Lab 5: Password-hashing (iterative hashing, salt, memory-hard functions)

1. zadatak

-U prvom zadatku pokušavamo procjeniti brzinu izvršavanja kriptografskih funkcija.

-Dekorator prima funkciju i vraća funkciju i dekorira je na način da izmjeri vrijeme izvršavanja

-provrtili smo par funkcija

-SHA512 i i SHA256 imaju otprilike jednaka vremena izvrsavanja

2. zadatak

-Implementacija procesa inicijalne registracije i login korisnika korištenjem sigurne Argon2 password hashing funkcije

-u folderu smo kreirali novu skriptu za autentifikacju

-implementirali smo dvije funkcije: jedna za registraciju i druga za logiranje

-koristili smo SQLite bazu podataka

-implementirali smo registration funkciju za registraciju korisnika, funkcija registrer prima argumente username i password (njega hashira). Funkcija sama generira sol i onda ce uz pasword hash vratiti sol i to će završiti u bazu podataka

-u funckiji do register smo definirali tri korisnika: prva dva imaju ista username-a, a prvi i treći imaju isti password. U bazi se nalazi tablica s dva inputa username i password. U bazi imamo dva username-a jer se jedan ponovio dva puta

-U funkciji do register korisnika se pita za unos username-a i ponavljanje username-a provjerava se s funkcijom get_user. Od korisnika se traži unos passworda pomoću getpass.

-argon2.verify provjerava je li unesena sifra tocna na siguran nacin