# OWASP

1. Pokvarena kontrola pristupa
    - Pristup resursima na osnovu permisija, osim za javne resurse
    - Login i registracija se vrši preko Keycloak
    - Access token traje 60 sekundi, koristimo refresh token koji traje 1800 sekundi.
2. Kriptografske greške
    - Enkriptovanje lozinke korisnika sa bezbednih algoritmom (SHA-256)
3. Napadi putem injekcije
    - Korišćenje ORM uz MySql
    - Provere na serveru
    - Provere na frontu (URL i input polja)
5. Bezbedosnosna greška u konfiguraciji
    - Bez importa nekorišćenih biblioteka
7. Greške u identifikaciji i autorizaciji
    - Implementirana višefaktorska autentifikacija
    - Provera slabih šifri putem crne liste
    - Regex za proveru da li je šifra dovoljno kompleksna
10. Falsifikovanje sertifikata na serveru
    - Provera i uklanjanje (sanitize) svih user input polja