#xss - > cross site scripting

Ein Angriff zwischen verschiedenen Aufrufen einer Seite.

Gemeint ist in der Regel nicht, dass unterschiedliche Websites beteiligt sind.

XSS ist HTML injection via JavaScript.

- drei arten (reflektiert, persistent, lokal)
    - reflektiert -> nur solange aktiv bis die seite neu vom server geladen wird
    - persistent -> solange bis der schadcode auf dem server entdeckt und beseitigt wird
    - lokal -> wenn ein url argument ohne prüfung direkt ausgegeben wird

- beispiele: entführen von benutzersessions, übernahme des browserbenutzers

- gegenmassnahmen:
    - eingehenden werte immer als unsicher betrachtet und vor der weiteren verarbeitung serverseitig prüfen
    - whitelist prüfverfahren bei eingabemöglichkeiten zählt zu best practices

- quelle: https://de.wikipedia.org/wiki/Cross-Site-Scripting