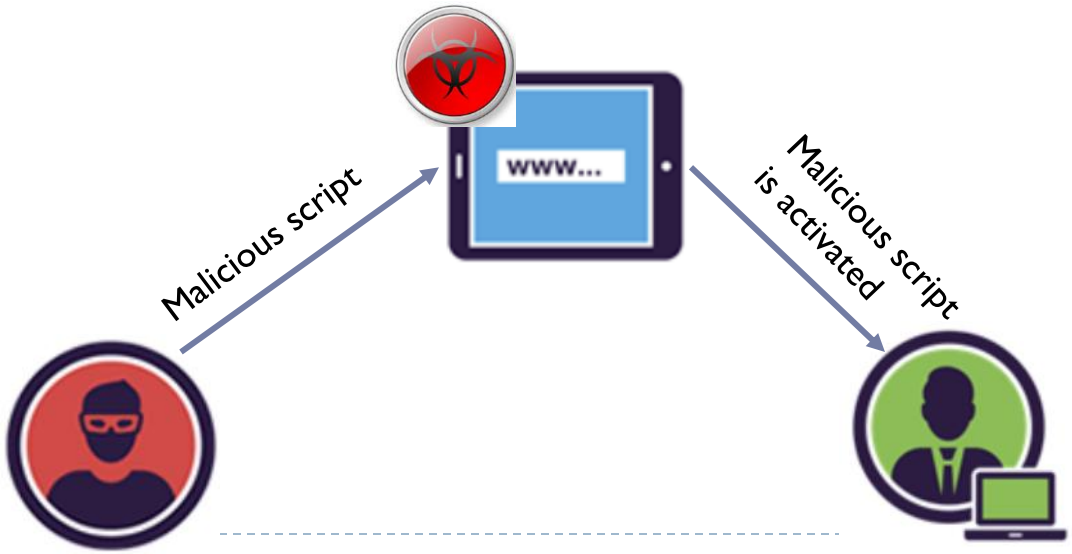
Stored XSS Attack (Persistent)

Attacker's code is stored persistently on the website

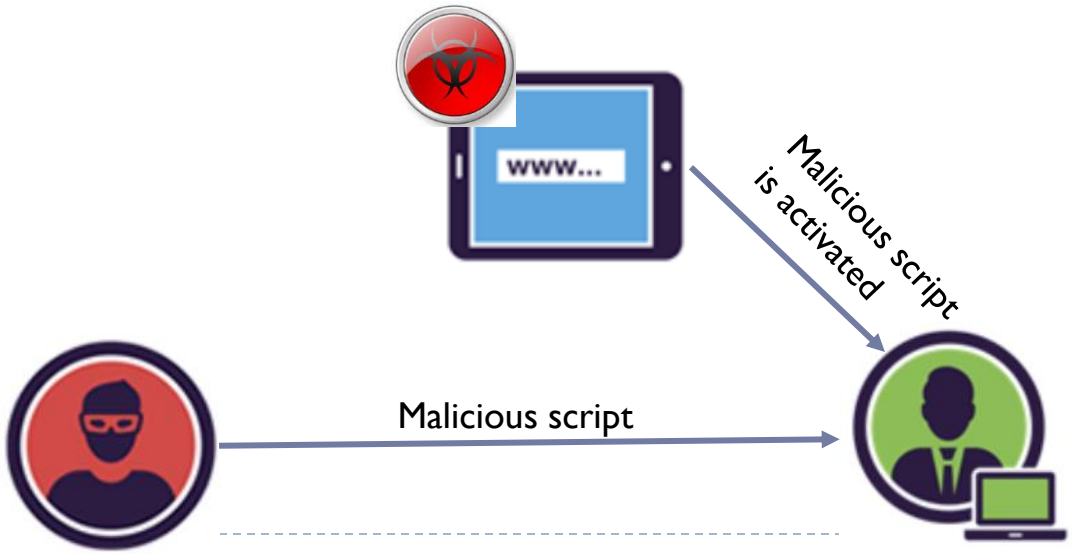
- The attacker discovers a XSS vulnerability in a website
- The attacker embeds malicious commands inside the input and sends it to the website.
- Now the command has been injected to the website.
- A victim browses the website, and the malicious command will run on the victim's computers.



Reflected XSS Attack (Non-persistent)

The attacker tricks the victim to put the code in the request and reflected from the server

- The attacker discovers a XSS vulnerability in a website
- The attacker creates a link with malicious commands inside.
- The attacker distributes the link to victims, e.g., via emails, phishing link.
- A victim accidently clicks the link, which actives the malicious commands.



Defenses against XSS

Content Security Policy (CSP)

- Instruct the browser to only use resources loaded from specific places.
- Policies are enforced by the browser.
- Examples of policies
  - Disallow all inline scripts
  - Only allow scripts from specific domains

Input inspection

- Sanitization: escape dangerous characters
- Validate and reject malformed input.