5.Security misconfiguration

Sa obzirom da nećemo postavljati našu aplikaciju da trči na nekom pravom serveru, tj. nećemo je stavljati u konkretnu upotrebu, ova tačka nije neophodna da se uradi.

3.Cross site scripting

Ovaj problem je rešen koristeći [*JSOUP*](https://jsoup.org/cookbook/cleaning-html/whitelist-sanitizer) *API*, koji između ostalog štiti serversku stranu od XSS napada.

JSOPU poseduje svoju *Whitelist-u*, na osnovu koje dozvoljava ili ne dozvoljava određene HTML tagove.

Koristeći metodu **Jsoup**.clean(unsafe, **Whitelist**.basic());

gde je *“unsafe”* string koji potencijalno sadrži opasnu skriptu, rešavamo se bilo kakve opasnosti da se taj string nekako uvuče i izvrši u našoj aplikaciji.

Ova metoda se koristi svuda gde se dobijaju podaci sa klijenta(login, registracija, pretraga, unos novog propisa, amandmana…), tj. na samom pocetku REST metoda kontrolera za obradu ovakvih podataka.