ویژگی‌هایی که فقط در سایت‌های مطمئن قابل استفاده هستند

موزیلا ارتباطات کاربران را امن‌تر خواهد کرد

همه کاربران اینترنت متقاعد شده‌اند که HTTPS یک گام رو به جلو و یک ضرورت به شمار می‌رود. در ماه‌های اخیر، دستورالعمل‌های زیادی از طرف مؤسسه‌های IAB، IETF و W3C به سراسر جهان مخابره شده است که از رمزنگاری روی برنامه‌های اینترنتی خود استفاده کنند که درباره وب به معنای به‌کارگیری HTTPS است. بعد از آن‌که یک تبادل نظر جدی توسط موزیلا با طرف‌های مخاطب این شرکت رد و بدل شد، این شرکت تصمیم گرفت روی اجرای یک توسعه جدید تمرکز کند که در نهایت به ایجاد وب ایمن تبدیل خواهد شد.

بر همین اساس، این شرکت تصمیم گرفت یک‌سری ویژگی‌ها را از سایت‌های ناامن حذف کند. موزیلا در نظر دارد تا به‌تدریج ارتباطات HTTPS را روی ارتباطات ناامن HTTP اجرا کند. برای این منظور، این شرکت در حال ساخت ویژگی‌های جدیدی برای مرورگر خود است. ویژگی‌هایی که فقط روی سایت‌های امن در دسترس خواهند بود. ریچارد بارنس، مدیر گروه امنیتی موزیلا، در همین رابطه در یادداشتی نوشت: «سازنده مرورگر فایرفاکس در نظر دارد بعد از گفت‌وگوها تاریخی را برای عرضه همه ویژگی‌های جدید اعلام کند که فقط برای سایت‌های ایمن در دسترس خواهند بود.» بر همین اساس، دو مرحله اصلی در این برنامه‌ریزی وجود دارند:

1- تنظیم زمان مشخص بعد از آن‌که همه ویژگی‌های جدید فقط برای سایت‌های ایمن در دسترس خواهند بود.
2- به‌تدریج از دور خارج کردن دسترسی به ویژگی‌های مرورگر برای سایت‌های غیرایمن به‌ویژه قابلیت‌هایی که امنیت کاربران را به مخاطره می‌اندازند.

درباره مرحله نخست باید بدانیم تعریف ویژگی جدید چیست؟ به‌طور مثال، یک تعریف از جدید بودن می‌تواند به چیزهایی شبیه به CSS و دیگر ویژگی‌های رندرینگ اجازه دهد همچنان روی سایت‌های ناامن مورد استفاده قرار گیرد، در حالی که یک صفحه برای رسم خود می‌تواند از روش خاص خود با استفاده از <canvas> اقدام کند. این ویژگی می‌تواند محدودیت‌هایی از قبیل دسترسی به ویژگی‌های سخت‌افزاری جدید را به همراه داشته باشد. عنصر دوم در این برنامه‌ریزی به مناسبات تجاری بین امنیت و سازگاری وب مربوط می‌شود.
حذف ویژگی‌ها از سایت‌های ناامن ممکن است روند کاری این سایت‌ها را با مشکل همراه سازد. همچنین، یک‌سری پیشنهادهایی در ارتباط با محدود ساختن کوکی‌ها روی سایت‌های ناامن ارائه شده‌اند. البته لازم به توضیح است، این برنامه هنوز هم استفاده از اسکیمای URI در محتوای موروثی را امکان‌پذیر می‌سازد.
با HSTS (سرنام HTTP Strict Transport Security) و به‌روزرسانی درخواست‌های ناامن در خصلت CSP، اسکیمای HTTP به‌طور خودکار توانایی انتقال به HTTPS را به مرورگر خواهد داد، به طوری که به‌صورت امن اجرا شود. این شرکت همچنین در نظر دارد تا به‌تدریج مرحله از دسترس خارج کردن ویژگی‌ها برای سایت‌های ناامن را

آغاز کند. به‌ویژه قابلیت‌هایی که مخاطرات امنیتی به همراه داشتند و حریم خصوصی کاربران را به خطر می‌اندازند.
بارن در ادامه افزود: «گروه کاری ما هنوز درباره این‌که چه ویژگی‌های جدیدی در سایت‌های غیرایمن بلوکه خواهند شد به توافق نرسیده است. به‌طور مثال، کاربران فایرفاکس هنوز هم توانایی مشاهده سایت‌های غیرایمن را دارند. اما این سایت‌ها به ویژگی‌های جدید از قبیل دستیابی به ویژگی‌های جدید سخت‌افزاری دسترسی نخواهند داشت. حذف ویژگی‌ها از سایت‌های ناامن به احتمال زیاد باعث خواهد شد بعضی سایت‌ها دچار مشکل شوند. بنابراین، ما در حال بررسی و نظارت بر میزان این درست کار نکردن و به تعادل رساندن آن با مزیت‌های امنیتی هستیم.»
بارنس همچنین در ادامه افزود: «موزیلا در حال اضافه کردن و بررسی محدودیت‌های بیش‌تری است که پیش روی سایت‌های نا امن قرار دارد تا تعادل مناسبی را در این زمینه برقرار کند. در حال حاضر، فایرفاکس از مدت‌ها قبل اقدام به بلوکه کردن برخی از این ویژگی‌ها کرده است. به‌طور مثال، ارائه مجوز پایدار به سایت‌های غیرایمن برای دستیابی به دوربین و تلفن همراه نمونه‌ای از این موارد به شمار می‌رود.»
راهبرد جدید موزیلا در ارتباط با بحث امنیت با رمزنگاری فرصت‌طلبانه آغاز شد که ماه گذشته آن را معرفی کرد. در این فناوری رمزنگاری روی محتوایی انجام می‌شود که در حالت عادی به‌صورت غیررمزنگاری شده قرار دارد. این فناوری کاربر را در برابر حمله man-in-the-middle امن نمی‌سازد، اما در برابر مشکلات استراق سمع کمک‌های فراوانی می‌کند. کارشناسان امنیتی به‌طور گسترده از این ویژگی استقبال کردند.

تاریخ انتشار:

25 خرداد 1394

نشانی منبع: https://www.shabakeh-mag.com/security/852