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, zahtev za sertifikat 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.
- Svi korisnici rest api-ja moraju da koriste https ukoliko pristupaju istom.
- Svi osetljivi podaci koji su čuvani su šifrovani i posoljeni - salted.
- Skup osetljivih podataka koji se čuvaju sveden je na minimum.
- Nije korišćen ni jedan zastareli - deprecated algoritam šifrovanja i heširanja.
- Korišćeni su pouzdani generatori random brojeva.

3. ***Injection***

- Pored standardne zaštite od injection napada koju pružaju angular i spring boot implementirana je validacija korisničkog unosa i na front-u i na back-u. Onemogućen je unos specijalnih karaktera razmaka, ograničen je broj karaktera.
- SQL injection je sprečen korišćenjem preporučenog načina rada sa bazom podataka u spring boot-u.

4. ***Insecure Design***

- Tokom izrade projekta trudili smo se da stalno reevaluiramo rešenje i da ga konstantno poboljšavamo. Obzirom na to da je dizajn sistema izveden iz specifikacije projekta trudili smo se da istu maksimalno ispoštujemo.

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 Vulnerable and Outdated Components***

- Sistem je implementiran i konfigurisan tako da ne postoje nepotrebne funkcionalnosti i nisu instalirane nikakve komponente i biblioteke koje bi potencijalno mogle da omoguće hakerima da kompromituju rad sistema. Nije moguće pristupiti serverima preko podrazumevanih korisničkih imena i šifara koje dolaze uz neki od korišćenih radnih okvira.
- Korišćene su komponente i biblioteke u podrazumevanim verzijama.

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.
- Sva neuspešna logovanja i zaključavanja naloga su logovana.
- 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 na svim idepotentnim metodama api-a kao i na svim metodama kada dođe do greške. Takođe moguće je ugraditi i alarme koji u realnom vremenu obaveštavaju administratore.
- Podaci koji se nalaze u logovima su informativni i sadrže sva polja koja nalažu najnoviji standardi
- Aplikacija u realnom vremenu može da detektuje da li je došlo do napada i da locira isti.

10. ***Server-Side Request Forgery***

- Naša aplikacija nema nikakav pristup drugim serverima sa kojima komunicira preko url -a te ssrf nije moguć