Univerzitet u Sarajevu

Elektrotehnički fakultet

Računarstvo i informatika

**Praktikum - Napredne Web Tehnologije**

**Projektna dokumentacija**

Ragib Smajić

1122/16668

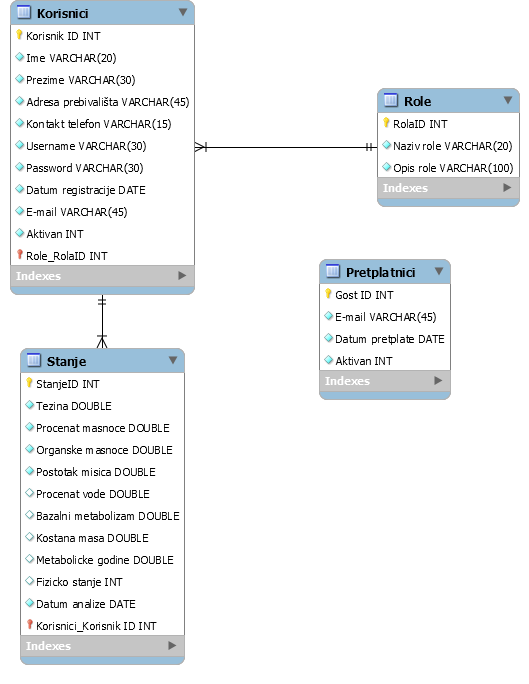
**Zadatak 1**

Jedan od modula koji je sastavni dio aplikacije jeste modul za korisnike. Moj zadatak je bio da u oviru zadatka 1 kreiram isti, odnosno da stavke zadatka 1 realiziram kroz modul za korisnike.

Modul za korisnike je jedan od mikroservisa koji se sastoji od 4 entiteta:

* Korisnik
* Pretplatnik
* Stanje
* Rola

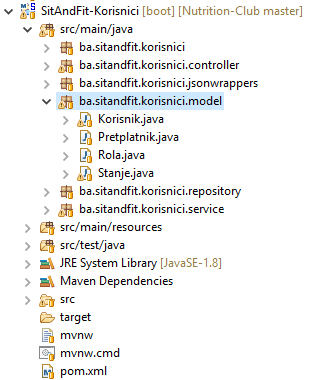
Na sl. 1 je prikazan ER dijagram za pomenuti modul i entitete.



Sl. 1. ERD – Modul za korisnike

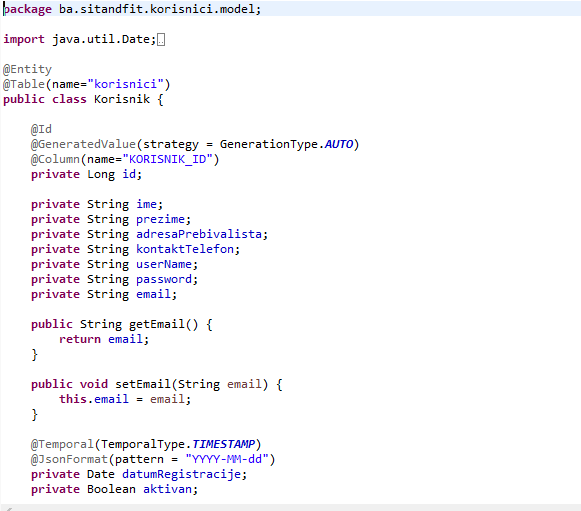
Modul za korisnike komunicira sa modulom za proizvode preko REST servisa koje nudi modul za proizvode.

U Spring Tool Suite (STS) kreirao sam novi Spring Starter Project, koji sam nazvao SitAndFit-Korisnici. U projektu sam kreirao paket model, koji sadži klase koje predstavljaju gore navedene entitete. To je prikazano na slici 1.1.



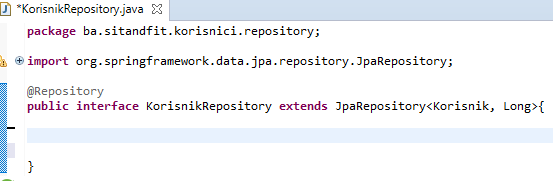
Sl. 1.1. Modeli (Entititeti)

Kako je rađen Code first pristup, odnosno entiteti u bazi podataka se generišu na osnovu kreiranih modela, bilo je potrebno modele označiti odgovarajućim anotacijama. To je urađeno za sve klase model paketa, a na slici 1.2 je prikazana klasa Korisnik.

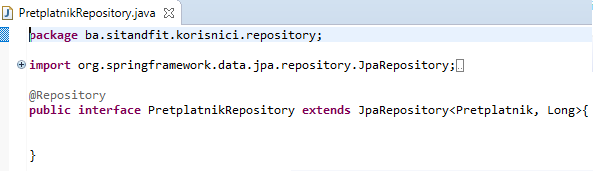


Sl. 1.2 Korisnik klasa sa odgovarajućim anotacijama

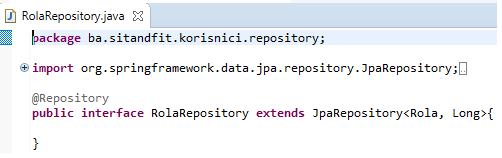
Za svaki od entiteta kreiran je interfejs koji proširuje JpaRepository interfejs, čija implementacija se kreira automatski prilikom builda aplikacije, a koji služi za komunikaciju sa bazom podataka. Na slikama 1.3.1, 1.3.2, 1.3.3 i 1.3.4 su prikazani interfejsi koji predstavljaju specifikaciju za repozitorij koji će biti kreiran automatski.



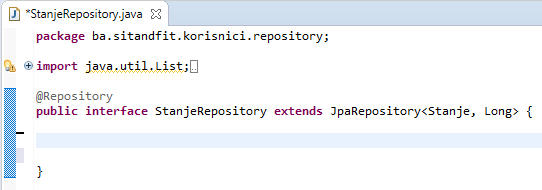
Sl. 1.3.1 KorisnikRepository za korisnike



Sl. 1.3.2 PretplatnikRepository za pretplatnike



Sl. 1.3.3 RolaRepository za role

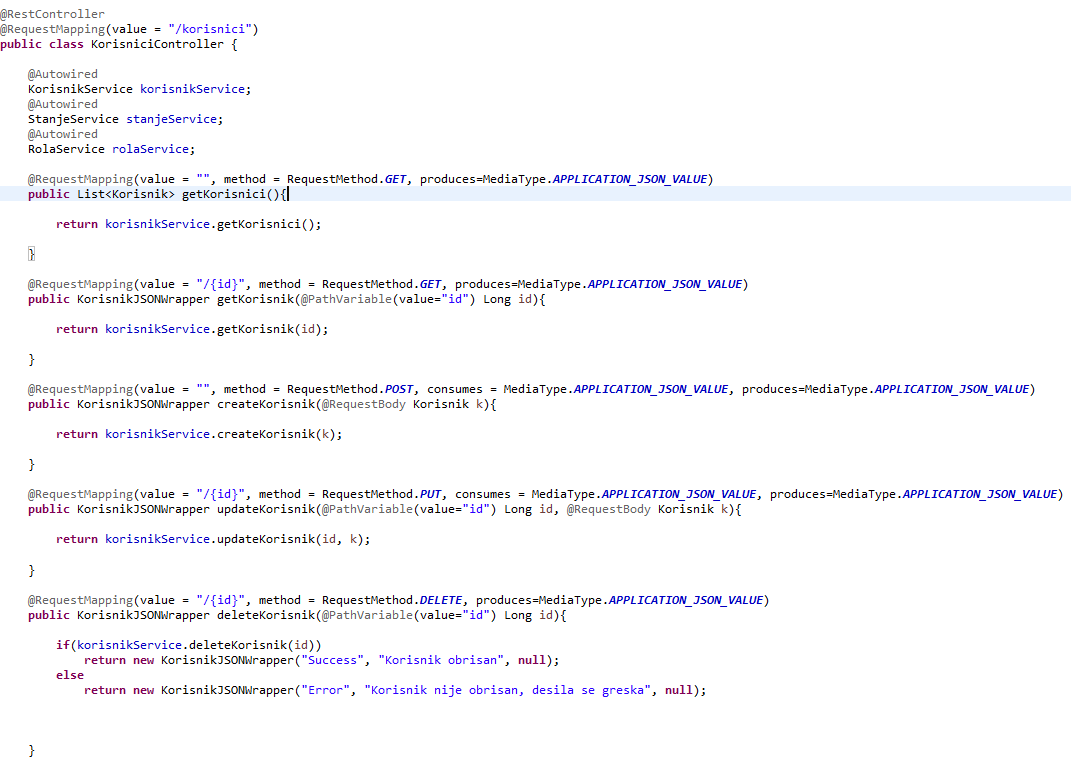


Sl. 1.3.4 StanjeRepository za stanja korisnika

Kako JpaRepository posjeduje osnovne metode za kreiranje, ažuriranje, pretraživanje i brisanje korisnika, čija implementacija će biti kreirana automatski, potrebno je kreirati kontrolere koji će omogućavati osnovne CRUD operacije.

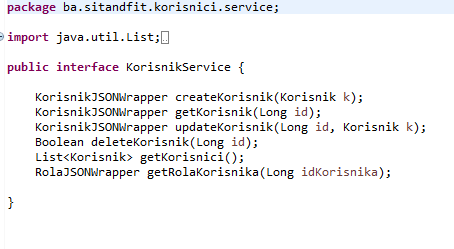
Za svaki od entiteta kreiran je kontroler koji omogućava pristup entitetima na koje se odnosi i za svaki od entiteta kreiran je Service layer koji sadrži svu biznis logiku.

Na slici 1.4 je prikazan kontroler koji na URI „/korisnici“ omogućava pristup resursu korisnicima i pruža osnovne CRUD operacije.



Sl. 1.4 Korisnici kontroler – Osnovne CRUD operacije

Kako kontroler ne bi bio pretrpan kodom koji predstavlja biznis logiku kreiran je layer Service koji enkapsulira istu. Zbog toga se u kontroleru samo poziva odgovarajuća metoda service layer-a, u ovom slučaju klase KorisnikService. KorisnikService (Sl. 1.5) je interfejs koji prestavlja specifikaciju metoda koje konkretna implementacija mora da podrži, te je stoga bilo potrebno kreirati konkretnu implementaciju interfejsa KorisnikService. To je urađeno klasom KorisnikServiceImpl koja je prikazana na slici 1.6.



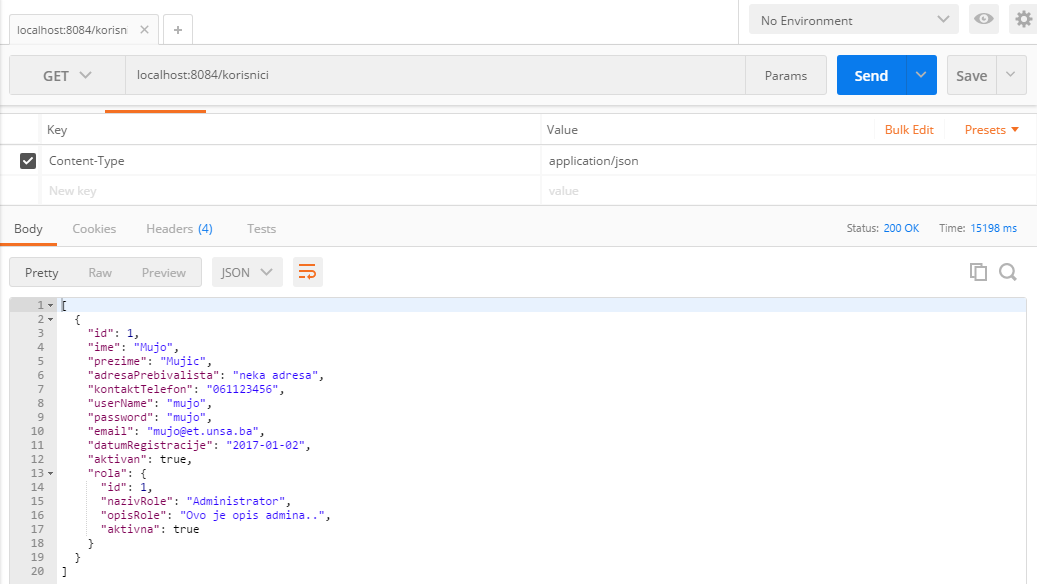
Sl .15 KorisnikService interjefs



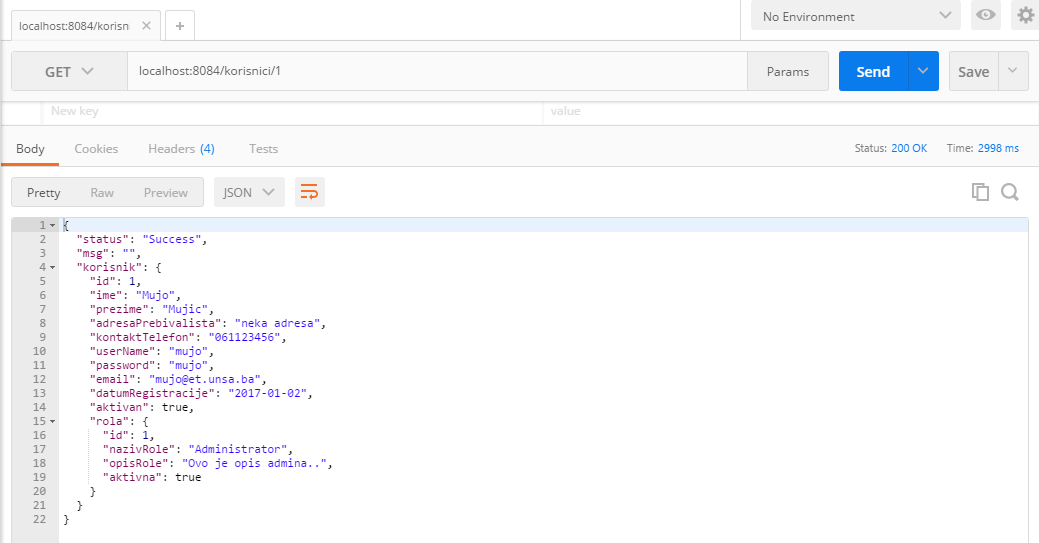
Sl. 1.6 KorisnikServiceImpl

Kreirana klasa (KorisnikServiceImpl) koristi usluge KorisnikRepository-a za dobavljanje podataka iz baze, čija implementacija je automatski kreirana i dodijeljena varijabli korisnikRepository, a pruža usluge klasi KorisnikController. Na taj način se obradi određeni zahtjev korisnika na URI „/korisnici“.

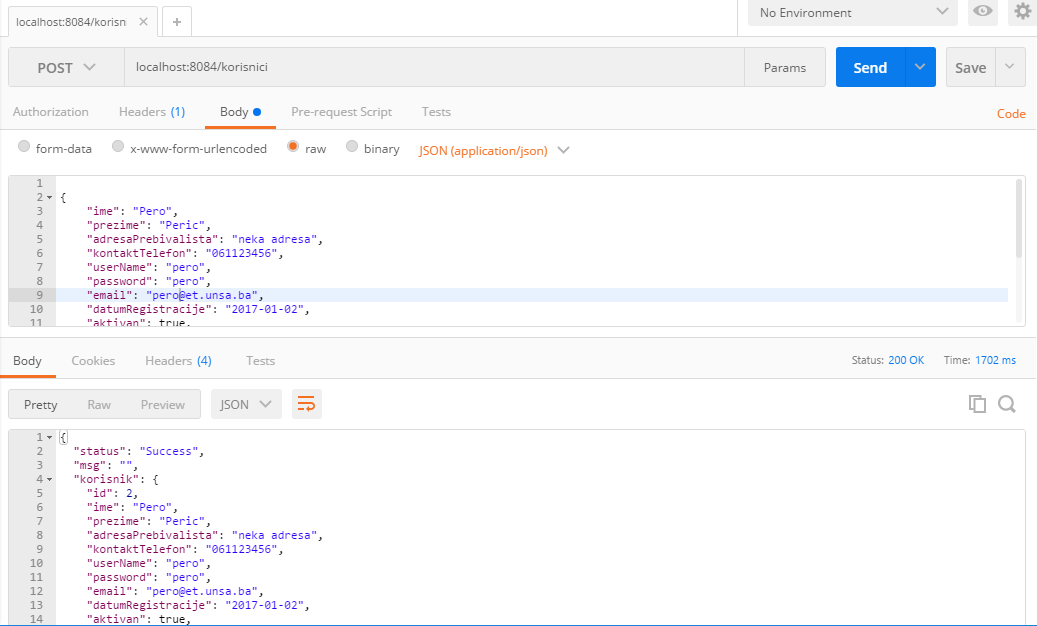
Na slikama 1.7.1, 1.7.2, 1.7.3, 1.7.4 i 1.7.5 su prikazani pozivi upućeni servisu „/korisnici“ u okviru aplikacije Postman.



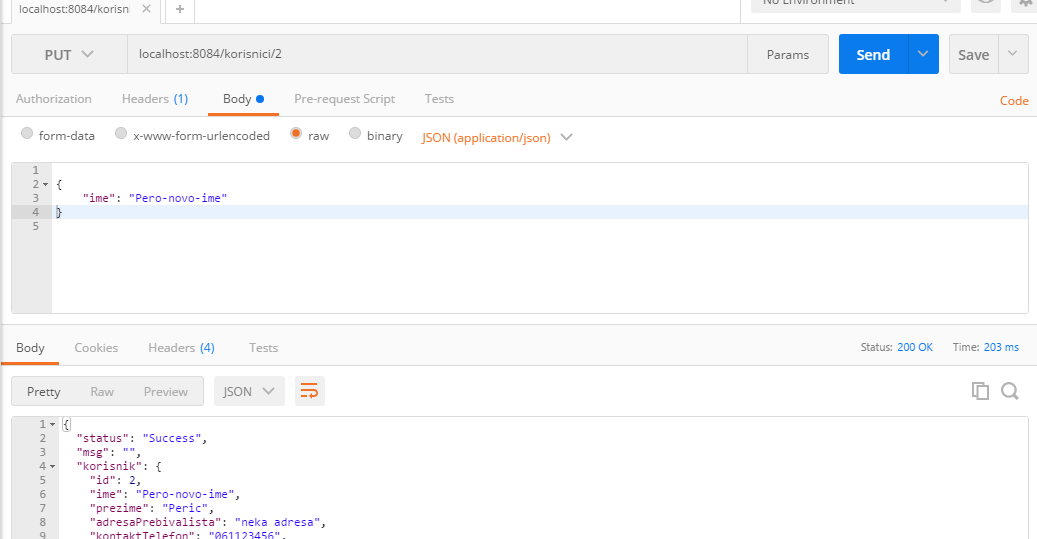
Sl. 1.7.1 GET zahtjev na /korisnici koji vraća sve korisnike iz baze



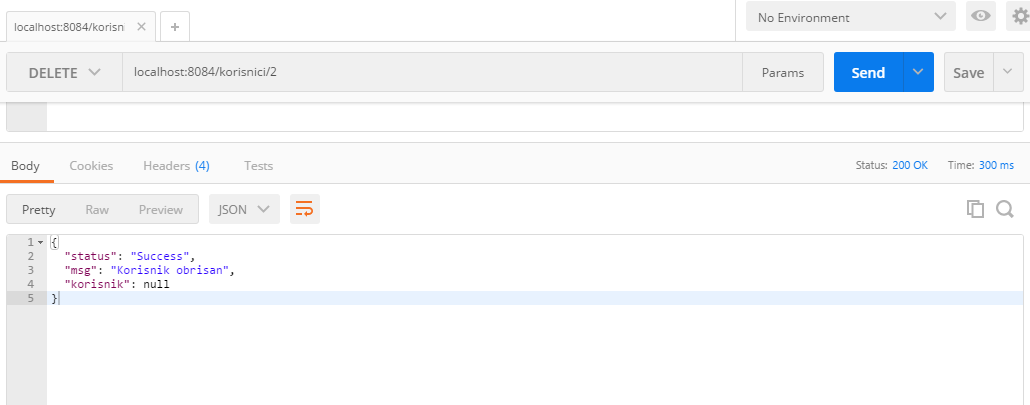
Sl. 1.7.2 GET zahtjev na /korisnici/{id} koji vraća korisnika sa proslijeđenim id-em



Sl. 1.7.3 POST zahtjev na /korisnici za kreiranje novog korisnika



Sl. 1.7.4 PUT zahtjev na /korisnici/{id} za update imena korisnika Pero



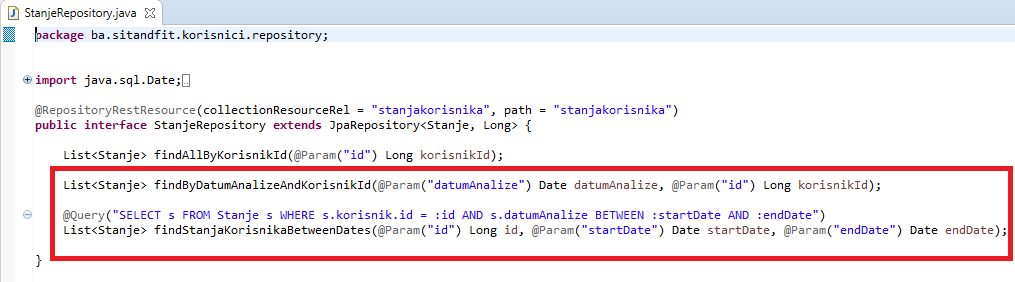
Sl. 1.7.5 DELETE zahtjev na /korisnici/{id} – Brisanje korisnika

Na isti način su realizirani end point servisi i za ostale entitete, odnosno za entitete Rola, Pretplatnik i Stanje.

**Zadatak 2**

Dvije metode koje su izabrane za implementaciju u okviru mikroservisa za korisnike su metoda koja stanja korisnika na određeni datum analize tijela korisnika i metoda koja daje stanja korisnika između proizviljna dva datuma.

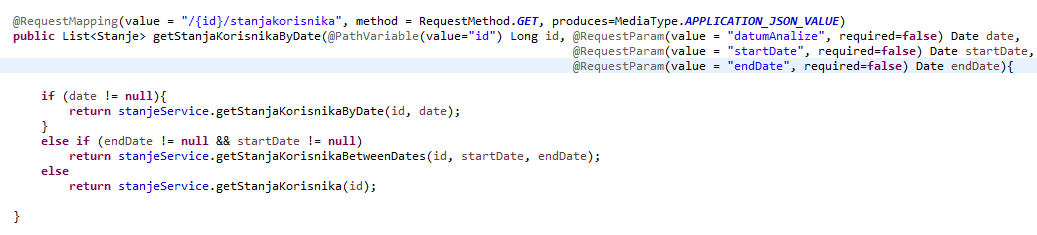
Na slici 2.1 su prikazane navedene metode (metode u crvenom pravougaoniku) u okviru repositorija, odnosno u oviru interfejsa StanjeRepository.



Sl. 2.1 Metode u okviru StanjeRepository interfejsa

Naravno, kako bi se imao pristup metodama preko http-a kreiran je odgovarajući kontroler u KorisnikController klasi, kao i odgovarajuće metode u StanjeService interfejsu.

Kontroler koji je zadužen za ove zahtjeve je prikazan na slici 2.2

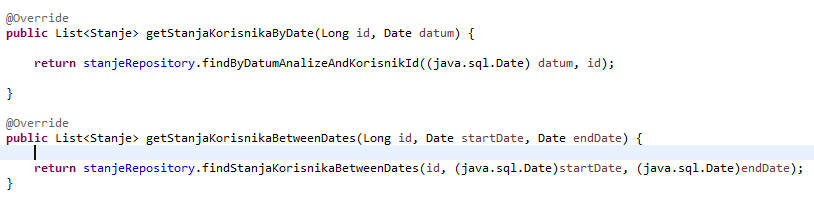


Sl. 2.2 Prikaz kontrolera

Kontroler zahtjeva kao PathVarijablu id korisnika i omogućava da se proslijede 3 dodatna URL parametra na osnovu kojih se odlučuje koja metoda StanjeService-a će se pozvati.

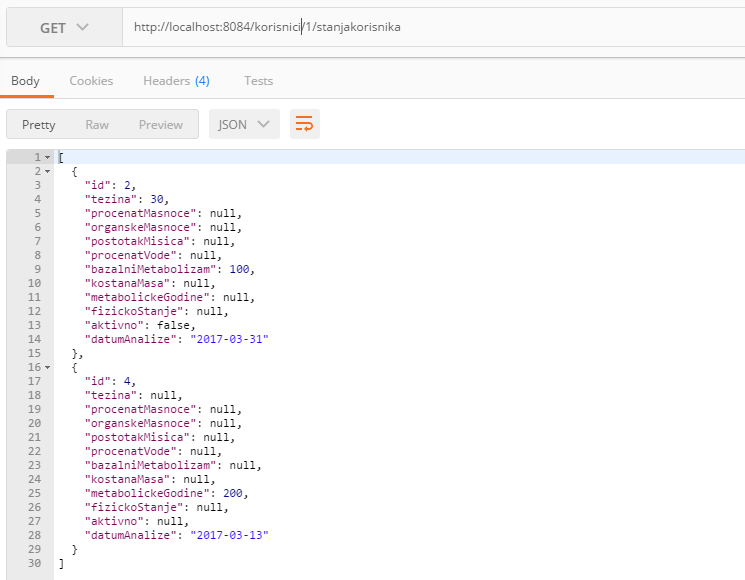
Ako se proslijedi paramterat date, poziva se metoda koja vraća stanja korisnika koja su zabilježena određenog datuma, ako se proslijede 2 parametra startDate i endDate poziva se metoda koja vraća stanja korisnika koja su zabilježena između tih datuma i ako se ne proslije nijedan parametar vraćaju se sva stanja korisnika.

Na slici 2.3 su prikazane metode klase StanjeServiceImpl koje su posrednik izmeđi kontrolera i metoda repozitorija.

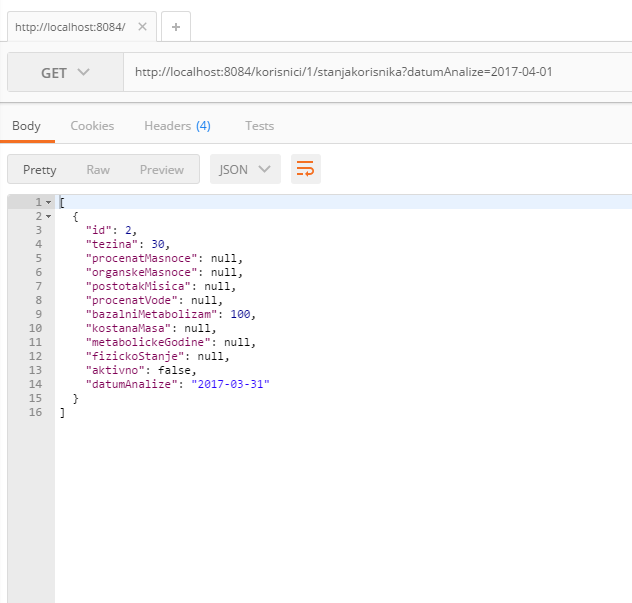


Sl. 2.3 Metode u StanjeServiceImpl – Implementacija StanjeService interfejsa

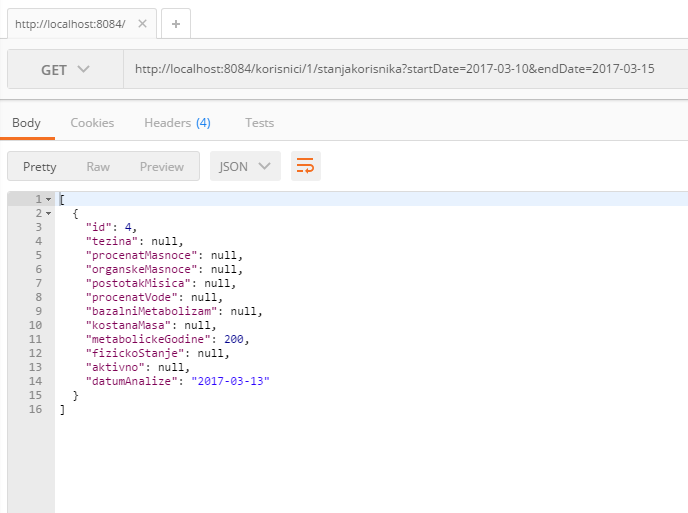
Na slici 2.4.1 je prikazan odziv kada se traže sva stanja korisnika sa id-em 1, na slici 2.4.2 kada se traže stanja na određeni datum i na slici 2.4.3 kada se traže stanja između datuma



Sl.2.4.1 Izlistavanje svih stanja korisnika sa id = 1



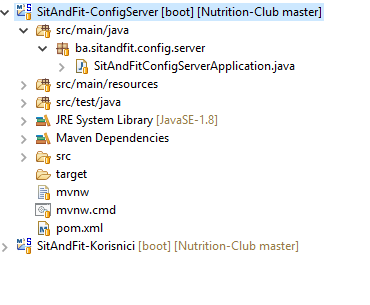
Sl. 2.4.2 Izlistavanje stanja na određeni datum



Sl. 2.4.3 Izlistavanje stanja između datuma

Pored kreiranja dodatne dvije metode u oviru mikroservisa za korisnike, zadatk mi je bio kreirati Spring Cloud Configuration Server, omogućiti osnovnu zaštitu putem autentifikacije i enkripciju konfiguracije.

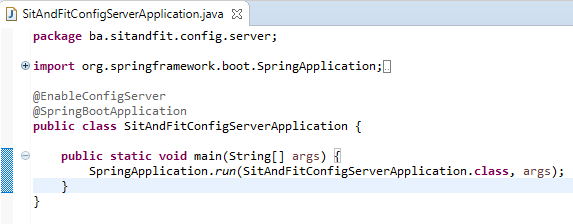
Prije svega bilo je potrebno napraviti novi Spring Boot Starter projekat koji sam nazvao SitAndFit-ConfigServer. To je prikazano na slici 2.5.



Sl. 2.5 Prikaz projekta za Config Server

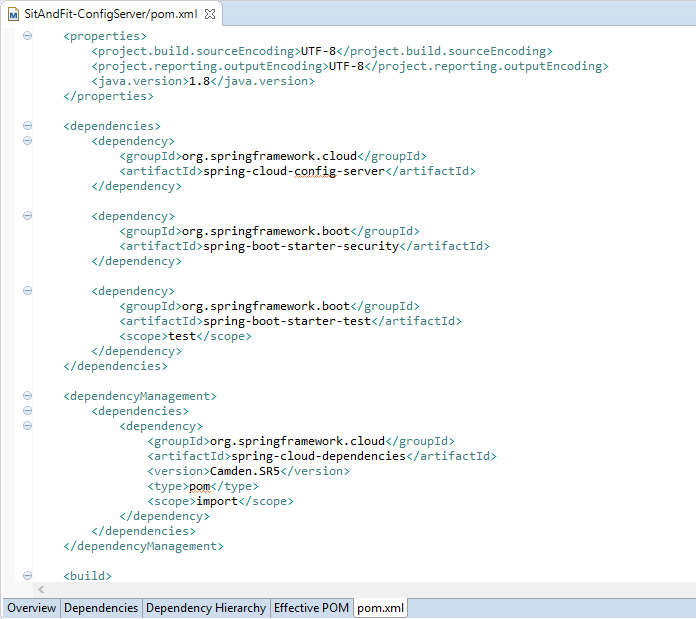
Kako bi se Spring Boot aplikacija ponšala kao konfig server potrebno je u main klasi dodati anotaciju @EnableConfigServer, dodati potrebne dependency-e u pom.xml i specificirati na kojoj lokaciji se nalaze konfiguracijski fajlovi za koje je zaduzen konfiguracijski server.

Na slici 2.6 je prikazana glavna klasa projekta i dodana anotacija.

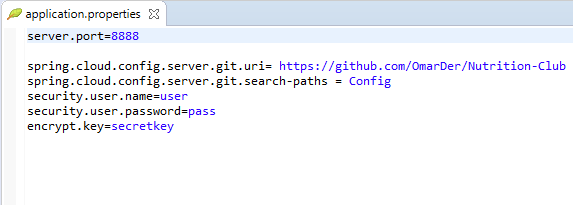


Sl. 2.6 Dodavanje anotacije @EnableConfigServer

Na slici 2.7 je prikazan pom.xml i na slici 2.8 je prikazan application.properties file u kojem je između ostalog specificirana lokacija na kojoj se nalaze konfiguracijski file-ovi za klijente.



Sl. 2.7 Prikaz pom.xml sa dependency-ima



Sl. 2.8 application.properties file koji služi za konfiguraciju samog servera

Prva linija kaže da server radi na portu 8888 što je i uobičajeni port za Spring Config Server.

Druga linija kaže da se konfiguracijski fajlovi za klijenta nalaze na GitHub repozitoriju Nutrition-Club.

Treća linija kaže da je potrebno pretražiti i poddirektorij „Config“ kako bi se našli konfiguracijski fajlovi s obzirom da isti nisu postavljeni direktno u korijen GitHub repozitorija nego se nalaze u folderu Config.

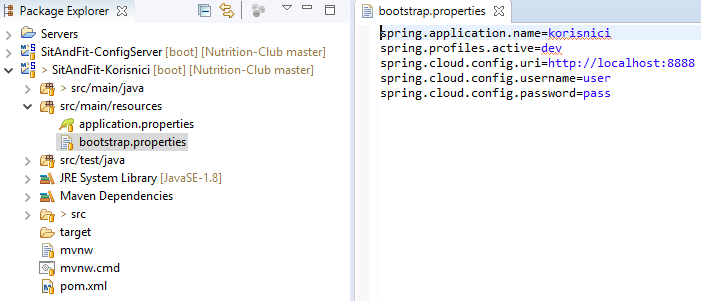
Kako je zadatak bio i omogućiti osnovnu zaštitu putem autentifikacije, u oviru ovog projekta koji se odnosi na Config Server, potrebno je dodati dependency u pom.xml koji se odnosi na Spring Security, koji se može vidjeti na sl. 2.7 ispod dependency-a za Config Server. Kada se doda navedeni dependency omogućena je osnovna zaštita autentifikacijom uz pomoć korisničkog imena i lozinke. Zbog toga četvrta i peta linija u application.properties file-u specificiraju korisničko ime i lozinku koju će koristiti klijenti kada budu od Config servera tražili konfiguraciju.

Pored ovoga, dodatni zahtjev je bio da se može koristiti enkripcija konfiguracije. Kako je po default-u na Config Serveru omogućena enkripcija, u slučaju simetrične enkripcije koja je ovdje izabrana, potrebno je specificirati tajni ključ koji se koristiti prilikom enkripcije i dekripcije.

To specificira šesta linija u application.properties file-u.

Ovim je konfiguracija Config Servera završena.

Kako bi klijenti koristili Config Server i pitali ga za konfiguraciju, potrebno ih je na neki način podesiti da to rade. Konkretno, u slučaju modula za korisnike za koji sam zadužen, napravio sam bootstrap.properties file i u njemu to specificirao. To je prikazano na sl. 2.9



Sl. 2.9 Prikaz boostrap.properties file-a

Ovaj file kaže da je ime aplikacije korisnici, da je trenutni aktivni profil dev, da se config server nalazi na localhost:8888 te da su korisničko ime i lozinka za pristup serveru gore navedeni. Ovo znači da u okviru Gihub repozitorija u folderu Config mora postojati file koji se naziva korisnici-dev.properties koji je konfiguracijski file za ovu aplikaciju. Na osnovu ovoga će modul za korisnike prije svega prilikom svog pokretanja prvo preuzeti konfiguraciju sa Config Servera.

Konfiguracija za mikroservis korisnici koja je kreirana i stavljena na repozitorij u folder Config je prikazana na slici 2.10.

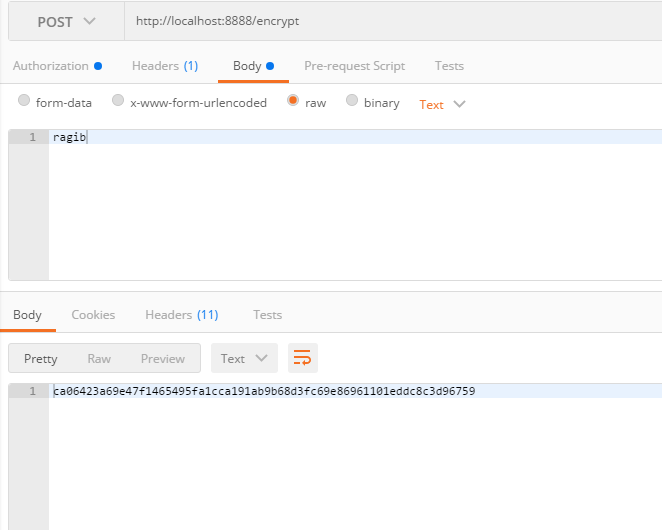


Sl. 2.10 Konfiguracijski file korisnici-dev.properties za mikroservis za korisnike

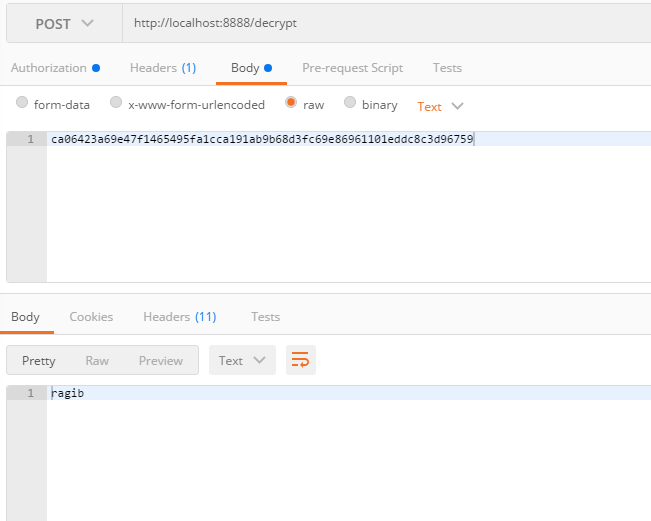
U konfiguraciji vidimo da su polja za username i password za bazu podataka kriptovana obzirom da je to bio jedan od zahtjeva. To je moguće uraditi POST zahtjevom na /encrypt endpoint Config Servera kojem proslijedimo plain text podatak a dobijemo kriptovani podatak i onda takav podatak sa prefiksom {cipher} stavimo u konfiguracijski file.

Prefiks {cipher} je potreban kako bi server znao koja polja je potrebno da dekriptuje prije isporuke konfiguracije nekom od klijenata.

Kriptovanje kao i dekriptovanje podataka upotrebom endpoint-a /encripty i /decrypt je prikazano slikama 2.11 i 2.12



Sl. 2.11 Prikaz enkripcije podataka upotrebom endpointa /encrypt



Sl. 2.11 Prikaz dekripcije podataka upotrebom endpointa /decrypt

Da bi ovo bilo moguće autentifikacijsko zaglavlje u okviru POST zahtjeva mora biti postavljeno sa odgovarajućim korisničkim imenom i lozinkom koji su određeni konfiguracijskim fileom Config Servera.