CSRF

Inhaltsverzeichnis

- 1 Funktionsweise
- 2 Typische Einsatzbereiche
- 3 Wichtige Hinweise
- 4 Fazit

CSRF (Cross-Site Request Forgery) missbraucht die bestehende Sitzung eines Nutzers, um unerwünschte Aktionen auf einer anderen Website auszulösen. Schutz braucht Tokens und strikte Request-Validierung.

1 Funktionsweise

Das Opfer ist in einer Web-App eingeloggt; eine fremde Seite löst einen Request an diese App aus. Browser senden Cookies automatisch mit – ohne zusätzliche Prüfung wirkt der Request legitim.

- **Session Riding:** Ausnutzen der Login-Session
- **State-changing Requests:** POST/PUT/DELETE besonders kritisch
- **Anti-CSRF-Token:** secret pro Formular/Session

2 Typische Einsatzbereiche

- Webanwendungen mit Cookie-Sessions
- Admin-Backends und Self-Service-Portale
- Security-Reviews und Secure Coding

3 Wichtige Hinweise

- SameSite-Cookies helfen, ersetzen aber nicht immer Tokens.
- APIs mit Bearer-Tokens sind anders bedroht.
- Idempotente GETs sollten keine Zustandsänderungen auslösen.

4 Fazit

CSRF bleibt ein Klassiker der Web-Sicherheit – mit Anti-CSRF-Tokens, SameSite und sauberer Request-Semantik gut beherrschbar.