OWASP Top 10

1. Broken Access Control

Budući da se prijava radi preko keycloak-a, gde je uključena i autorizacija i autentifikacija, imamo centralizovana kontrolu pristupa resursima, uz pomoć permisija i uloga unutar Keycloak-a.

Svaki korisnik ima samo jednu ulogu, koja ima minimalan skup permisija koje su mu potrebne da odradi svoj posao. Svaki resurs ima određena prava pristupa samo za uloge koje bi trebalo da mogu da mu pristupe.

2. Cryptographic Failures

Korišćenjem SHA-256 algoritma za enkripciju i dekripciju resursa omogućujemo bezbednu komunikaciju i visok nivo zaštite.

3. Injection

Nevalidan unos sprečavam uz pomoć raznih validacija polja unosa na klijentskoj strani, kao i korišćenjem ugrađenih biblioteka u Spring za prevenciju XSS napada na serverskoj strani.

Korišćenjem JPA i Hibernate paketa automatski sanitizujemo svaki upit koji dolazi u našu bazu podatak.

5. Security Misconfiguration

Koristimo isključivo biblioteke koje su neophodne za rad same aplikacije.

7. Identification and Authentication Failures

Zahtevanjem da lozinka bude kompleksna uz pomoć regex-a kao i zabranjivanjem čestih lozinki smanjujemo rizik od brute force napada.

Upotrebom *two factor authentication* kao i *single sign on* dodatno smanjujemo rizik od ovakvih napada