OWASP top10

1. ***Broken access control***

- Svi zahtevi na back su onemogućeni od strane ne autentifikovanih korisnika osim onih koji moraju biti, kao što su login, registracija, verifikacija i slično.
- Na frontu-u su korišćeni guard-ovi koji onemogućavaju pristup putanjama korisnicima koji nemaju odgovarajuću ulogu za pristup istima.
- Na beck-u je implementiran rback koji onemogućava pristup rest api-ju ukoliko korisnik nije autentifikovan te nema odgovarajući autoritet za pristup putanji.
- Koristimo jwt token koji se invalidira pri logout-u.
- Jwt token je korišćen u kombinaciji sa kolačićima - cookie.
- Postoji crna lista - blacklist za invalidirane tokene.

2. ***Cryptographic Failures***

- U aplikacijama je implementiran https i to sigurnija TLS implementacija.
- Svi osetljivi podaci koji su čuvani su šifrovani i posoljeni - salted.
- Nije korišćen nijedan zastareli - deprecated algoritam šifrovanja i heširanja.
- Implementiran je najnoviji spring security

3. ***Injection***

- Pored standardne zaštite od injection napada koju pružaju angular i java spring boot, implementirana je validacija korisničkog unosa i na front-u i na back-u.
- Kako bi se umanjile šanse za SQL injection napad koriste se validacije i Parametrized Queries

4. ***Insecure Design***

• Tokom izrade projekta veliku pažnju smo poklonili planiranju same arhitekture, kako bi se smanjila redudantnost koda, ali i povećala sigurnost.
• Aplikacija se sastoji od 2 front-end aplikacije. Jedna je namenjena za admina, a druga za regularne korisnike. Back-end logika je smeštena u jednoj aplikaciji.

5. ***Security Misconfiguration & 6. Vulnerable and Outdated Components***

- Sistem je implementiran tako da je korišćenje eksternih biblioteka svedeno na minimum. Korišćene su isključivo biblioteke koje su poznate i korišćene od strane sistema širom sveta, kao što je recimo Material koji je razvijen od strane Google-a
- Sve funkcionalnosti su implementirane u skladu sa specifikacijom, bez deprecated komponenti

7. *Identification and Authentication Failures*

- Implementirana je zaštita od automatizovanih napada pri logovanju na aplikaciju. Ukoliko dođe do automatizovanog napada (određen broj neuspešnog logovanja) nalog biva zaključan.
- Prilikom logovanja svaki put se generiše novi random kod kojie se šalje korisniku na mejl i koji korisnik mora da unese
- Sve važne akcije u sistemu kao što su prijava, brisanje entiteta i slično se loguju.
- Postoji polisa za sadržaj šifre koja zahteva određen cifara, velikih i malih slova i specijalnih znakova.
- Unete šifre ne smeju biti sa liste najkorišćenijih šifara.
- Prilikom logout-a dolazi do invalidiranja tokena gde se taj token stavlja na crnu listi te ga kasnije nije moguće koristiti.
- Šifre su heširane i posoljene u skladištu

8. *Software and Data Integrity Failures*

- U aplikacijama su korišćeni pouzdani izvori koda kao što su maven i npm.

9. *Security Logging and Monitoring Failures*

- U aplikacijama je implementirano logovanje svih značajnih aktivnosti.
- Aktivnosti i logovi se prikazuju adminu u realnom vremenu, admin ima i mogućnost da dodaje nove alarme.
- Greške se hvataju na mestima koja su namenjena za to i prikazuju se sigurne poruke koje su u skladu sa standardom.

10. *Server-Side Request Forgery*

- Naša aplikacija nema nikakav pristup drugim serverima sa kojima komunicira
- Koriste se snažna autorizacija i autentifikacija, implementiran je potpuni RBACK
- Postoji lista zabranjenih ip adresa
- Vodi se računa o tome da poruke koje se prikazuju korisnicima ne otkrivaju osetljive podatke koji se kasnije mogu zloupotrebiti