CSRF Protection

حماية CSRF (Cross-Site Request Forgery) هي آلية أمان تهدف إلى منع الهجمات التي تستغل ثقة المستخدمين في مواقع الويب .تسمح هذه الحماية للمواقع بالتحقق من أن الطلبات القادمة من مستعرض المستخدم تأتي من نفس الموقع وليس من موقع ويب ضار .ببساطة، تمنع حماية CSRF المتسللين من استغلال المستخدمين الذين قاموا بتسجيل الدخول إلى موقع ويب معين لإجراء عمليات غير مصرح بها على هذا الموقع.

كيف تعمل حمايةCSRF ؟

تعتمد حماية CSRF عادةً على استخدام رموز فريدة (أو "رموز") تُعرف بـ "رموز مكافحة CSRF" أو "رموز CSRF". يتم إنشاء هذه الرموز بواسطة الخادم وتضمينها في النماذج أو الطلبات التي يرسلها المستخدم .عندما يرسل المستخدم طلبًا، يتحقق الخادم من صحة رمز CSRF الموجود في الطلب، وإذا لم يكن الرمز موجودًا أو كان غير صحيح، يتم رفض الطلب.

أمثلة على حماية CSRF:

- الرموز المميزة:

يتم تضمين رمز مميز فريد وعشوائي في حقل مخفي داخل نموذج الويب .عند إرسال النموذج، يتحقق الخادم من صحة هذا الرمز.

- تزامن الرموز مع ملفات تعريف الارتباط:

يتم مزامنة رمز CSRF مع ملف تعريف الارتباط الخاص بالمستخدم، ويتحقق الخادم من تطابق الرمزين قبل معالجة الطلب .

أهمية حماية CSRF:

- منع العمليات غير المصرح بها:

تمنع حماية CSRF المتسللين من تنفيذ إجراءات غير مصرح بها على موقع الويب من خلال استغلال ثقة المستخدمين.

- حماية خصوصية المستخدمين:

تساهم حماية CSRF في حماية بيانات المستخدمين وخصوصيتهم من الوصول غير المصرح به.

- ضمان سلامة العمليات:

تضمن حماية CSRF أن العمليات التي تتم على الموقع تتم بناءً على طلبات شرعية من المستخدمين.

XSS Prevention

XSS، أو برمجة نصية عبر المواقع، هو نوع من الهجمات التي تسمح للمهاجمين بحقن نصوص برمجية خبيثة في مواقع ويب موثوقة .هذا النوع من الهجمات يستغل ثغرات في تطبيقات الويب تسمح بإدخال بيانات غير معالجة في المخرجات، مما يتيح للمهاجمين تنفيذ تعليمات برمجية ضارة في متصفحات المستخدمين

كيف يعمل هجومXSS ؟

1. الحقن:

يقوم المهاجم بحقن نص برمجي خبيث، عادةً ما يكون بلغةJavaScript ، في موقع ويب يحتوي على ثغرة أمنية.

2. التنفيذ:

عندما يزور مستخدم موقع الويب المصاب، يتم تحميل وتنفيذ النص البرمجي الخبيث في متصفحه.

3. الضرر:

يمكن للنص البرمجي أن يقوم بعدة أمور ضارة، مثل:

- **سرقة ملفات تعريف الارتباط :(Cookies)** يمكن للنص البرمجي سرقة معلومات تسجيل الدخول الخاصة بالمستخدم، مما يتيح للمهاجم الوصول إلى حسابه.
- **سرقة البيانات الحساسة :**يمكن للنص البرمجي الوصول إلى أي بيانات يعرضها الموقع في متصفح المستخدم، مثل معلومات الحساب المصرفي أو بيانات شخصية أخرى.
- **إعادة توجيه المستخدمين :**يمكن للنص البرمجي إعادة توجيه المستخدمين إلى مواقع ويب ضارة أخرى.
- **تشويه مواقع الويب :**يمكن للنص البرمجي تغيير محتوى صفحات الويب، مما قد يؤدي إلى تشويهها أو جعلها غير قابلة للاستخدام .

كيفية الوقاية من هجمات XSS:

1. التحقق من صحة المدخلات:(Input Validation)

يجب التحقق من صحة جميع المدخلات التي يقدمها المستخدمون للتأكد من أنها آمنة وأنها لا تحتوي على أي تعليمات برمجية ضارة.

2. ترميز المخرجات:(Output Encoding)

يجب ترميز جميع المخرجات التي يتم عرضها على صفحات الويب، خاصةً تلك التي تستند إلى مدخلات المستخدم.

3. استخدام قوائم الأمان:(Content Security Policy - CSP)

يمكن استخدام CSP لتحديد مصادر المحتوى الموثوق بها، مما يحد من قدرة النصوص البرمجية الخبيثة على التنفيذ.

4. تحديث البرامج والتطبيقات:

يجب تحديث البرامج والتطبيقات بانتظام لإصلاح أي ثغرات أمنية معروفة.

5. استخدام أدوات فحص الأمان:

يمكن استخدام أدوات فحص الأمان لتقييم مواقع الويب والتطبيقات بحثًا عن نقاط ضعف XSS.