

در بخش اول از این سری مقالات در خصوص اهمیت امنیت مرورگرهای وب و تعدادی مسائل مربوط به امنیت که در تمام یا بخشی از مرورگرهای معروف رایج هستند، توضیحاتی ارائه شد. در بخش دوم به مکانیزم های امنیتی و نحوه پیاده سازی و پیکربندی مرورگر IE پرداخته شد. در بخش سوم بهترین پیکربندی امنیتی برای مرورگر IE مایکروسافت مورد بررسی قرار گرفت. در بخش های ۴ و ۵ در خصوص مکانیزم های امنیتی گوگل کروم و بهترین پیکربندی امنیتی آن توضیحاتی داده شد. در این بخش قصد داریم تا به مکانیزم های امنیتی مرورگر موزیلا فایرفاکس بپردازیم.

امنیت فایرفاکس

با توجه به اطلاعات آماری موجود مرورگر فایرفاکس هم چنان به عنوان یکی از محبوب ترین مرورگرها به حساب می آید. در حال حاضر برای کاربران این مرورگر نحوه اعمال تنظیمات امنیتی و استفاده از ویژگی های خاص مرورگر مهم می باشد. در ابتدا به مکانیزم های امنیتی آخرین نسخه از فایرفاکس نگاهی می اندازیم. این مکانیزم ها شامل مکانیزم های حفاظتی می باشد که در بخش های قبل برای مرورگرهای کروم و IE پرداخته شد. در این مرورگر مکانیزم ها ضد بدافزار و ضد سرقت هویتی وجود دارد که به عنوان یک استاندارد در تمامی مرورگرها به کار می رود و گزینه به روز رسانی خودکار به طور پیش فرض فعال می باشد. هم چنین مرورگر فایرفاکس شامل یک خط مشی امنیت محتوی (CSP) می باشد که در برابر حملات اسکرپت بین سایتی محافظت می نماید و این کار را از طریق پیکربندی دامنه های خاص انجام می دهد و می توان مشخص کرد که کدام اسکرپت ها امن بوده و می توانند اجرا شوند. مابقی اسکرپت ها غیرقابل اجرا می باشند. می توانید اطلاعات بیشتر در خصوص این ویژگی را از وب سایت Mozilla Developer Network دریافت نمایید.

ویژگی Instant Website ID

ویژگی که موزیلا نام آن را "Instant Website ID" نهاده است برای هشدار به کاربر در خصوص وب سایت های مشکوک یا برای شناسایی سایت های رمزگذاری شده با SSL از آیکون های رنگی استفاده می کند. آیکون های شناسایی سایت که در سمت چپ آدرس URL در نوار ابزار می توان مشاهده کرد، در زیر توضیح داده می شوند:

(آیکون خاکستری جهان): این آیکون بدان معناست که وب سایت رمزگذاری نشده است. هیچ اطلاعات شناسایی از جمله گواهینامه برای این سایت وجود ندارد. می توان این آیکون را در بسیاری از سایت های HTTP مشاهده کرد.

(آیکون محافظ): زمانیکه شما وب سایتی را مشاهده می کنید که آیکون محافظ برای آن به نمایش در می آید در واقع پیامی است مبنی بر آنکه فایرفاکس محتوایی که امن نمی باشد را مسدود کرده است اما شما می توانید با کلیک بر روی آن به سایت اجازه دهید تا به نمایش درآید یا از دیدن آن منصرف شوید. اگر شما تصمیم بگیرید که محتوی سایت را مشاهده کنید می توانید با انتخاب Disable Protection در باکس سمت چپ این صفحه این کار را انجام داده و پس از آن آیکون محافظ به آیکون زیر تغییر می یابد.

(آیکون مثلث نارنجی با علامت تعجب): این آیکون یک پیام هشدار است. این آیکون در مورد سایت های HTTPS ای نشان داده می شود که از محتوی ترکیبی (امن و نامن) استفاده می کنند و هشدار می دهد در حالیکه آدرس URL به شما HTTPS را نشان می دهد اما قسمتی از محتوی این سایت به صورت HTTP منتقل می شود و می تواند توسط مهاجمان خوانده شده و یا تغییر کند.

(آیکون قفل خاکستری): این آیکون برای مشخص کردن سایت های HTTPS نمایش داده می شود در نتیجه نشان می دهد که سایت مورد نظر دارای گواهینامه دیجیتالی معتبر SSL است که توسط مرکز صدور گواهینامه (CA) مانند Verisign یا Thawte منتشر شده است. هم چنین بدان معناست که تراکنش های به سایت یا از سایت با پروتکل SSL رمزگذاری می شود. البته باید توجه داشت که هویت دارنده گواهینامه در این آیکون صد در صد تضمین نمی شود. هر کسی می تواند یک گواهینامه را خریداری کرده و ادعا کند که از طرف شخص یا شرکت خاصی است.

(آیکون قفل سبز): این آیکون برای سایت های HTTPS ای به نمایش در می آید که یک گواهینامه EV معتبر دارند. بدان معنا که نه تنها تراکنش ها رمزگذاری می شود بلکه هویت دارنده گواهینامه نیز برای CA مشخص می باشد. این آیکون با سبز شدن کل نوار آدرس URL در IE هم ارز می باشد.

در قسمت دوم این مقاله تنظیم ویژگی های امنیتی فایرفاکس و قابلیت های حریم خصوصی توضیح داده می شود.