Vjezbe 5

Na ovim vjezbama smo prvo usporedili brzinu razlicitih HASH-eva i enkripcija pa smo tako usporedili brzinu AES-a, sha256 i sha512 nakon 100 iteracija. Vidjeli smo da je razlika prilicno znacajna (ako se dobro sjecam razlika izmedu AES-a i sha 512 je bila cak *10^3) a postoje i brze i sporije funkcije od tih. Poanta toga je bila da vidimo o kakvim razlikama je rijec i razmislimo o tome kada valja koju upotrijebiti ovisno o tome je li nam bitnija brzina ili otjerati potencijalnog napadaca.

U drugom dijelu vjezbi smo sa kodom generiranim uz pomoc ChatGPT-a napravili osnovni sistem registracije korisnika koje smo pohranjivali u SQL bazu u koju smo spremali username i HASH password-a.

Zatim smo pokusali unijeti 3 nova korisnika od kojih dva sa istim username-om sto nam naravno nije dozvoljelo jer nam je username PRIMARY KEY te je odbacilo taj pokusaj registracije.

Za obje osobe koje smo uspjesno registrirali smo stavili isti password cime smo vidjeli utjecaj salt-a pri HASH-iranju jer su password HASH-evi spremljeni u bazu bili potpuno drugaciji sto dodatno otezava napadacev posao jer mu je onemogucen napad sa precomputed dictionary-jem.

Kod log in-a argon2 funkcija prima uneseni password i spremljeni HASH te zatim ponovno HASH-ira uneseni password i usporeduje dobiveni HASH sa spremljenim kako bi potvrdio valjanost unesenog password-a.

Takoder kao dodatnu ali jednostavnu i znacajnu mjeru opreza trazi se da se unese i username i password prije nego sto se dogodi ikakva provjera jer time dodajemo sansu da napadac pogrijesi i username a pogodi password ali ne zna u cemu je zapravo greska.