Problem

➡ An attacker can inject **arbitrary javascript code** in the page that will be executed by the browser

- **Inject illegitimate content** in the page (same as content spoofing)

- **Perform illegitimate HTTP requests** through Ajax (same as a CSRF attack)

- **Steal Session ID** from the cookie

- **Steal user's login/password** by modifying the page to forge a perfect scam

Problem

➡ An attacker can inject **arbitrary javascript code** in the page that will be executed by the browser

- **Inject illegitimate content** in the page (same as content spoofing)
- **Perform illegitimate HTTP requests** through Ajax (same as a CSRF attack)
- **Steal Session ID** from the cookie
- **Steal user's login/password** by modifying the page to forge a perfect scam

Forging a perfect scam

* _Notice that Youtube is **not** vulnerable to this attack_