OWASP

1. **Broken Access Control**

Autorizacija i autentifikacija su podržane upotrebom LDAP baze i primenom RBAC sistema. Definisane su uloge u LDAP bazi i u Keycloak realm-u koji su povezani. Dozvole su definisane nad resursima predstavljenim endpoint-ovima i ograničen je pristup svakom od njih na osnovu uloge korisnika. Dozvole su definisane na nivou scope-a. Korisnici se čuvaju u LDAP bazi. Na klijentskoj strani, korisćen je Keycloak servis preko koga se vrši prijava i registracija i koristi se njihov AuthGuard za autorizaciju pri pristupanju stranicama na frontu.

2. **Cryptographic Failures**

Korišćeni su ažurni RSA algoritmi za enkripciju. Omogućena je HTTPS komunikacija na klijentskoj i serverskoj strani. Osetljive podatke poput lozinki čuva spoljašnji servis Keycloak-a u LDAP bazi, gde se heširaju i koristi *salt*.

3. **Injection**

Zaštita od *injection* napada je podržana u aplikaciji. Zaštita od SQL injection napada je ostvarena kroz upotrebu JpaRepository-ja koji koristi parametrizovane upite. XSS napadi su sprečeni korišćenjem XSSFiltera definisanog u konfiguraciji serverskog dela aplikacije. Filter prerađuje tekst koji može da izazove ove napade tako da ne mogu da se ubace u DOM stablo na klijentskoj strani. Upotrebljena je i posebna klasa za detekciju potencijalnih napada među podacima koji se šalju ka serverskoj strani, koja proverava url i telo zahteva i sprečava maliciozne podatke da prođu dalje od ulaza u kontroler.

4. **Insecure Design**

Nije implementirano.

5. **Security Misconfiguration**

Zavisnosti u aplikaciji su minimalne i svedene na one u upotrebi. Koriste se stabilne, međusobno kompatibilne verzije sa poznatim nedostacima za koje je utvrđeno da ne predstavljaju rizik za rad i integritet aplikacije. U application.properties konfiguracionom falju na serverskoj strani prisutan je minimalan skup podešavanja.

6. **Vulnerable and Outdated Components**

Nije implementirano.

7. **Identification and Authentication Failures**

Spamovanje sistema za registraciju je ograničeno upotrebom Guglovog reCAPTCHA servisa. Omogućena je višefaktorska autentifikacija preko OTP-a koji se čitaju sa mobilnog uređaja. Definisana su pravila za kreiranje lozinki po globalno prihvaćenim standardima. Proverava se i da li se željena lozinka nalazi u crnoj listi čestih lozinki. Trajanje lozinke je ograničeno na godinu

dana, nakon čega je potrebno promeniti lozinku, s tim da ona ne sme da bude ista kao prethodne 3 lozinke.

8. **Software and Data Integrity Failures**

Nije implementirano.

9. **Security Logging and Monitoring Failures**

Nije implementirano.

10. **Server-Side Request Forgery**

Nije implementirano.