XSS

- Ausnutzen einer XSS Schwachstelle führt JavaScript aus, der nicht von dem Autor der Website selbst dort platziert wurde
- Umgeht Sicherheitsmechanismen wie Same Orgin Policy (SOP)
- verschiedene Untertypen von XSS Schwachstellen

Reflected XSS

- "reflektiert" eine Anfrage im Ergebnis vom Server zurück an den Browser
- im Browser wird das JavaScript ausgeführt
    - kann daher zb in Suchfeldern ausgenutzt werden
    - oder direkt in der URL im Abschnitt für das Query

Stored XSS

- Angreifer speichert JavaScript Code in der Datenbank die der Server nutzt
- der Server liefert Code aus sobald beliebger User zugreift
- im Browser wird das JavaScript ausgeführt

Nachweis

- XSS Schwachstelle wird über Funktionsaufruf demonstriert
- häufig wird alert() Funktion genutzt um Popup zu erzeugen

Code Snippets

```
<script>alert(1)</Script>
```