



Pröblen

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

• **Inject illegitimate content** in the page  
(content spoofing)

• **Perform illegitimate HTTP requests** through Ajax

(another way to do a CSRF attack)

o'st a'si on iD fi n th e c o k i e

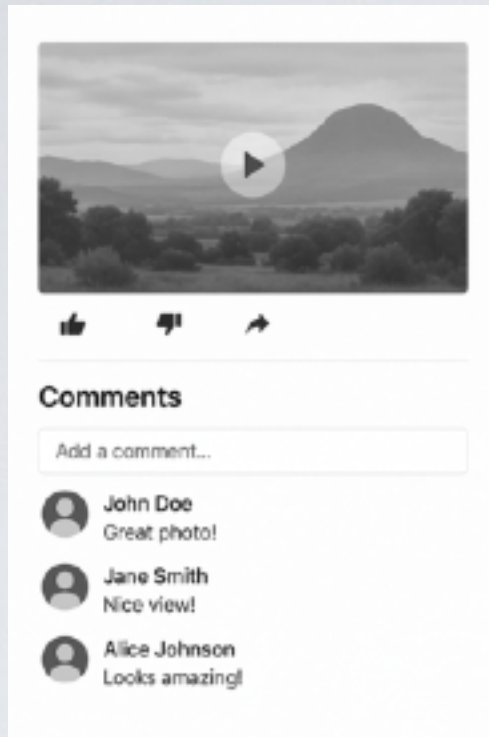
● **Steal user's login/password** by modifying the page to  
forge a perfect scam

# Problem

- ➔ An attacker can inject **arbitrary javascript code** in the page that will be executed by the browser
- ⦿ **Inject illegitimate content** in the page  
(content spoofing)
- ⦿ **Perform illegitimate HTTP requests** through Ajax  
(another way to do 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



### Login

Username

Password

Log In

[Forgot password?](#)