امنیت به زبان ساده: حمله «سرقت کوکی» یا «سرقت نشست» چگونه انجام می‌شود؟ - دیجیاتو

شایان ضیایی | جمعه، ۱۵ اسفند ۱۳۹۹

حمله سرقت نشست (Session Hijacking) که تحت عنوان حمله سرقت کوکی نیز شناخته می‌شود، زمانی اتفاق می‌افتد که نشست شما درون یک وب‌سایت توسط مهاجم ربوده می‌شود. هنگامی که شما درون یک سرویس لاگین می‌کنید، یک نشست ایجاد می‌شود، مثلا زمانی که وارد اپلیکیشن بانکداری می‌شوید. و وقتی هم از آن بیرون می‌آیید، نشست به پایان می‌رسد. این دست از حملات به دانش مهاجم راجع به کوکی نشست شما متکی هستند و به همین خاطر سرقت کوکی هم نامیده می‌شوند. اگرچه هر نشستی در کامپیوتر را به می‌توان به سرقت برد، سرقت نشست معمولا در مرورگر و وب اپلیکیشن‌ها اتفاق می‌افتد.

در اکثر مواقعی که شما وارد یک وب اپلیکیشن می‌شوید، سرور یک کوکی نشست موقت درون مرورگرتان قرار می‌دهد تا یادش بماند که شما وارد سرویس شده‌اید و هویت‌تان نیز احراز شده. HTTP پروتکلی بدون حالت است و اتصال کوکی‌ها به هدر HTTP، یکی از محبوب‌ترین روش‌های شناسایی مرورگر یا نشست فعلی شما از سوی سرور به حساب می‌آید.

برای سرقت نشست، مهاجم باید آی‌دی نشست (یا کلید نشست) قربانی را بداند. این کار یا از طریق سرقت کوکی نشست انجام می‌شود یا ترغیب کاربر به کلیک روی لینکی آلوده که شامل یک آی‌دی نشست از پیش آماده خواهد بود. در هر دو مورد، بعد از اینکه کاربر توسط سرور احراز هویت می‌شود، هکر می‌تواند با استفاده از همان آی‌دی، برای سرقت نشست و اجرای آن در نشست مروگر خودش استفاده کند.

هکرها بعد از سرقت موفقیت‌آمیز نشست چه می‌کنند؟

اگر مهاجم موفق باشد، قادر به انجام هر کاری خواهد بود که کاربر اصلی در جریان نشست فعال خود قادر به انجام‌شان بوده است. بسته به اپلیکیشن هدف، چنین چیزی می‌تواند به معنای انتقال پول از حساب بانکی قربانی، جعل هویت قربانی برای خرید از فروشگاه‌ها، دسترسی به اطلاعات شخصی برای جعل هویت، سرقت اطلاعات شخصی کاربر از سیستم‌های یک کمپانی، رمزنگاری اطلاعات ارزشمند و درخواست باج برای رمزگشایی آن‌ها و چیزهایی از این دست باشد.

یک خطر برجسته برای سازمان‌های بزرگ اینست که از کوکی‌ها برای شناسایی کاربران احراز هویت شده روی سیستم‌های شناسایی یگانه نیز استفاده می‌شود. این یعنی یک سرقت نشست موفقیت‌آمیز در چنین سیستم‌هایی به مهاجم اجازه خواهد داد که به وب اپلیکیشن‌های متعددی دسترسی بیابد، از سیستم‌های مالی گرفته تا سیستم‌های حاوی سوابق مشتری و همه این‌ها می‌توانند شامل اطلاعات بسیار ارزشمند باشند.

هر کاربر نیز هنگام استفاده از سرویس‌های خارجی برای لاگین درون اپلیکیشن‌ها با خطراتی مشابه مواجه شده است، اما به خاطر تدابیر امنیتی موجود هنگام لاگین با اکانت‌های فیسبوک یا گوگل، سرقت کوکی نشست برای سرقت خود نشست کافی نخواهد بود.

تفاوت میان سرقت نشست و جعل نشست چیست؟

اگرچه هر دو ترفند شدیدا به یکدیگر شباهت دارند، اما تفاوت میان جعل و سرقت نشست در زمان‌بندی حمله ظاهر می‌شود. همانطور که از نامش پیداست، سرقت نشست به حمله به کاربری اشاره می‌کند که هم‌اکنون لاگین کرده و احراز هویت کرده. بنابراین از نقطه نگاه قربانی، حمله معمولا به کرش کردن اپلیکیشن هدف یا رفتارهای عجیب از سوی آن منجر می‌شود. هنگام جعل نشست، مهاجم از اطلاعات ربوده شده برای ایجاد یک نشست جدید و جعل هویت کاربر اصلی (که شاید اصلا از حمله باخبر نباشد) استفاده می‌کند.

متدهای سرقت نشست چیست؟

هکرها هنگام سرقت یک نشست، گزینه‌های زیادی پیش روی خود می‌بینند و این گزینه‌ها وابسته به وکتور حمله و جایگاه مهاجم هستند. اما رایج‌ترین نوع حمله، با تمرکز بر تداخل در کار کوکی‌ها انجام می‌شود:

اسکریپت‌نویسی بین سایتی (XSS): این احتمالا خطرناک‌ترین و رایج‌ترین متد سرقت نشست وب باشد. با اکسپلویت کردن آسیب‌پذیری‌های سرور یا اپلیکیشن، مهاجمان می‌توانند اسکریپت‌های سمت مشتری (معمولا جاوا اسکریپت) را درون وب پیج‌ها تزریق کنند و مرورگر هم به صورت خودسرانه کدها را به اجرا در می‌آورد. اگر کوکی‌های نشست از قابلیت HTTPOnly بهره‌مند نباشند، اسکریپت‌های تزریق شده می‌توانند به کلید نشست شما دسترسی یافته و اطلاعات لازم برای سرقت نشست را در اختیار هکرها قرار دهند.

برای مثال هکرها ممکن است در ایمیل‌ها یا پیام‌های شخصی گروهی، لینکی دست‌ساز را منتشر کنند که به یک سایت شناخته شده و قابل اعتماد منتهی می‌شود. اما این لینک می‌تواند شامل پارامترهای HTTP باشد که از یک آسیب‌پذیری برای تزریق کد اسکریپت استفاده می‌کند.

حمله طرف نشست (Session Side Jacking): این نوع از حمله نیازمند مشارکت فعال مهاجم است. با استفاده از تکنیک پکت اسنیفینگ (استراق سمع پکت‌های شبکه)، مهاجمین می‌توانند ترافیک شبکه کاربر را پایش و بعد از احراز هویت کاربر در سرور، در کار کوکی‌ها تداخل ایجاد کنند. اگر وب‌سایت تنها از رمزنگاری SSL و TLS صرفا برای صفحات لاگین استفاده کرده باشد و نه تمام نشست، مهاجم می‌تواند از کلید نشست اسنیف شده برای سرقت نشست استفاده کند. از آن‌جایی که هکرها در این متد به شبکه قربانی نیاز دارند، رایج‌ترین سناریوها شامل هات‌اسپات‌های وای‌فای می‌شوند. یعنی هکر یا قادر به پایش ترافیک در یک شبکه عمومی است یا اکسس پوینت مخصوص به خودش را راه می‌اندازد تا قادر به انجام یک حمله مرد میانی باشد.

سرقت کوکی با بدافزار یا دسترسی مستقیم: یک راه بسیار رایج برای به دست آوردن کوکی‌های نشست، نصب بدافزار روی کامپیوتر کاربر است تا به صورت خودکار، نشست‌ها را اسنیف کند. به محض نصب شدن، مثلا بعد از اینکه کاربر به یک وب‌سایت آلوده رفت یا روی یک لینک آلوده در میان ایمیل‌های اسپم کلیک کرد، بدافزار شروع به اسکن ترافیک شبکه کاربر می‌کند تا قادر به یافتن کوکی‌های نشست و ارسال‌شان برای مهاجم باشد. یک راه دیگر برای به دست آوردن کلید نشست، دسترسی مستقیم به فایل کوکی در فضای ذخیره‌سازی موقت مرورگر کاربر است. این حمله هم می‌تواند توسط بدافزار و هم مهاجمی که دسترسی محلی یا از راه دور به سیستم دارد انجام شود.

حمله جستجوی فراگیر (Brute Force): در نهایت در این متد حمله، مهاجم می‌تواند خیلی آسان کلید نشست در نشست فعال یک کاربر را حدس بزند. این متد تنها در اپلیکیشن‌هایی قابل اجرا است که از شناسه‌های کوتاه و قابل پیش‌بینی استفاده می‌کنند. در گذشته دور، کلیدهای تابع یک نقطه ضعف رایج بودند، اما اپلیکیشن‌ها و شناسه‌های نشست مدرن طولانی بوده و به صورت رندوم تولید می‌شوند. برای اطمینان از مقاومت در برابر حملات بروت فورس، الگوریتم تولید کلید باید مقادیری واقعا غیر قابل پیش‌بینی تحویل دهد تا حملاتی که با حدس انجام می‌شوند، غیر قابل انجام باشند.

چطور می‌توان از سرقت نشست جلوگیری کرد؟

خطر سرقت نشست ناشی از محدودیت‌های پروتکل بدون حالت HTTP است. کوکی‌های نشست راهی برای فائق آمدن بر این محدودیت‌ها هستند و به وب اپلیکیشن‌ها اجازه می‌دهند که سیستم‌های کامپیوتری را شناسایی و اطلاعات‌شان را در وضعیت کنونی نشست ذخیره کنند. مثلا سبد خرید شما در یک فروشگاه آنلاین.

برای کاربران عادی مرورگرها، پیروی از چند قانون ساده می‌تواند ریسک این حملات را کاهش دهد، اما از آن‌جایی که سرقت نشست با سوء استفاده از مکانیزم‌های بنیادین تعبیه شده از سوی گستره وسیعی از وب اپلیکیشن‌ها صورت می‌گیرد، هیچ راهی برای تضمین امنیت در برابر این متد وجود دارد. برخی از رایج‌ترین کارهایی که می‌توان انجام داد به شرح زیر است:

- استفاده از HTPPS برای حصول اطمینان از اینکه تمام ترافیک نشست رمزگذاری می‌شود. این باعث می‌شود هکرها قادر به دستیابی به آی‌دی نشست در قالب متنی آشکار نباشند، حتی در صورتی که ترافیک قربانی را پایش کنند.
- استفاده از HttpOnly در هدر HTTP تا از دسترسی به کوکی‌ها از طریق اسکریپت‌های سمت مشتری جلوگیری شود. این باعث می‌شود XSS و دیگر حملات وابسته به تزریق جاوا اسکریپت در مرورگر، قابل انجام نباشند.
- به جای ساخت ابزار مدیریت نشست جدید خودتان، بهتر است از وب فریم‌وورک‌هایی استفاده شود که آی‌دی‌های قابل اعتماد برای نشست می‌سازند.
- می‌توان بعد از احراز هویت اولیه کاربر، یک کلید نشست جدید ساخت. به این ترتیب بعد از احراز هویت، کلید نشست فورا تغییر کرده و هکر حتی با در دست داشتن آی‌دی ابتدایی دیگر قادر به انجام هیچ کاری نخواهد بود.

- انجام احراز هویت اضافی، فراتر از کلید نشست هم کارآمد خواهد بود. این یعنی نه‌تنها باید از کوکی‌ها استفاده کرد، بلکه باید فاکتورهای دیگر مانند آی‌پی آدرس همیشگی کاربر و الگوهای مصرف از اپلیکیشن را نیز مد نظر قرار داد. نقطه ضعف این رویکرد آن است که هرگونه هشدار اشتباه می‌تواند باعث آزار رسیدن به کاربر واقعی شود.

دیجیاتو