Autentifikacija i autorizacija

Informaciona bezbednost

FAKULTET TEHNIČKIH NAUKA

V5

Sadržaj

- Autentifikacija
- Lozinka (Hash+Salt)
- Kontrola pristupa - autorizacija
- Json Web Token
- Zadaci

Autentifikacija

Autentifikacija pokušava da identifikuje identitet korisnika i da li je korisnik zapravo osoba koju predstavlja

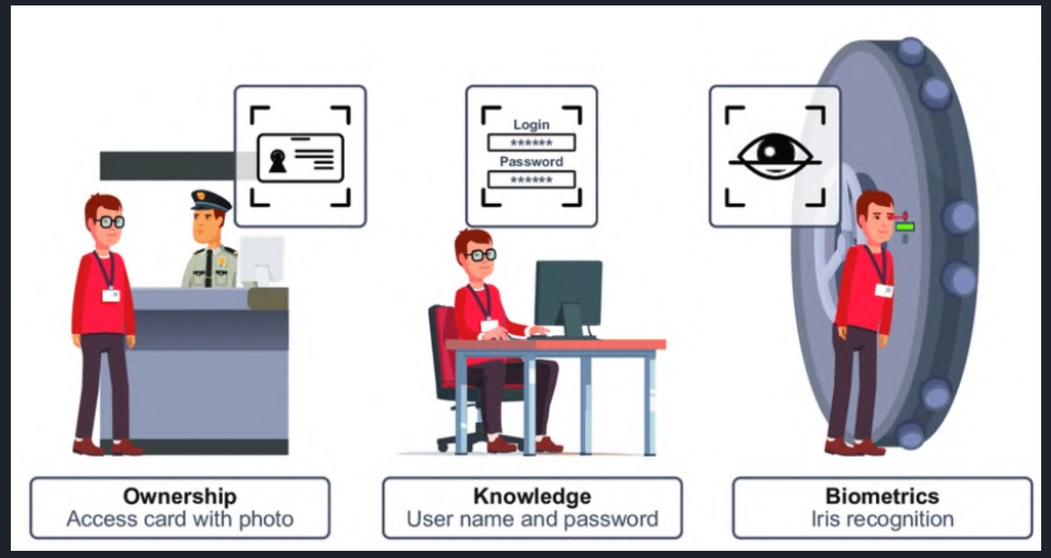
Identitet možemo da potvrdimo na osnovu nečega što znamo, posedujemo ili na osnovu ličnih karakteristika

U veb aplikacijama, koji je osnovni način potvrde identiteta?

Autentifikacija

Autentifikacija identiteta se može ostvariti na četiri načina:

- Nešto što znam (lozinka)
- Nešto što imam (tokeni - fizički ključevi, smart kartice)
- Nešto što jesam (statička biometrija - otisak prsta, lica, irisa)
- Nešto što radim (dinamička biometrija - prepoznavanje glasa, potpisa)



Lozinka

Prilikom potvrde identiteta uglavnom se koristi neka lozinka

- Minimalna dužina lozinke- progress bar koji pokazuje jacinu lozinke
- Karakteri koji moraju da se pojave
- Crna lista dobro poznatih lozinki

Kako skladištimo lozinku?

ODNOS POTREBE ZA BEZBEDNOSCU I OPTERECENJA KORISNIKA?

Hash & salt

Koje su osobine hash funkcije?

Sta ako Pera i ja imamo istu lozinku?

Gde se čuva salt?

hash(lozinka+salt)

Kontrola pristupa - autorizacija

Kontrola pristupa je osnovni element bezbednosti koji formalizuje ko može da pristupi određenim aplikacijama, podacima i resursima i pod kakvim uslovima.

Prilikom registracije svakom korisniku biva dodeljena uloga u sistemu.
Svaka uloga ima prava pristupa.
Prava pristupa predstavljaju resurse koji mogu da se vide i kojima može da se upravalja.
Pristup resursu odeđuje da li će osoba koja je poslala HTTP zahtev moći da pristupi određenom podatku.
Korisnik može imati vise uloga, a za jednu ulogu može biti vezano vise permisija.

RBAC (engl. Role Based Access Control)

Uloge, poznate i kao „kontrola pristupa zasnovana na ulogama“, uobičajeni su način da se pojednostavi logika autorizacije i za inženjere i za korisnike.

Uloga je način za grupisanje dozvola. Kada se korisniku dodeli uloga, korisnik dobija svaku dozvolu koju ta uloga ima.

Dozvola je radnja koju korisnik može da preduzme na resursu.

Json Web Token

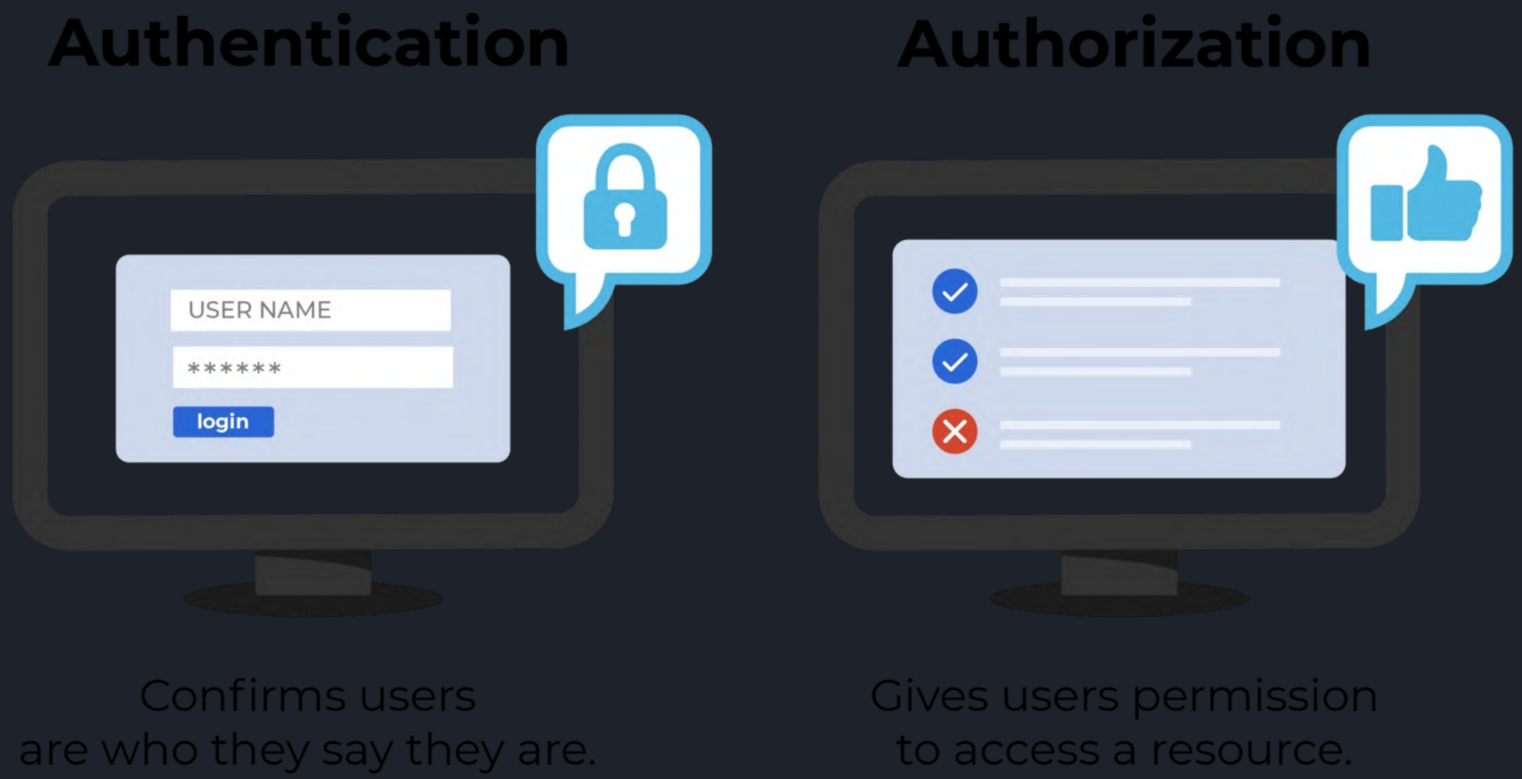
JSON objekat za bezbedan prenos informacija

- podaci su bezbedni zato sto su digitalno potpisani
- nakon što se korisnik uspešno prijavi na sistem generiše mu se token koji će koristiti u narednom zahtevu

Tri Base64-URL enkodovana stringa, razdvojena tackom

https://jwt.io/

Autentifikacija vs Autorizacija



Autentifikacija vs Autorizacija

Autentifikacija

- Određuje da li su korisnici oni za koje tvrde da jesu.
- Izaziva korisnika da potvrdi akreditive.
- Obično se radi pre autorizacije.
- Zaposleni u kompaniji moraju da se autentifikuju preko mreže pre nego što pristupe imejlu svoje kompanije

Autorizacija

- Određuje čemu korisnici mogu, a čemu ne mogu da pristupe.
- Proverava da li je pristup dozvoljen putem smernica i pravila.
- Obično se radi nakon uspešne autentifikacije.
- Nakon što se zaposleni uspešno autentifikuje, sistem određuje kojim informacijama je dozvoljen pristup

Zadaci

1. Šta biste radili nakon nekoliko neuspešnih prijava?
2. Čemu služi aktivacija naloga?
3. Oporavak naloga: pitanja bazirana na znaju?
4. Da li treba ograničiti trajanje lozinki?