CSRF

التزوير عبر الموقع (CSRF) هو ثغرة أمنية في تطبيق الويب تسمح للمهاجم بتنفيذ إجراءات غير مصرح بها نيابة عن المستخدم الضحية. يحدث ذلك عندما يخدع أحد المهاجمين متصفح المستخدم لتقديم طلب إلى موقع ويب مستهدف دون علم المستخدم أو موافقته.

**كيفية منع هجمات CSRF كمطور**

تتمثل إحدى أفضل الطرق لمنع CSRF في استخدام الرموز المميزة المتغيرة بشكل متكرر بدلاً من الاعتماد على ملفات تعريف الارتباط للجلسة لتشغيل تغيير الحالة على الخادم.

توفر العديد من أطر العمل الخلفية الحديثة الأمان ضد CSRF، لذلك إذا كنت ترغب في تجنب الجوانب الفنية لتعزيز CSRF بنفسك، فيمكنك معالجتها بسهولة باستخدام أطر عمل من جانب الخادم تأتي مع الرموز المميزة المضادة لـ CSRF.

عند استخدام رمز مضاد لـ CSRF، فإن الطلبات المستندة إلى الخادم تنشئ سلاسل عشوائية بدلاً من ملفات تعريف الارتباط للجلسة الأكثر ثباتًا، وبهذه الطريقة، يمكنك حماية جلستك من التخمين من قبل الخاطف.

يؤدي تطبيق نظام مصادقة ثنائية (2FA) لتشغيل المعاملات على تطبيق الويب الخاص بك أيضًا إلى تقليل فرص CSRF.

من الممكن بدء CSRF عبر البرمجة النصية عبر المواقع (XSS)، والتي تتضمن

إدخال البرنامج النصي في حقول المستخدم مثل نماذج التعليقات، ولمنع هذا، من الممارسات الجيدة تمكين ميزة الهروب التلقائي لـ HTML في جميع حقول نماذج المستخدم عبر موقع الويب الخاص بك، حيث يمنع هذا الإجراء حقول النموذج من تفسير عناصر HTML.