حمله Session Fixation چیست و چگونه کار می کند؟ (نسخه PDF)

session fixation به نوعی زیر مجموعه ای از حملات application-level session hijacking محسوب میشود که در بحث نوع عملکرد و اجرا اگرچه اصول خود را حفظ کرده است اما تفاوت های اشکاری با سایر روش های موجود در این نوع حملات ندارد. اما به عنوان یک متخصص امنیت شبکه باید با مفهوم و عملکرد آن آشنا باشید چرا که فقط در صورت دانستن مکانیزم اجرایی اینگونه حملات خواهید توانست تمایز موجود بین انواع روش های session hijacking را بدرستی درک کنید.

Session Fixation

Session fixation حمله ای است که مستقیما هدف آن ربودن session معتبر یک کاربر است. برای اجرای این حمله، مهاجم از مزیت وجود محدودیت در نرم افزارهای تحت وب در رابطه با مدیریت session ID استفاده لازم را میبرد.نرم افزار تحت وب بجای صادر کردن یک session ID جدید، به کاربر این اجازه را میدهد تا با استفاده از session ID موجود خود را احزار هویت نماید. در این حمله مهاجم با دردست داشتن یک session ID معتبر، قربانی را به استفاده از آن هدایت میکند. اگر مرورگر قربانی از این session ID استفاده کند، مهاجم با علم به این که کاربر از این session ID استفاده میکند، میتواند براحتی session اعتباردهی شده کاربر را برباید.

یک حمله session fixation، نوعی از حمله session hijacking است. فرق بین این دو حمله در آن است که در حمله session hijackingحمله با استفاده از سرقت session برقرار شده پس از Login کاربر صورت میپذیرد در صورتی که حمله session fixation شروع حمله قبل از Login کاربر است. این حمله با استفاده از تکنیک های مختلفی میتواند اجرا شود. نوع تکنیک انتخاب شده توسط مهاجم بستگی به رفتار مرورگر مورد نظر با توکن های session دارد. در زیر برخی از روش های رایج در اجرای حمله session fixation آورده شده است:

- Session token در آرگومان URL
- Session token در فرم مخفی
- Session ID در کوکی

حمله session Fixation

در تکنیک HTTP header response از حمله session fixation، مهاجم مرتبا با جستجوی پاسخ های ارسالی از طرف سرور، بدنبال پیدا کردن session ID است. علاوه بر این مهاجم این امکان را نیز دارد تا session ID مورد نظر خود را با کمک پارامتر set cookie درون کوکی جای گذاری نماید. هنگامی که کوکی بصورت دلخواه تنظیم شد، مهاجم آن را بسوی مرورگر قربانی ارسال میکند. Session fixation در سه فاز انجام میشود:

- مرحله برقراری و ایجاد session ID: در این فاز مهاجم نخست یک session ID معتبر را با استفاده از برقراری ارتباط با نرم افزار تحت وب، بدست میآورد. تعداد کمی نرم افزار تحت وب وجود دارد که قابلیت session time-out را پشتبانی کنند. از این رو مهاجم با بدست آوردن session ID محدودیت زمانی برای اجرای حمله نخواهد داشت. در آندسته از نرم افزارخای تحن وبی که این قابلیت را پشتیبانی میکنند، مهاجم باید مرتبا و پیوسته درخواست هایی را به منظور تمدید و زنده نگهداشتن session ارسال نماید.
- مرحله تثبیت (fixation): در این فاز مهاجم session ID را درون مرورگر قربانی وارد میکند و session را تثبیت مینماید.
- مرحله ورود (Entrance): در این فاز مهاجم منتظر میماند تا کاربر با استفاده از session ID تله گذاری شده به وب سرور login کند.

فرض کنید که قربانی میخواهد از خدمات اینترنتی بانک استفاده کند. همچنین فرض کنید که آدرس بانک مورد نظر HTTP:////citibank.com باشد. مهاجم اگر بخواهد که این session را تثبیت نماید باید مراحل گفته شده در زیر را انجام دهد:

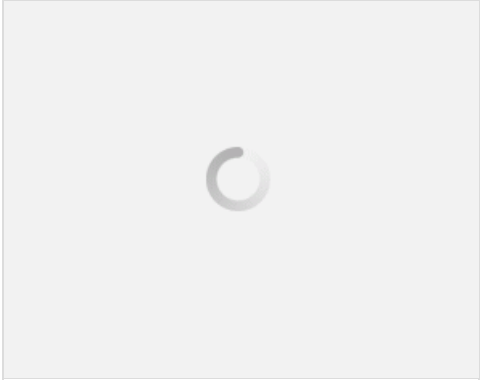
۱. ابتدا مهاجم بایستی با استفاده از یک اعتبار کاربری به وب سایت بانک login کند.
۲. سپس HTTP:////citibank.com یک session ID برای آن صادر میکند. (۰D۶۴۴۱FEA۴۴۹۶C۲)
۳. مهاجم session ID را درون لینکی آلوده جای گذاری کرده (HTTP://citibank.com/? SID=۰D۶۴۴۱FEA۴۴۹۶C۲) و آن را بسوی قربانی ارسال میکند و با ترفند کاربر را به کلیک بر روی لینک آلوده ترغیب خواهد کرد.
۴. هنگامی که قربانی بر روی لینک مورد نظر با فرض این که لینک معتبر برای ورود به سایت بانک است، کلیک کرد، مستقیما با

session ID مورد نظر مهاجم وارد سایت بانک میشود. (۰D۶۴۴۴۱FEA۴۴۹۶C۲)

۵. وب سرور بانک با بررسی session ID مورد نظر متوجه میشود که این session از پیش برقرار شده و حالت فعال دارد؛ بنابراین دیگر نیازی به صدور یک session ID جدید نمیبیند.

۶. حالا مهاجم میتواند با استفاده از session ID معتبر خودش و کاربری شخص قربانی، دست به اعمال مجرمانه خود بزند.

برای جمع بندی این نوع حمله، میتوان گفت که در این روش، قربانی با اسـتفاده از session ای که از پیش مهاجم آماده کرده است، login میکند.



نویسنده: احسان امجدی

منبع: انجمن تخصصی فناوری اطلاعات ایران

مطلب اصلی