CSRF

عندما تقوم بتسجيل الدخول إلى حسابك على موقع ما، يتم إنشاء جلسة

(session)

تحتفظ بمعلوماتك، مثل هويتك وصلاحياتك على الموقع. تُرسل هذه المعلومات مع كل طلب تقوم به على .الموقع لتحديد هويتك والتأكد من صلاحياتك

، يستغل المهاجم هذه الجلسة المفتوحة لديك لإرسال طلبات إلى الموقع من حسابك CSRF الآن، في هجوم دون معرفتك. المهاجم يبني صفحة ويب ملغومة تحتوي على طلبات مُخادعة تُرسل تلقائيًا إلى الموقع .الذي أنت مسجل دخول عليه

لنفترض أنك مسجل دخول على حسابك في البنك على موقع ما، ثم تقوم بزيارة صفحة ويب أخرى تحتوي على رابط مُخادع. عند فتح هذا الرابط، ستبدأ الطلبات الخبيثة في التنفيذ من حسابك في البنك بشكل غير .مرئي

CSRF الأضرار التي يمكن تسببها الهجوم

تشمل تغيير كلمات المرور، إجراء عمليات مالية غير مصرح بها، حذف البيانات، إرسال رسائل بريد .إلكتروني بالنيابة عنك، وغيرها

، CSRF لمنع الهجمات

CSRF tokens يمكن استخدام تقنيات مثل

، حيث يتم إضافة رموز فريدة لكل طلب يتم إرساله إلى الموقع، وتحتوي هذه الرموز على معلومات .تحقق للتأكد من أن الطلب يأتي من مستخدم حقيقي وليس من مهاجم