OWASP Top 10

1. Broken Access Control (Pokvarena kontrola pristupa)

- Login i registracija korisnika se obavljaju putem Keycloak sistema za autentifikaciju i autorizaciju, koji omogućava centralizovano upravljanje korisničkim pristupom.
- Korišćenje access tokena koji traju 5 minuta za verifikaciju zahteva, dok refresh tokeni za produžavanje sesija traju 30 minuta.
- Osim za javne resurse, pristup resursima je ograničen na osnovu dozvola koje korisnici imaju.

2. Cryptographic Failures (Kriptografske greške)

- Korisničke lozinke su enkriptovane korišćenjem SHA-256 algoritma koji pruža visok nivo zaštite.

3. Injection (Napad putem injekcije)

- Sprovođenje validacija na serverskoj i klijentskoj strani,input polja i URL-ova kako bismo osigurali da su svi unosi ispravni i sigurni.
- Sprečavanje SQL injekcija pomoću ORM(Object-Relational Mapping) tehnologija, konkretno JPA i Hibernate koji automatski sanitizuju SQL upite.

5. Security Misconfiguration (Pogrešna konfiguracija sigurnosti)

- Importovanje samo biblioteka koje su potrebne za rad aplikacije.

7. Identification and Authentication Failures (Greške u identifikaciji i autorizaciji)

- Korišćenje regexa za provere kompleksnosti lozinke i blackliste za sprečavanje slabih lozinki.
- Dodatan sloj sigurnosti putem višefaktorske autentifikacije, implementirana 2FA,SSO..