**OWASP TOP 10**

**6. Sensitive data exposure**

TLS(HTTPS), digitalno potpisivanje, enkripcija podataka uradjeno.

Ovi sigurnosni propusti, koji se javljaju prilikom izlaganja osetljivih podataka, rešeni su tako što je koršćen HTTPS (TLS) protokol, kako bi se obezbedila enkripcija podataka koji se šalju. Što se tiče lozinki koji se čuvaju u bazi, one su heširane i za to je korišćen ALGORITAM.

Formirani dokumenti (propis, amandman itd.) koji se čuvaju u bazi, čuvaju se potpisani i enkriptovani, kao još jedan vid rešenja na dati sigurnosni propust. Za to su korišćeni jaki i noviji kriptografski algoritmi.

Postoje još neke mere zaštite, koje je neophodno uzeti u obzir, a nisu korišćene u ovoj aplikaciji... Na primer, neophodno je isključiti autocomlete u formama kod prikupljanja osetljivih informacija, takođe je neophodno i isključiti keširanje stranica koje sadrže osetljive informacije.

**4. Insecure direct object references**

Postoje dva načina od ove vrste napada. Prvi je da se objekti indirektno referenciraju, a drugi da se objekti direktno referenciraju uz proveru prava pristupa. Naš način odbrane od ovog napada jeste taj da prilikom svakog pristupa određenom resursu, proveravamo da li je korisnik ulogovan i koja su njegova prava pristupa (dakle, drugi način).

U datoj aplikaciji, ovo je rešeno tako što je ulogovanom korisniku prikazano samo ono što je njemu predviđeno. Na primer, ulogovan građanin ne može uneti novi propis već može samo vršiti pretragu postojećih propisa, kao i pregled istih, odbornik ne može prihvatati akte itd. Naravno, prava pristupa se proveravaju prilikom svake akcije. Ukoliko ulogovani građanin pokuša da preko URL-a ode na određenu stranicu na kojoj nema prava pristupa, biće redirektovan.

Provera prava pristupa su konkretno implementirana na front-end-u u html stranicama (šta ulogovani korisnik sme da vidi od funkcionalnosti), kao i u kontrolerima u kojima se proveravaju prava pristupa svaki put pre nego što se izvrši neki servis za dobavljanje podataka na osnovu direktnih referenci (AngularJS).