Cross Site Scripting (XSS)

Apa itu XSS?

- Injection attack
- Mengeksploitasi client-side code
- Malicious code akan dijalankan pada browser user
- Bypass "same-origin policy"
- Antara Risiko: Attacker boleh curi cookie dan menyamar menjadi si mangsa

Jenis-Jenis XSS

- Reflected
- Stored
- DOM-based

Reflected XSS

- XSS paling basic
- Script di-"embed" terus ke dalam malicious link
- Script akan dijalankan apabila mangsa pergi ke link tersebut

Stored XSS

- Script akan disimpan di dalam "database" website yang di-eksploit
- Contoh, bahagian komen di dalam forum. Setiap kali pengguna lain load page dengan komen tersebut, script akan dijalankan.

DOM-based XSS

- JavaScript pada client-side akan di-eksploitasi
- ??? :P