XSS (Cross-Site Scripting)

Inhaltsverzeichnis

XSS (Cross-Site Scripting) schleust schädlichen JavaScript-Code in Webseiten ein, der im Browser anderer Nutzer ausgeführt wird. So lassen sich Sitzungen stehlen, Inhalte manipulieren oder Aktionen im Namen des Opfers auslösen.

1 Funktionsweise

Angreifer platzieren Script-Fragmente in Eingaben oder URLs, die unzureichend gefiltert ausgegeben werden. Der Browser des Opfers vertraut der Seite und führt den Code aus.

- **Stored XSS:** dauerhaft gespeicherter Payload
- **Reflected XSS:** über URL/Parameter zurückgespiegelt
- **DOM XSS:** unsichere Client-seitige Verarbeitung

2 Typische Einsatzbereiche

- Webapps, CMS und Admin-Oberflächen
- Security-Reviews und Penetrationstests
- Secure Coding und Output-Encoding

3 Wichtige Hinweise

- Context-aware Encoding (HTML, JS, URL) ist entscheidend.
- CSP reduziert Auswirkungen, ersetzt aber keine saubere Ausgabe.
- HttpOnly-Cookies mindern Session-Diebstahl, nicht jede XSS-Wirkung.

4 Fazit

XSS bleibt ein Kernrisiko im Web – beherrschbar durch strikte Ausgabe-Kodierung, Validierung und Defense-in-Depth im Browser.