

آشنایی با پروتکل HTTPS و مراحل دریافت گواهینامه SSL

شاید اطلاعاتی در خصوص SSL داشته باشید ولی من هم یک توضیح اجمالی خدمتون میدم و میریم سراغ بحث اصلی مون یعنی نحوه نصب و کانفیگ SSL بر روی دامنه در Cpanel که یکی از بحث های داغ امروز وبمستران هست.

تعریف SSL :

نمیخواهم منم مثل سایت های دیگه از اصطلاحات تخصصی حرف بزنم و خیلی کوتاه عرض میکنم که وقتی شما وبسایتی دارید که قرار هست یکسری اطلاعات برای مرورگر کاربر ارسال کنه و در قالب صفحات HTML به کاربر نشون بده و از طرفی هم قراره که یکسری اطلاعات رو از کاربر بگیره و در سمت سرور عملیات و یا پردازش هایی رو بر روی اونها انجام بده

در حالت معمولی صاحبان اکثر وبسایت ها برای ارتباط مرورگر کاربر با سرورشون از پروتکل HTTP بدلیل رایگان بودن استفاده میکنند که بصورت پیشفرض بر روی وبسریس ها کانفیگ شده است ولی این پروتکل هیچگونه رمزنگاری روی اطلاعات رد و بدل شده بین مرورگر و سرور شما رو انجام نمیده و اطلاعات به همان شکل اصلی ارسال و دریافت میشه که این مدل از ارتباط ناامن هست .

شاید بپرسید اصلا پروتکل چیه ؟ خوب در جواب باید بگم پروتکل یعنی پیمان و قرارداد و یه کلمه انگلیسی هست که نیاز نیست شما ازش بترسید.

در دنیای بین آدمای یکسری قانون ها توسط خود آدمای وضع شده، مثلا این یک قانون هست که وقتی دو تا آدم به هم میرسن ابتدا باید به همدیگه سلام بدن و بعد احوالپرسی و بعد هم صحبت های دیگه و مثلا قانون دیگه آدمها اینه که وقتی یک شخص فقیر در مقابل یک شخص پولدار قرار گرفت ابتدا باید دستهایش را بر روی سینه اش قرار دهد و به او در بهترین حالت احترام بگذارد

خوب این ها قراردادهایی هستند که حداقل بشر امروزی به آن پایبند هست.

در دنیای کامپیوتر هم وقتی دوتا کامپیوتر میخوان با هم ارتباط برقرار کنن باید با یک قرارداد نامه ای این کار رو انجام بدن که عمومی ترین این قرارداد ها HTTP هست .

پس هرگاه شما در آدرس بار مرورگرتون این قرارداد رو ذکر کردین و در ادامه اش آدرس یک وبسایت رو تایپ کردین ، دارین به یک کامپیوتری که میزبان اون سایت هست میگین که من میخوام با قرارداد HTTP باهات ارتباط داشته باشم و خودشم میخوام این سایتی که برات فرستادمو برام بفرستی

سرور هم در جواب میگه موردی نیست و من در خدمتتم و برمیگرده سایت رو در قالب همون قوانین HTTP براش برمیگردونه ، حالا اینکه دقیقا در این نوع ارتباط چه مکانیزم هایی بین دوتا کامپیوتر اتفاق میفته رو میزاریم کنار و انشالله هرکی دوست داشت میتونه در زمینه های شبکه و اینترنت مطالعه کنه بفهمه که چه

اتفاقاتی میفته ولی در این مقاله من فقط به یک تفاوت این دوتا پروتکل میپردازم و اونم اینه که در پروتکل HTTPS اطلاعات قبل از ارسال رمز میشن و ارسال میشن و حالا هر دو کامپیوتر از نوع رمزنگاری همدیگه مطلع هستن و میتونن اطلاعات دریافتی رو به اصطلاح دیکد کنن و به داده های اصلی برسن

البته شاید براتون سوال بشه که چه لزومی داره اطلاعات قبل از ارسال رمزنگاری بشن ، در پاسخ باید بگم که تصور کنید کاربر شما در مرورگر خودش آدرس وبسایت شمارو تایپ میکنه و با متد GET یا POST یا هر متد دیگه ای اطلاعات لاگین خودش رو هم برای ورود به داشبورد خودش به سرور ارسال میکنه ، خوب این درخواست به همراه اطلاعات حساس کاربر از بستر شبکه به سرور ارسال میشه ، خوب این بستر کجاست ؟ معلومه از خونه شما تا سرور ، پس هر کسی که در این مسیر ارتباط قرار داشته باشه میتونه با یکسری نرم افزارهای شبکه مثل Traffic Listener داده های ارسالی کاربران سایت شما رو ببینه و به اصطلاح شنود کنه ، پس اگه این اطلاعات رمزنگاری نشن ، افراد سود جو خیلی راحت میتونن اطلاعات اکانت یا حساب های کاربری سایت شمارو بدست بیارن و با اطلاعات اونا وارد سایت شما بشن و از حساب اونا استفاده کنن ، اینجاست که پروتکل HTTPS به داد ما میرسه و اگه وبسایتی رو با این پروتکل صدا بزنین مرورگر اطلاعات ارسالی به سایت رو خودش رمز میکنه و میفرسته براش که حتی اگه ISP شما یا هر کسی که بخواد ترافیک سایت شمارو شنود کنه با اطلاعاتی کدشده مواجه میشه و براش ارزشی نداره

نگران هیچ چیز نباشید قرار نیست همه این هایی که توضیح دادمو شما انجام بدید، اینارو خود کامپیوترها با نرم افزارهای خاصی که دارن انجام میدن و توضیحات رو صرفا به خاطر آگاهی شما دادم

پس کافیه شما فقط یاد بگیرین که چطور باید این پروتکل رو فعال کنید.

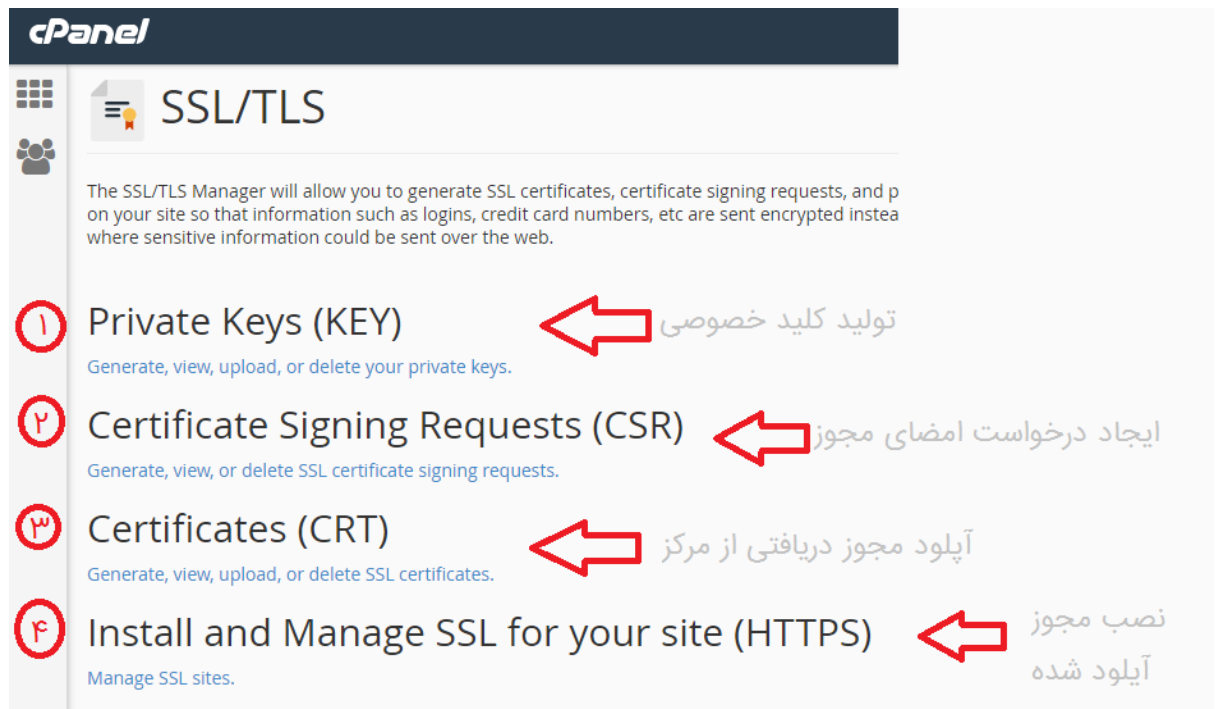
راه اندازی پروتکل HTTPS بر روی سرور :

برای راه اندازی ابتدا شما باید از یک مرکز معتبری که گواهینامه های SSL رو صادر میکنند ، یک گواهینامه دیجیتالی دریافت کنید که خیلی راحت و شما معمولا این گواهینامه ها با ثبت نام در سایتشون براحتی دریافت میکنید و بصورت لحظه ای هم هستن و از شما اطلاعات دامنه و سرورتون رو میگیرن و برای شما بصورت آنلاین سرتیفیکیت صادر میکنن که یا در قالب یکسری فایل های با پسوند crt. در اختیارتون قرار میدن یا در قالب یکسری نوشتار که در هردو حالت شما باید اینها رو در سی پنل هاست خودتون آپلود کنید و نصب کنید .

اما نکته ای که وجود داره اینه که قبل از اینکه شما به وبسایت این عزیزان مراجعه کنید و ازشون گواهینامه SSL بخرید ، ابتدا وارد سی پنل هاست خودتون بشید و در بخش SECURITY سی پنل بدنال گزینه SSL/TLS بگردید و این بخش رو باز کنید .

پس هنوز هیچ اقدامی انجام ندادیم و فقط وارد این بخش شدیم.

در این صفحه شما با چند گزینه مواجه میشد



طبق تصویر بالا شما برای راه اندازی SSL بر روی دامنه خودتون ۴ مرحله رو انجام خواهید داد.

مرحله اول همونطور که در عکس بالا شماره گذاری کردم ، مرحله تولید کلید خصوصی هست که قبل از هر اقدامی باید این کلین منحصر بفرد را از طریق این بخش ایجاد کنید.

مرحله دوم ایجاد درخواست گواهینامه جهت ارائه به مرکز برای شناسایی وبسایت شما میباشد . در این قسمت از شما کلید خصوصی که ساختین رو میخواند و یکسری اطلاعات هویتی از شما میخواند که باید مثل یک فرم پر کنید و کلید ایجاد رو در پائین بزنید تا درخواست ایجاد شود.

دقت کنید تا اینجای کار شما هیچ اقدامی خارج از وبسرور خودتون انجام ندادید.

خوب حالا دو مرحله بعدی طبق تصویر بالا بایستی بعد از اخذ مجوز از مرکز صادر کنند گواهینامه SSL تنظیم شود . پس میریم سراغ یکی از این مراکز که خودتون میتونید جستجو کنید ولی دقت کنید که به عنوان یک مرکز معتبر شمرده شود (بخصوص از دید گوگل) پس انتخاب مراکز صادر کننده رو به عهده خودتون میزارم .

برای انجام اینکار وارد وبسایت شون میشد و معمولا از شما درخواست میکنن که در سایتشون عضو بشید و همون کدهای ایجاد شده در مرحله دوم را از شما میخوان (این کدها حاوی تمامی مشخصات دامنه شما و وبسایت شماست که با یک الگوریتمی انکد شده)

پس نام دامنه ای رو قصد دارید گواهینامه براش صادر بشه رو وارد میکنید و همین اطلاعات کدشده ای که هاست خودتون در مرحله دوم براتون ایجاد کرد رو هم وارد میکنید و دکمه صدور رو میزنید تا مجوز شما صادر بشه که اگه مشکلی نبود مجوز ایجاد میشه

بهتون تبریک میگم شما الان دارای مجوز SSL برای دامنه خودتون شدید. البته همون لحظه و آنلاین این اتفاق می افته و یکسری نوشتار کد شده به شما تحویل میدن که همون مجوز شماست و یا یک فایل با پسوند crt. بهتون میدن و یا هر دو رو که بستگی به خودتون داره که کدوم رو دریافت کنید . البته معمولا توی داشبورد شما قرار میگیره و هر موقع خواستید دانلود کنید میرین توی همون سایت صادر کننده و دانلود می کنید.

امیدوارم تا اینجای کار متوجه همه چیز شده باشید.

الان نوبت دو مرحله آخر هست که باید بریم سراغ سی پنل خودمون و اون دو بخش رو هم تکمیل کنیم

در مرحله سوم باید همین مجوزی که دریافت کردیم رو آپلود کنیم

در مرحله ۴ که مرحله آخر کار هست باید مجوز آپلود شده رو نصب کنیم

در این مرحله سی پنل از شما اطلاعات کلید خصوصی + اطلاعات درخواست خودتون + اطلاعات مجوز صادر شده رو میخواد و وقتی این ۳ تا مورد رو براش مشخص کردید یه دکمه در پایین داره که نوشته install certificate که با زدن اون ، مجوز شروع به نصب بر روی سرور شما میکنه

بعد نصب موفقیت آمیز ، پروتکل HTTPS برای شما قابل استفاده مییاشد و حالا میتونید با این پروتکل وبسایت خودتون رو باز کنید .

موفق و موید باشید

ارادتمند شما مهدی حسامی

وبلاگ من : phpkar.blog.ir

شماره من : ۰۹۱۹۲۴۲۱۸۶۵