# Opis slučaja korištenja

## Ime

Autentifikacija i autorizacija

## Cilj

Omogućiti korisnicima proces autentifikacije na sustav tj. prijavljivanje na sustav. Nakon što korisnik bude prijavljen na sustav potrebno ga je autorizirati tj. dodijeliti mu određene privilegije za korištenje sustava.

## Tim odgovoran za slučaj korištenja

Tim za razvoj backend-a i baze

Tim za razvoj frontenda-a

## Preduvjeti

* Baza koja za svakog korisnika sprema njegovu rolu u sustavu
* Mogućnost autorizacije korisnika na način da „login“ ruti pošalje svoje korisničko ime i lozinku
* Backend rute zaštićene i dostupne samo korisnicima čiji zahtjevi za dohvat tih ruta su ispravno autorizirani
* Frontend stranica preko koje se korisnici mogu uspješno autentificirati i autorizirati za korištenje zaštićenih backend ruta

## Stanje nakon slučaja korištenja

Autoriziran korisnik koji dobiva mogućnosti korištenja funkcionalnosti sustava koje su dostupne samo korisnicima sa njegovom rolom

## Ograničenja i rizici

Napadač može pokušati provaliti lozinku korisnika na način da se pokušava prijaviti sa ogromnim brojem kombinacija lozinki.

## Okidači događaja

Korisnik unosi svoje korisničko ime i lozinku i šalje zahtjev za prijavu na sustav

## Primarni sudionik

Korisnik

## Sporedni sudionik odnosno sudionici

Zaposlenik i administrator

# Imena putova slučaja korištenja

## Primarni put

Korisnik unosi ispravno korisničko ime i lozinku, zatim se uspješno prijavljuje na sustav.

## Alternativni putovi

* Korisnik unosi pogrešne podatke za prijavu, može pokušati ponovno
* Korisnik premaši broj mogućih pokušaja prijava za svoje korisničko ime
* Ukoliko se korisnik ne sječa svoje lozinke, može je resetirati putem email-a, ovu opciju može pozvati i nakon što premaši broj mogućih prijava

## Putovi u slučaju iznimke

* Sustav nije dostupan
* Korisnikov račun je iz nekog razloga suspendiran

# Detalji slučaja korištenja

## Ime puta

Primarni put – uspješna autentifikacija i autorizacija korisnika

### Okidač događaja

Korisnik unosu korisničko ime i lozinku i šalje zahtjev za prijavu

### Osnovi slijed koraka

* Korisnik šalje zahtjev za prijavu, u zahtjevu šalje svoje korisničko ime i lozinku
* Server provjerava da li u sustavu postoji korisnik sa datim korisničkim imenom
* Ako postoji, sustav provjerava da li je poslana lozinka također ispravna za tog korisnika
* Ako jeste server autorizira korisnika tj. korisnik dobiva mogućnosti korištenja sustava sukladne njegovoj roli.

### Poslovna pravila

Korisnik za dato korisničko ime ima određeni broj pokušaja za prijavu (8). Ako se korisnik za redom ne uspije prijaviti u datom broju pokušaja, njegov račun biva privremeno zaključan od prijava. Korisnik može kontaktirati službu i riješiti ovaj problem.

### Ograničenja i rizici

Korisnik ima određeni broj pokušaja da unese ispravne podatke za prijavu. Napadač može pokušati „pogoditi“ podatke nekog drugog korisnika.

## Ime puta

Alternativni put – korisnik unosi pogrešne podatke za prijavu

### Okidač događaja

Korisnik se pokuša prijaviti na sustav sa korisničkim imenom koje ne postoji ili netočnom lozinkom.

### Osnovi slijed koraka

* Korisnik šalje zahtjev za prijavu, u zahtjevu šalje korisničko ime i lozinku
* Server provjerava da li u sustavu postoji korisnik sa datim korisničkim imenom
* Ako postoji, sustav provjerava da li je poslana lozinka također ispravna za tog korisnika
* Ukoliko dati korisnik ne postoji ili poslana lozinka nije ispravna, server korisniku šalje informaciju o neuspješnoj prijavi
* Korisnik može pokušati ponovno

### Poslovna pravila

Korisnik ima određeni broj pokušaja za prijavu, ukoliko za redom premaši taj broj pokušaja, njegov račun se suspendira na određeno vrijeme. Korisnik može kontaktirati službu i riješiti ovaj problem.

### Ograničenja i rizici

Napadač može pokušati „pogoditi“ podatke nekog drugog korisnika ili sam korisnik može pokušati previše puta sa prijaviti sa pogrešnim podacima, čime se zaključava njegov račun

# Tehničke informacije o slučaju korištenja

## Prioriteti

Prioritet i ispravna implantacija ovog dijela sustava su od ključne važnosti. Od ovog dijela sustava ovisi sigurnost aplikacije.

## Performanse

Proces autentifikacije i autorizacije bi trebao biti jako brz (u najgorem slučaju 3-4 sekunde).

## Učestalost

Svaki put kada korisnik želi pristupati svom korisničkom računu. To može biti i nekoliko puta dnevno.

## Korisničko sučelje

Sučelje treba biti jednostavno i intuitivno za korištenje (podrazumijeva standardno sučelje za prijavu kakvo se viđa na drugim sustavima). Polja za unos korisničkog imena i lozinke kao i dugme za prijavu.