OWASP Top Ten

1. Broken Access Control (Oštećena kontrola pristupa)
    a. Resursima se pristupa preko permisija, osim javnih resursa
    b. Login i registracija se vrše preko Keycloak-a
    c. Access token ima rok trajanja od 60 sekundi, a u upotrebi su i refresh tokeni čiji je rok trajanja podešen na 1800 sekundi

2. Cryptographic Failures (Kriptografske greške)
    a. Enkripcija korisničkih lozinki upotrebom bezbednog algoritma (SHA-256)

3. Injection (Napadi injekcijom)
    a. Korišćenje ORM-a (Object Relation Mapping-a) sa H2 bazom podataka
    b. Provere na serveru
    c. Provere URL-a i input polja na frontend-u

4. Security Misconfiguration (Greške u konfiguraciji bezbednosti)
    a. Izvršena je provera i uklanjanje importa biblioteka koje se ne koriste

5. Identification and Authentication Failures (Greške u identifikaciji i autorizaciji)
    a. Implementirana je višefaktorska autentifikacija uz upotrebu TOTP aplikacije na mobilnom uređaju
    b. Implementirana je provera svih lozinki putem crne liste
    c. Takođe, postavljen je regex za dodatnu proveru da li je šifra dovoljno kompleksna

6. Server-Side Request Forgery (Falsifikovanje zahteva na serverskoj strani)
    a. Izvršena je provera i uklanjanje svih korisničkih polja za unos