

# Bezbednost Interneta

Neke diskusije o zaštiti lozinki

Andrija Urošević

Univerzitet u Beogradu  
Matematički fakultet

April, 2022.

# Pitanja

---

Koliko vas je hakovano?

Koliko vas je hakovalo?

Koliko vas će hakovati?

# Pregled

---

1. Kako čuvati lozinke?
2. Menadžer lozinki
3. CTF: Capture The Flag

# Čuvanje lozinki

---

## Ključno pitanje

Pretpostavimo sledeći scenario: Razvijamo neku veb aplikaciju. Da bi naša aplikacija funkcionisala zahteva sistem prijavljivanja radi autentifikacije korisnika. Odlučili smo da autentifikaciju vršimo preko lozinke.

*Kako čuvati lozinke u bazi podataka?*

# Otvoreni tekst

---

## Otvoreni tekst

Otvoreni tekst u kriptografiji predstavlja nešifrovanu informaciju.

username	password
nikola	password1
marko	matrix
petar	yep59f\$4txwrr

# Otvoreni tekst

---

## Otvoreni tekst

Otvoreni tekst u kriptografiji predstavlja nešifrovanu informaciju.

username	password
nikola	password1
marko	matrix
petar	yep59f\$4txwrr

Pozitivno:

# Otvoreni tekst

---

## Otvoreni tekst

Otvoreni tekst u kriptografiji predstavlja nešifrovanu informaciju.

username	password
nikola	password1
marko	matrix
petar	yep59f\$4txwrr

Pozitivno:

- lako se implementira

# Otvoreni tekst

---

## Otvoreni tekst

Otvoreni tekst u kriptografiji predstavlja nešifrovanu informaciju.

username	password
nikola	password1
marko	matrix
petar	yep59f\$4txwrr

Pozitivno:

- lako se implementira

Negativno:



# Otvoreni tekst

## Otvoreni tekst

Otvoreni tekst u kriptografiji predstavlja nešifrovanu informaciju.

username	password
nikola	password1
marko	matrix
petar	yep59f\$4txwrr

Pozitivno:

- lako se implementira

Negativno:

- vidljive lozinke

# Šifrovanje lozinki

## Šifrovanje

*Šifrovanje* je proces enkodiranja informacija. Tokom šifrovanja originalna reprezentacija informacije (otvoreni tekst) se konvertuje u alternativnu reprezentaciju koja se naziva *šifrat*.

username	rot13(password)
nikola	cnffjbeq1
marko	zngevk
petar	lrc59s\$4gkjee

# Šifrovanje lozinki

## Šifrovanje

*Šifrovanje* je proces enkodiranja informacija. Tokom šifrovanja originalna reprezentacija informacije (otvoreni tekst) se konvertuje u alternativnu reprezentaciju koja se naziva *šifrat*.

username	rot13(password)
nikola	cnffjbeq1
marko	zngevk
petar	lrc59s\$4gkjee

Pozitivno:

# Šifrovanje lozinki

## Šifrovanje

*Šifrovanje* je proces enkodiranja informacija. Tokom šifrovanja originalna reprezentacija informacije (otvoreni tekst) se konvertuje u alternativnu reprezentaciju koja se naziva *šifrat*.

username	rot13(password)
nikola	cnffjbeq1
marko	zngevk
petar	lrc59s\$4gkjee

Pozitivno:

- lozinke su skrivene

# Šifrovanje lozinki

## Šifrovanje

*Šifrovanje* je proces enkodiranja informacija. Tokom šifrovanja originalna reprezentacija informacije (otvoreni tekst) se konvertuje u alternativnu reprezentaciju koja se naziva *šifrat*.

username	rot13(password)
nikola	cnffjbeq1
marko	zngevk
petar	lrc59s\$4gkjee

Pozitivno:

- lozinke su skrivene

Negativno:

# Šifrovanje lozinki

## Šifrovanje

*Šifrovanje* je proces enkodiranja informacija. Tokom šifrovanja originalna reprezentacija informacije (otvoreni tekst) se konvertuje u alternativnu reprezentaciju koja se naziva *šifrat*.

username	rot13(password)
nikola	cnffjbeq1
marko	zngevk
petar	lrc59s\$4gkjee

Pozitivno:

- lozinke su skrivene

Negativno:

- otvoreni tekst + šifrat  $\Rightarrow$  ključ

# Heš funkcija

---

## Heš funkcija

*Heš funkcija* je funkcija koja preslikava podatke proizvoljne veličine u vrednosti fiksirane veličine. Vrednost koju dobijemo primenom heš funkcije zovemo *heš vrednosti* ili *heš*.

username	md5(password)
nikola	7c6a180b36896a0a8c02787eeafb0e4c
marko	21b72c0b7adc5c7b4a50ffcb90d92dd6
petar	47ad898a379c3dad10b4812eba843601

# Heš funkcija

## Heš funkcija

*Heš funkcija* je funkcija koja preslikava podatke proizvoljne veličine u vrednosti fiksirane veličine. Vrednost koju dobijemo primenom heš funkcije zovemo *heš vrednosti* ili *heš*.

username	md5(password)
nikola	7c6a180b36896a0a8c02787eeafb0e4c
marko	21b72c0b7adc5c7b4a50ffcb90d92dd6
petar	47ad898a379c3dad10b4812eba843601

Pozitivno:



# Heš funkcija

## Heš funkcija

*Heš funkcija* je funkcija koja preslikava podatke proizvoljne veličine u vrednosti fiksirane veličine. Vrednost koju dobijemo primenom heš funkcije zovemo *heš vrednosti* ili *heš*.

username	md5(password)
nikola	7c6a180b36896a0a8c02787eeafb0e4c
marko	21b72c0b7adc5c7b4a50ffcb90d92dd6
petar	47ad898a379c3dad10b4812eba843601

Pozitivno:

- heš funkcija nema inverz

# Heš funkcija

## Heš funkcija

*Heš funkcija* je funkcija koja preslikava podatke proizvoljne veličine u vrednosti fiksirane veličine. Vrednost koju dobijemo primenom heš funkcije zovemo *heš vrednosti* ili *heš*.

username	md5(password)
nikola	7c6a180b36896a0a8c02787eeafb0e4c
marko	21b72c0b7adc5c7b4a50ffcb90d92dd6
petar	47ad898a379c3dad10b4812eba843601

Pozitivno:

- heš funkcija nema inverz

Negativno:

# Heš funkcija

## Heš funkcija

*Heš funkcija* je funkcija koja preslikava podatke proizvoljne veličine u vrednosti fiksirane veličine. Vrednost koju dobijemo primenom heš funkcije zovemo *heš vrednosti* ili *heš*.

username	md5(password)
nikola	7c6a180b36896a0a8c02787eeafb0e4c
marko	21b72c0b7adc5c7b4a50ffcb90d92dd6
petar	47ad898a379c3dad10b4812eba843601

Pozitivno:

- heš funkcija nema inverz

Negativno:

- *rainbow* tabele

# Soljenje

## Soljenje

*Soljenje* predstavlja dodavanje nasumičnih podataka ulaznom podatku na kome se primenjuje heš funkcija.

username	salt	sha256(password+salt)
nikola	3]iPP	bbe64abee254782ee5eed1e9e9...
marko	PeRap	9c09e1f111a3f526749099b9da...
petar	E54Fb	f0a92d959e539c9d9711ba77da...

# Soljenje

## Soljenje

*Soljenje* predstavlja dodavanje nasumičnih podataka ulaznom podatku na kome se primenjuje heš funkcija.

username	salt	sha256(password+salt)
nikola	3]iPP	bbe64abee254782ee5eed1e9e9...
marko	PeRap	9c09e1f111a3f526749099b9da...
petar	E54Fb	f0a92d959e539c9d9711ba77da...

Pozitivno:

# Soljenje

## Soljenje

*Soljenje* predstavlja dodavanje nasumičnih podataka ulaznom podatku na kome se primenjuje heš funkcija.

username	salt	sha256(password+salt)
nikola	3]iPP	bbe64abee254782ee5eed1e9e9...
marko	PeRap	9c09e1f111a3f526749099b9da...
petar	E54Fb	f0a92d959e539c9d9711ba77da...

Pozitivno:

- *rainbow* tabele ne funkcionišu

# Soljenje

## Soljenje

*Soljenje* predstavlja dodavanje nasumičnih podataka ulaznom podatku na kome se primenjuje heš funkcija.

username	salt	sha256(password+salt)
nikola	3]iPP	bbe64abee254782ee5eed1e9e9...
marko	PeRap	9c09e1f111a3f526749099b9da...
petar	E54Fb	f0a92d959e539c9d9711ba77da...

Pozitivno:

- *rainbow* tabele ne funkcionišu

Negativno:

# Soljenje

## Soljenje

*Soljenje* predstavlja dodavanje nasumičnih podataka ulaznom podatku na kome se primenjuje heš funkcija.

username	salt	sha256(password+salt)
nikola	3]iPP	bbe64abee254782ee5eed1e9e9...
marko	PeRap	9c09e1f111a3f526749099b9da...
petar	E54Fb	f0a92d959e539c9d9711ba77da...

Pozitivno:

- *rainbow* tabele ne funkcionišu

Negativno:

- brzo računanje heš vrednosti (napad rečnikom)



# Dodatna poboljšanja

---

- Biber tehnika (dodajemo nasumični podatak pri heširanju koji je zajednički za sve korisnike)
- Heširanje u iteracijama (nekoliko puta primenjujemo heš funkciju)
- Spajanje više tehnika (so + biber + heš funkcija u iteracijama)
- bcrypt[Pravos and Mazieres, 1999]

# Menadžer lozinki

---

## Ključno zapažanje

Kako broj usluga raste na Internetu, broj lozinki koje prosečan čovek treba da upamti raste respektivno, sve do trenutka kada mnogi ljudi ne mogu da upamte novu i jaku lozinku.

Korisnici rešavaju ovaj problem na dva načina:

- Koriste istu lozinku za različite sajtove.
- Koriste *menadžer lozinki*.

# Menadžer lozinki

---

## Ključno zapažanje

Kako broj usluga raste na Internetu, broj lozinki koje prosečan čovek treba da upamti raste respektivno, sve do trenutka kada mnogi ljudi ne mogu da upamte novu i jaku lozinku.

Korisnici rešavaju ovaj problem na dva načina:

- Koriste istu lozinku za različite sajtove.
- Koriste *menadžer lozinki*.

## Menadžer lozinki

*Menadžer lozinki* je program koji korisnicima pruža mogućnost čuvanja, generisanja, i menadžment lozinki za lokalne aplikacije ili Internet usluge.

# Šta menadžer lozinki čini sigurnijim?

---

## A.1 Prednosti otvorenog kôda

- korisnici mogu prijaviti ranjive delove
- smanjuje se pritisak na programere

## A.2 Mane otvorenog kôda

- neće svi korisnici prijaviti ranjive delove

## B.1 Prednosti zatvorenog kôda

- potencijalna eksploatacija ranjivosti je smanjena

## B.2 Mane zatvorenog kôda

- korisnik mora verovati kompaniji
- manji broj ljudi radi reviziju koda

# Teorijski dizajn dobrog menadžera lozinki

---

[Luevanos, Elizarraras, Hirschi, and Yeh, 2017] preporučuju:

# Teorijski dizajn dobrog menadžera lozinki

---

[Luevanos, Elizarraras, Hirschi, and Yeh, 2017] preporučuju:

1. Prioritet je sigurnost, a ne slučajevi upotrebe.

# Teorijski dizajn dobrog menadžera lozinki

---

[Luevanos, Elizarraras, Hirschi, and Yeh, 2017] preporučuju:

1. Prioritet je sigurnost, a ne slučajevi upotrebe.
2. Otvorenog kôda.

# Teorijski dizajn dobrog menadžera lozinki

---

[Luevanos, Elizarraras, Hirschi, and Yeh, 2017] preporučuju:

1. Prioritet je sigurnost, a ne slučajevi upotrebe.
2. Otvorenog kôda.
3. Master lozinka mora biti snažna, tj. mora da zadovoljava 2017 NIST standard.[NIST 800-63A]



# Teorijski dizajn dobrog menadžera lozinki

---

[Luevanos, Elizarraras, Hirschi, and Yeh, 2017] preporučuju:

1. Prioritet je sigurnost, a ne slučajevi upotrebe.
2. Otvorenog kôda.
3. Master lozinka mora biti snažna, tj. mora da zadovoljava 2017 NIST standard.[NIST 800-63A]
4. Funkcionalnost automatskog popunjavanja, zbog *keylogger*-a.

# Teorijski dizajn dobrog menadžera lozinki

---

[Luevanos, Elizarraras, Hirschi, and Yeh, 2017] preporučuju:

1. Prioritet je sigurnost, a ne slučajevi upotrebe.
2. Otvorenog kôda.
3. Master lozinka mora biti snažna, tj. mora da zadovoljava 2017 NIST standard.[NIST 800-63A]
4. Funkcionalnost automatskog popunjavanja, zbog *keylogger*-a.
5. Samozaključavanje nakon nekog vremena.

# CTF: Capture The Flag

---

## CTF (Capture The Flag)

**CTF** je specijalna vrsta takmičenja u oblasti računarske bezbednosti. Cilj takmičenja je osvojiti što više *flag*-ova, tako što timovi pronalaze rupe u sistemu, koje onda eksploatišu. *Flag* je obično oblika `FLAG{neki_tekst}`

# Vrste CTF-ova

---

- **Jeopardy:** Timovi rešavaju unapred zadate zadatke.
- **Attack-Defense:** Dva tima pokušavaju da eksploatišu jedni druge, dok u isto vreme pokušavaju da se zaštite od napada.
- **Mixed:** Varijacije na temu. (na primer: wargames).

# Vrste CTF zadataka

---

- crypto (Kriptografija)

# Vrste CTF zadataka

---

- crypto (Kriptografija)
- rev (Obrnuto inženjerstvo)

# Vrste CTF zadataka

---

- crypto (Kriptografija)
- rev (Obrnuto inženjerstvo)
- pwn (Osvojiti pristup)

# Vrste CTF zadatka

---

- crypto (Kriptografija)
- rev (Obrnuto inženjerstvo)
- pwn (Osvojiti pristup)
- stego (Steganografija)



# Vrste CTF zadatka

---

- crypto (Kriptografija)
- rev (Obrnuto inženjerstvo)
- pwn (Osvojiti pristup)
- stego (Steganografija)
- web (Eksploatacija veb aplikacija)

# Vrste CTF zadatka

---

- crypto (Kriptografija)
- rev (Obrnuto inženjerstvo)
- pwn (Osvojiti pristup)
- stego (Steganografija)
- web (Eksploatacija veb aplikacija)
- misc (Razno)

# Vrste CTF zadatka

---

- crypto (Kriptografija)
- rev (Obrnuto inženjerstvo)
- pwn (Osvojiti pristup)
- stego (Steganografija)
- web (Eksploatacija veb aplikacija)
- misc (Razno)
- hardware (Eksploatacija hardvera)

# Vrste CTF zadatka

---

- crypto (Kriptografija)
- rev (Obrnuto inženjerstvo)
- pwn (Osvojiti pristup)
- stego (Steganografija)
- web (Eksploatacija veb aplikacija)
- misc (Razno)
- hardware (Eksploatacija hardvera)
- ...

# Reference

---



Sirapat Boonkrong (2012)

Security of Passwords

*Information Technology Journal* 8(2), 112 – 117



Vaadata (2020)

How to Securely Store Passwords in Database?

*Vaadata blog article*



Niels Prayos and David Mazieres (1999)

A Future-Adaptable Password Scheme

*In Proceedings of 1999 USENIX Annual Technical Conference* 81 – 92



Ah Kioon, Mary Cindy and Wang, Zhao Shun and Deb Das, Shubra (2013)

Security Analysis of MD5 Algorithm in Password Storage

Instruments, Measurement, Electronics and Information Engineering, *Trans Tech Publications Ltd* 347(10), 2706 – 2711

# Reference

---



C. Luevanos, J. Elizarraras, K. Hirschi and J. Yeh (2017)

Analysis on the Security and Use of Password Managers

*18th International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT)*, 17 – 24



Paul A. Grassi, James L. Fenton, Naomi B. Lefkovitz, Yee-Yin Choong, Jamie M. Danker, Mary F. Theofanos (2017)

Digital Identity Guidelines: Enrollment and Identity Proofing Requirements

*NIST Special Publication 800-63A*

# Reference

---



## CTFtime

All about CTF (Capture The Flag)

*[ctftime.org](https://ctftime.org)*



## OverTheWire

We're hackers, and we are good-looking. We are the 1%.

*[overthewire.org](https://overthewire.org)*

**I šta ćemo sad?**



# I šta ćemo sad?

`https://capturetheflag.withgoogle.com`