Top 10 OWASP List

- A01:2021 Broken Access Control
  - Implementacija AuthGurad-a na front-end aplikaciji
  - CORS konfiguracija podešena na najmanji opseg
  - Implementacija RBAC-a (Role Based Access Control).
  - REST API – krajnje tačke (endpoints) aplikacije su posmatrane kao resurs. U nekim slučajevima grupa krajnjih tačaka čini resurs.
  - Login i registracija se oslanja na Keycloak servis.
  - Minimalne privilegije dodeljene pomću scope, resource i permission entiteta koje Keycloak nudi.
  - Korišćenje Access Tokena i Refresh Tokena
    - JWT tokeni
    - Bearer atribut u header-u
  - Implementacija podržana od strane Keycloak servisa za autorizaciju i autentifikaciju
    - Koristi Policy Enforcer adapter na strani servera na kome se nalaze resursi
  - Za više detalja o implementaciji pogledati projekat ili posetiti zvaničnu dokumentaciju: https://www.keycloak.org/docs/latest/authorization_services/index.html

- A02:2021 Cryptographic Failures
  - Obezbeđen HTTPS između front-end aplikacije i back-end aplikacije
  - HSTS
  - Koriste se trenutno pouzdani i optimalni kriptografski i heš algoritmi
  - Validacija sertifikata
  - Osetljivi podaci se bezbedno čuvaju
  - Isključeno keširanje podataka
  - Bezbedno čuvanje lozinki, salt i hash
- A03:2021 Injection
  - SQL Injection pokriven korišćenjem JPA/Hibernate (Java Persistance API), korišćenjem parametrizovanih upita.
  - XSS Stored pokriven specijalnih header vrednostima koji naznačavaju pretraživačima da obrate pažnju. Dodat filter u spring boot security filter chain koji vršiti sanitizaciju vrednosti.

    - Validacija ulaznih podataka od strane servera.
    - Consumes i Produces atributi na nivou krajnjih tačaka
- A04:2021 Insecure Design
    - Nije podržano i provereno
- A05:2021 Security Misconfiguration
    - Obrisane krajnje tačke koje nisu u upotrebi
    - Proverene komponente i zavisnosti, koriste se verzije koje imaju najmanje sigurnosnih rizika, takođe provereni su i mogući sigurnosni rizici koje trenutne verzije nose.
    - Zavisnosti koje se ne koriste su obrisane kao i importi unutar klasa
- A06:2021 Vulnerable and Outdate Components
    - Nije podržano i provereno
- A07:2021 Identification and Authentication Failures
    - Implementacija multifaktorske autentifikacije
        - Konkretno dvofaktorske autentifikacije
    - Crna lista lozniki (10k)
        - Loznike koje ne mogu biti postavljene
    - Trajnosti lozniki na 365 dana nakon čeka je potrebno resetovanje
    - Oporavak naloga
    - Korišćenje keycloak-a za praćenje sesije
    - Detekcija brute-force napada i privremeno ili trajnje blokiranje naloga, u zavisnosti od broja pokušaja pristupa.
- A08:2021 Software and Data Integrity Failures
    - Nije podržano i provereno
- A09:2021 Security Logging and Monitoring Failures
    - Nije podržano i provereno
- A10:2021 Server-Side Request Forgery
    - Nije podržano i provereno

Projekat se u većoj meri oslanja na Keycloak servis implementiran u Java programskom jeziku. Za više detalja pročitati dokumentaciju:

https://www.keycloak.org/documentation