Lab 5

U ovim vježbama smo za početak vidjeli brzinu različitih HASH funkcija kao što su AES, SHA256 i SHA512 nakon određenog broja iteracija. Razlike u brzinama su bile značajne, čime smo vidjeli da se različite HASH funkcije koriste u različite svrho ovisno o njihovoj brzini.

Nakon toga smo u python-u napravili osnovni sistem registracije korisnika čiji smo username i hashirani password spremali u SQL bazu podataka. Pokušali smo unijeti više korisnika s istim usernamom, što nije bilo moguće, te smo za dva uspješno unesena usera postavili da imaju isti password. Hash passworda je bio potpuno drugačiji u bazi čime smo vidjeli utjecaj soli. Prilikom logiranja argon2 funkcija uzima uneseni password i spremljeni hash te ponovno heshira uneseni password i usporedi ga s onim spremljenim u bazi podataka kako bi se utvrdila ispravnost unesenog passworda. Kao dodatnu mjeru sigurnosti smo prilikom unosa usernama i passworda postavili da na sustav javlja pogrešku tek nakon što unesemo oboje kako bi se otežalo kako saznati jeli greška u usernamu ili u passwordu.