OWASP

1. Broken Access Control
   - Autentifikacija i autorizacija. Samo je login dostupan svima.
   - Black lista jwt tokena - tokeni se dodaju u nju kada se korisnik izloguje
2. Cryptographic Failures
   - HTTPS
   - Hesiranje lozinke (salt + hashing algorithm)
   - Keširanje po defaultu isključeno u Spring Security
   - Šifrovanje poruka koje šalju uređaji, šifrovane poruke se čuvaju u fajlu
3. Injection
   - Urađena validacija podataka i na frontu i na beku (white list - regexi)
4. Insecure Design
5. Security Misconfiguration
6. Vulnerable and Outdated Components
   - Uklonjene su biblioteke i zavisnosti koje se ne koriste
7. Identification And Authentication Failures
   - Proverićemo listu 10000 najgorih lozinki
   - Blokiranje korisnika nakon N neuspešnih logovanja
   - Postoji format lozinke koji se mora ispoštovati (najmanje 13 karktera, da sadrži veliko, malo slovo, broj i specijalni znak)
8. Software and Data Integrity Failures
   - Zavisnosti i biblioteke preuzimane samo preko maven-a i npm-a
9. Security Logging and Monitoring Failures
   - Implementirano logovanje. Loguje se svaka akcija na svakoj aplikaciji. Čuva se vreme kada se izvršila akcija, koji korisnik je izvršio, na kojoj aplikaciji, da li je radnja uspešna i ako nije šta je dovelo do greške
10. Server Side Request Forgery(SSRF)
    - Klijentu se vraćaju DTO objekti