Was ist ein CSRF-Fehler?

Das Campact-Team - 2021-10-26 - in Aktionsteilnahme

Der Hinweis CSRF-Fehler (Cross-Site Request Forgery; zu dt. Website-übergreifende Anfragenfälschung) tritt sehr selten auf. Er ist das Ergebnis eines Sicherheitschecks, der sicherstellt, dass wir Anfragen, die z.B. durch Absenden eines Teilnahmeformulars an unseren Server geschickt werden, wirklich vertrauen können. Er tritt unter anderem dann auf, wenn Sie ein Teilnahmeformular im Browser geöffnet und länger als dreißig Minuten nichts auf der Seite gemacht haben. Wenn Sie dann das Formular ohne erneutes Laden der Seite absenden, erhalten Sie unsere Fehlermeldung.

Um die Fehlermeldung nicht mehr zu erhalten und an den Aktionen teilnehmen zu können, laden Sie die Seite bitte neu. Sie können dann an der Aktion teilnehmen. Sollte der Fehler bestehen bleiben aktualisieren Sie bitte Ihren Browser auf die neuste Version.

Der CSRF-Mechanismus ist ein bekannter Weg für Angriffe auf Computersysteme, vor denen wir uns und unsere Besucher*innen schützen müssen, auch wenn der allergrößte Teil der Fehlermeldung - wie vermutlich auch bei Ihnen - Fehlalarme bleiben.

Wie läuft ein solcher Angriff ab:

- Ein*e Nutzer*in nutzt eine Webanwendung, z. B. Onlinebanking, und authentifiziert sich.
- Der Browser erhält vom Server einen Cookie zur Wiedererkennung, die so genannte Session-ID (zu dt. eine “Identifikationsnummer für die Sitzung”).
- Der*die Nutzer*in navigiert, ohne sich abzumelden, auf eine andere Seite (oder öffnet einen weiteren Browser-Tab oder ein -Fenster). Beispielsweise öffnet er über einen Link in einer E-Mail eine angebliche Umfrage zum Onlinebanking.
- Auf dieser Seite ist ein Formular oder Skript verborgen, mit dessen Hilfe der Browser dazu veranlasst wird, eine Website innerhalb der anderen Webanwendung, also dem Onlinebanking, zu öffnen.
- Das noch gültige Cookie der ersten Webanwendung wird automatisch mitgeschickt. Der*die Angreifer*in hat dadurch vollen Zugriff und kann eine Transaktion in der Webanwendung durchführen. Bei CSRF werden die durch das Cookie im Browser gespeicherten Informationen missbraucht, um im Namen des Nutzers*der Nutzerin Aktionen auf einer Website durchzuführen.

Tags

Cross-Site Request Forgery

csrf

fehler