Curs 13 - PHP

* În mod normal, dacă userul se delogează sau apasă pe săgeata „înapoi", nu ar mai trebui să se poată accesa contul de altcineva

* Toate cererile sunt independente! Serverul trebuie să știe că toate acțiunile fac parte din aceeași sesiune (între login și logout)
* Se replică valoarea cookie-ului de sesiune → serverul poate grupa

- htmlentities → previne Sql injection
- addslashes → ajută la \ : evită unele caractere " \
- funcția header(" "); → setează un atet http care precede un newline care precede conținutul trimis
- session_start → populează tabela SESSION (tablou asociativ), unde se vor pune variabilele de sesiune
- session_destroy(); → depopulează tabela
  ↳ trebuie înainte în fișier să apară session_start()

* Isonfidentificationtoken → pasat de frontend pe backend pentru a menține un cookie

* cheie secretă de sesiune → negociată prin https, din pt același motiv
* la cookie poți să îi setezi durata: la cele de sesiune e bine să nu fie prea mare (de obicei când se dă logout, expirare explicită; expiră singur, implicit (setabil))
* valoarea cookie-ului de sesiune este critică d.pd.v. al securității, deoarece te poți da drept alt user!

- o sesiune ≠ user logat (nu neapărat): se pot face acțiuni și fără să fi logat pt. că unele site-uri asociază cu vechile cookiuri
- cookie-urile de sesiune pot fi reciclate

* Sql injection se pot face și la username și la parolă
* pot exista vulnerabilități și la librării => cod vulnerabil