OWASP – TOP 10

1. **Injection**

Svako polje u modelu koje je tipa string anotirano je @SqlInjectionSafe anotacijom koja sprečava unos izvršivih SQL naredbi (Drop table, Insert into, ...). Hibernate, takođe u sebi ima ugrađene mehanizme koji sprečavaju SQL Injection napade.

2. **Broken Authentication**

Prilikom registracije korisnika na sistem od njega se zahteva da lozinka ima minimalno deset karaktera. Nakon unosa lozinke, potrebno je ponoviti je gde se proverava da li se lozinke podudaraju. Svaka lozinka se “hešira” pomocu BCryp mehanizma.

3. **Sensitive Data Exposure**

Odrađen je ACL (Access Control List) koji onemogućuje pristup fajlovima sa osetljivim podacima.

4. **XML External Entities (XXE)**

Onemogućavanjem DTD-ova (Document Type Definition) I eksternih entiteta se sprečava ovakva vrsta napada.

5. **Broken Access Control**

Implementiran je RBAC model koji podrazumeva da svaki korisnik u sistemu ima svoju ulogu a svaka uloga u sistemu ima svoje permisije. Pristup svakoj metodi obezbeđen je tako što je svaka metoda anotirana sa @PreAuthorize anotacijom gde se proverava uloga korisnika.

6. **Security Misconfiguration**

Na mikroservisima je implementiran Spring Security. U svakom kontroleru je implementiran mehanizam upravljanja greškama.

7. **Cross-Site Scripting XSS**

Problem XSS zaštite je delimično razrešen je tako što je na input poljima na frontendu postavljena validacija kroz Regex, a na backendu kroz Patterne. Nije dozvoljen unos specijalnih karaktera kao što su <, >, što predstavlja vid zaštite od ovakvih napada.

8. **Insecure Deserialization**

Problem nesigurnih deserijalizacija razrešen je upotrebom novijih verzija dependency-ja. Opisano u pdf fajlu “Analiziranje ranjivosti”.

9. **Using Components with Known Vulnerabilities**

Urađen Check Dependency I razrešene sve ranjivosti. Opisano u pdf fajlu “Analiziranje ranjivosti”.

10. **Insufficient Logging & Monitoring**

Logging mehanizam je kompletno odrađen na mikroservisnoj aplikaciji. Za svaki servis definisano je tri tipa Log fajova: Info, Warn I Error. Logging mehanizam je implementiran tako da su ispunjeni zahtevi kao što su kompletnost, pouzdanost, upotrebljivost i konciznost.