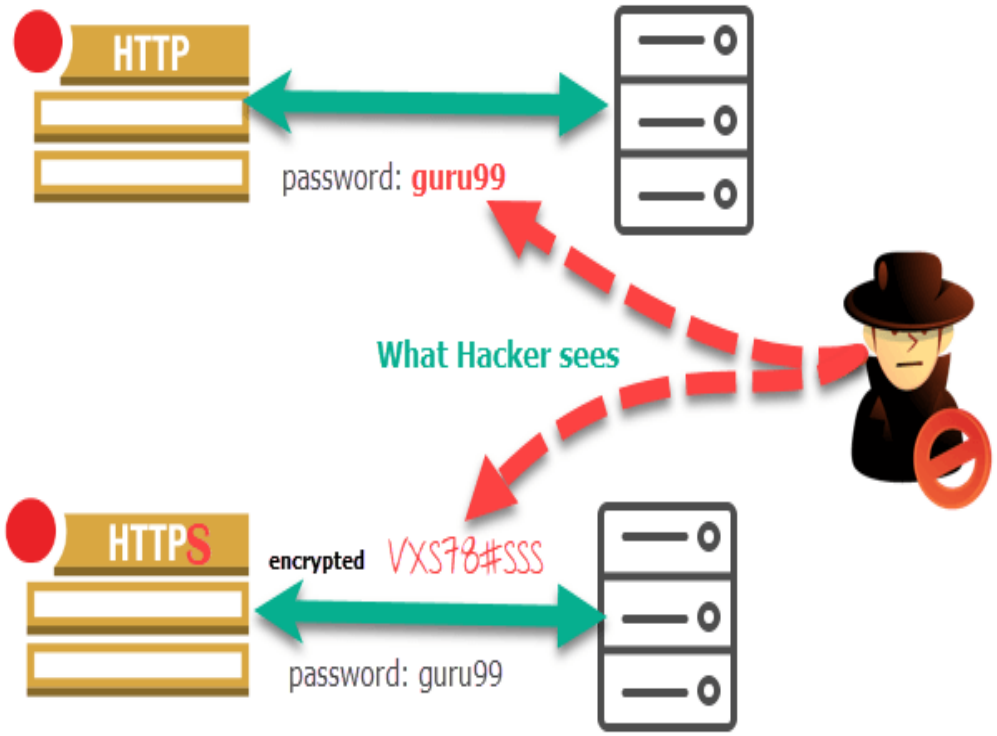
محدودیت هایHTTPS

پروتکل HTTPS نمی تواند جلوی سرقت اطلاعات محرمانه از صفحات ذخیره شده در مرورگر را بگیرد.

داده های SSL فقط هنگام انتقال بر روی شبکه رمزگذاری می شوند. بنابراین نمی تواند متن را در حافظه مرورگر پاک کند.

HTTPSمی تواند قدرت محاسباتی و قدرت شبکه از سازمان را افزایش دهد.

تفاوت بین HTTP وHTTPS



همانطور که اشاره شد، مهم ترین تفاوت HTTP و HTTPS در رمزنگاری داده ها و امنیت است.

پارامتر	HTTP	HTTPS
پروتکل	hypertext transfer protocol	hypertext transfer protocol with secure
امنیت	از امنیت کمتری برخوردار است زیرا داده ها می توانند در برابر هکرها آسیب پذیر باشند.	برای جلوگیری از دسترسی هکرها به اطلاعات مهم طراحی شده است. در برابر چنین حملاتی ایمن است.
پورت	به صورت پیش فرض از پرت ۸۰ استفاده می کند.	به صورت پیش فرض از پرت ۴۴۳ استفاده می کند.
شروع با	HTTP://	HTTPS://
کاربرد	بیشتر برای وبلاگ ها مورد استفاده قرار می گیرد.	اگر وب سایت نیاز به جمع آوری اطلاعات خصوصی مانند شماره کارت اعتباری داشته باشد، پروتکل مطمئن تری است
اسکرمبلینگ	HTTPداده های منتقل شده را تبدیل به رمزنگاری نمی کند. به همین دلیل احتمال بیشتری وجود دارد که اطلاعات انتقال یافته در اختیار هکرها باشد.	HTTPSقبل از انتقال، داده ها را رمز و تبدیل به حروف بی معنی می کند در انتها گیرنده، داده ها را با استفاده از کلید، رمزگشایی کرده و بنابراین، اطلاعات منتقل شده امن است که نمی تواند هک شود.
پروتکل	در سطح TCP / IP عمل می کند.	HTTPSهیچ پروتکل جداگانه ای ندارد. با استفاده از HTTP عمل می کند اما از اتصال SSL / TLS رمزگذاری شده استفاده می کند.
اعتباردامنه	وب سایت HTTP نیازی به SSL ندارد	HTTPSبه گواهی SSL نیاز دارد.
رمزگذاری داده ها	وب سایت HTTP از رمزگذاری استفاده نمی کند.	وب سایت های HTTPS از رمزگذاری داده استفاده می کنند.
رده بندی جست وجو	HTTPرتبه بندی جستجو را بهبود نمی بخشد.	HTTPSبه بهبود رتبه جستجو کمک می کند.
سرعت	سریع	اهسته تر ازHTTP
آسیب پذیری	در برابر هکر ها اسیب پذیر است.	بسیار امن است زیرا داده ها رمز گذاری می شوند.

انواع گواهینامه SSL و TLS استفاده شده باHTTPS

- **اعتبارسنجی دامنه :**اعتبارسنجی دامنه تأیید می کند که شخصی که متقاضی صدور گواهینامه است صاحب نام دامنه است. این نوع اعتبارسنجی معمولاً چند دقیقه تا چند ساعت طول می کشد.
- **اعتبار سنجی سازمان :**سازمان صدور گواهینامه نه تنها مالکیت دامنه را تأیید می کند بلکه صاحبان آن را نیز شناسایی می کند. این بدان معناست که از یک مالک خواسته می شود تا سند اثبات شناسنامه شخصی را برای اثبات هویت خود ارائه دهد.
- **اعتبار سنجی تمدید :**اعتبار سنجی گسترده بالاترین سطح اعتبارسنجی است. این شامل اعتبار مالکیت دامنه، هویت مالک و همچنین اثبات ثبت نام کسب و کار است.

SSL/TLS

تفاوت های کلیدی HTTP وHTTPS

- HTTPفاقد مکانیزم امنیتی برای رمزگذاری داده ها است، در حالی که HTTPS برای تأمین امنیت ارتباط بین سرور و مشتری ایجاد شده است، SSLیا TLS گواهی دیجیتال را فراهم می کند.
- HTTPدر Application Layer عمل می کند در حالی که HTTPS در Transport Layer فعالیت می کند.
- HTTPبه طور پیش فرض روی پورت ۸۰ کار می کند در حالی که HTTPS بصورت پیش فرض در پورت ۴۴۳ کار می کند.
- HTTPداده ها را با متن ساده انتقال می دهد در حالی که HTTPS داده ها را با متن رمزگذاری شده انتقال می دهد.
- HTTPنسبت به HTTPS سریع است زیرا HTTPS برای محاسبه رمز کانال ارتباطی از قدرت محاسباتی استفاده می کند.

برخی از مرورگرها دیگر صفحات http را باز نمی کنند و اخطاری مانند تصویر زیر را به شما نشان می دهند . در این صورت با انتخاب لینک Proceed to می توان به صفحه مورد نظر دسترسی داشت.