# Arbeitsblatt

Gruppe:

Was man braucht:

* Entwicklungsumgebung zum Bearbeiten von Webanwendungen / JS, z.B. [VSC](https://code.visualstudio.com/)
* Laufende JavaScript-Laufzeitumgebung, z.B. [Node.js](https://nodejs.org/de)
* Vorbereiteter Code: Zu [GitHub](https://github.com/Stefzockt/CSRF/)
* Evtl. Folien der Präsentation (Ebenfalls auf [GitHub](https://github.com/Stefzockt/CSRF/))

**Was ist CSRF?**

**Wie funktioniert CSRF? Was sind die Voraussetzungen?**

**Für was können CSRF-Angriffe genutzt werden?**

**Was können die Folgen von CSRF-Angriffen sein?**

**Wie kann man sich gegen CSRF schützen?**

**Übung**

Anna war eine erfolgreiche Geschäftsfrau. Sie leitete ein kleines Unternehmen, das Software für Unternehmen entwickelte. Eines Tages erhielt Anna eine E-Mail von einem angeblichen Kunden, der Hilfe bei einem Softwareproblem benötigte.

Anna war immer bereit, ihren Kunden zu helfen, also öffnete sie die E-Mail. Die E-Mail enthielt einen Link zu einer Website, die angeblich die Website ihres Unternehmens war.

Dieser Link leitete sie aber auf eine andere Website, welche nichts mit ihrem Unternehmen zu tun hatte. Anna bemerkte vorerst nichts, als sie aber einige Tage später auf ihren Account schaute, bemerkte sie, dass ihr Guthaben weniger geworden ist.

**Simulation eines CSRF-Angriffs**

Simulieren sie einen CSRF-Angriff, indem sie eine bösartige Anfrage auf der Fake Website evil-examples.html erstellen, die den User Anna dazu bringt, Geld von ihrem Account der Website home.html an den User BoeserMann zu senden.

Tipp: Anna einloggen nicht vergessen

**Implementierung einer Schutzmaßnahme**

Implementieren sie eine Methode zum Schutz vor CSRF-Angriffen, indem sie einen Anti-CSRF-Token verwenden. (Double Submit Cookies müssen nicht beachtet werden)

Beispiele:

* Video: <https://www.youtube.com/watch?v=80S8h5hEwTY>
* Tutorial 1: <https://www.invicti.com/blog/web-security/protecting-website-using-anti-csrf-token/>
* GitHub: [https://github.com/valexandersaulys/tiny-csrf](https://github.com/valexandersaulys/tiny-csrf%20)