**Kratki opis sustava zaštite**

Sustav koristi kriptografsku funkciju sažetka (**argon2id**) kako bi zaštitio lozinke. Prilikom svakog unosa nove lozinke (pri kreiranju korisnika ili mijenjanju sadašnje lozinke), koristi se novi ***salt*** te je na taj način osigurava da napadač ne može odrediti je li lozinka uistinu promijenjena ili nije.

Tijekom unosa lozinke **nisu vidljive**.

Preventirani su **vremenski napadi**, tj. *timing attacks*, na način da su prilikom usporedbe *hasheva* korištene funkcije s konstantnim vremenom usporedbe (metoda *verify*).

Također, čak i ako korisnik ne postoji u bazi, logiranje u sustav će se **imitirati**, kako bi se napadaču spriječilo dobivanje bilo kakve informacije o korisnicima i lozinkama.

**Neimplementirane zaštite**

Enkripcija korisničkog imena (*username*)

Napadač će prilikom pristupa datoteci s lozinkama imati uvid u popis korisnika. To nužno ne mora predstavljati problem, ovisno o namjeni sustava. Korisnička imena se uglavnom sastoje od alfanumeričkih znakova te bi njihovo enkriptiranje (ili *hashiranje*) usporilo sustav, a ne bi značajno doprinijelo zaštiti sustava.