7. Laboratorijska vježba iz "Web aplikacija u Javi"

7.1. Korištenje Spring Security frameworka

Svrha laboratorijske vježbe je upoznavanje je sa Spring Security frameworkom kroz dodavanje prijave korisnika u aplikaciju.

7.2. Zadatak

Potrebno je izmijeniti postojeću Java web aplikaciju tako da se ograniči pristup aplikaciji dok se korisnik ne prijavi. Upute se odnose na Spring Boot projekt ako nije drugačije navedeno.

1. Dodati potrebne ovisnosti u pom.xml datoteku kako je prikazano na predavanjima / auditornim vježbama.

2. U „schema.sql" datoteku dodati DDL naredbe za tablicu „korisnik" i „grupaKorisnika" zapisa te dodati „many-to-many" tablicu koja povezuje usere s authorityima. Tablica „user" treba imati kolone „id", „korisnickoIme", „lozinka", „ime" i „prezime". Tablica „grupaKorisnika" treba imati kolone „id" i „naziv".

3. U „data.sql" datoteku dodati DML naredbe za nove tablice definirane u prethodnom koraku. U „grupaKorisnika" tablicu treba unijeti vrijednosti "ROLE_ADMIN" i "ROLE_USER". U „korisnik" tablicu je potrebno unijeti barem dva korisnika. Jednog s ADMIN rolom i jednog s USER rolom. Lozinke trebaju biti enkriptirane Bcrypt algoritmom.

4. Referencirati datoteku Primjer implementacije JWT access refresh tokena dostupnu na stranicama kolegija. Ova datoteka sadržava sve implementacijske klase vezane uz rad Spring Security frameworka s JWT standardom. Prilagoditi nazive paketa da odgovaraju onima u projektu.

5. U „application.properties" datoteku dodati jwt.token-validity-seconds i jwt.base64-secret sa pripadnim vrijednostima.

6. Implementirati dohvat trenutačno prijavljenog korisnika prema korisničkom imenu i izložiti pristup na putanji "localhost:8080/api/user/current-user". Slobodno koristiti metode iz „SecurityUtils" klase dostupne u „security" packageu.

7. Obavezno napraviti KorisnikDTO za korisnika. On mora imati polja „id", „korisnickoIme", „ime", „prezime" i „grupe". Polje „grupe" treba biti set String vrijednosti naziva rola koje korisnik ima.

8. Doraditi i vlastitu Angular aplikaciju. Obratiti pozornost na DTO i command objekte.

   DTO za Review treba imati field „korisnickoIme" kako bi se znalo koji korisnik je napisao review. Samo korisnik sa rolom ADMIN smije brisati review za Restoran. Korisnici-i sa rolom USER smiju upisati maksimalno jedan review po restoranu i raditi izmjene samo na review koji su oni napisali.

9. Pripaziti na izložene putanje spring boot aplikacije.

10. Implementirati Spring Security konfiguraciju tako da daje pristup samo autentificiranim korisnicima. Autentifikacija korisnika se treba odvijati na putanji "localhost:8080/api/authenticate" koja je izložena u 4. koraku s LoginController klasom.

¶