**OWASP TOP 10**

**10. Unvalidated redirects and forwards**

Jedan od načina zaštite od ove vrste napada na back-endu je izbegavanje redirect i forward mehanizama koji smo i mi usvojili. Na kontrolerima na back-endu (Spring) nemamo ni jedan redirect ili forward, return nam predstavljaju podaci koji se naknadno obradjuju na front-endu i prikazuju korisnicima.

Na front-endu (AngularJS) koristimo $state mehanizam koji nam omogućavamo da redirektujemo na osnovu naziva stanja, a ne zadavanjem URL koji bi omogućio napadaču da pošalje maliciozan string koji upućuje na maliciozan sajt.

Korisnike treba obrazovati i dati im do znanja da ne treba da klikću na neproverene linkove koji im stižu u e-mailu ili u poruci kako ne bi na apsurdan način doveli našu aplikaciju u stanje u kome mora da se brani od napadača. Seminare i slične skupove, koji bi obrazovali naše korisnike, treba organizovati što češće kako bi korisnici bili obavešteni o najnovijim informacijama koji se tiču bezbednosti na internetu, kao i iz razloga što korisnici koji nisu informatički najobrazovaniji moraju se podsećati šta ne bi trebali da rade inače će u jednom trenutku svakako napraviti grešku.

**9. Using components with known vulnerabilities**

**8. Cross-site request forgery**

Korisnik prilikom logovanja na aplikaciju dobija svoj JWT (JSON Web Token) koji se smešta u Local Storage korisnikovog pretraživača. Prilikom sledećeg pristupa aplikaciji korisnik šalje njegov JWT i na osnovu njega se proverava da li ima pristup nekom od resursa aplikacije, ako nema JWT da pošalje odbija se njegov zahtev i šalje se na login stranicu aplikacije. Kao dodatna zaštita implementiran je i HTTPS mehanizam koji omogućava kriptovanje zahteva i smanjuje mogućnost da se ukrade JWT. Ako se korisnik izloguje sa sistema njemu se briše JWT iz Local Storage i ukoliko ponovo pokuša da pristupi aplikaciji moraće ponovo da se uloguje kako bi dobio novi JWT koji se generiše samo za njega.

Problem kod ovoga je što ako neko drugi koristi korisnikov računar može da pristupi i tokenu ukoliko se korisnik nije izlogovao sa aplikacije i time izbrisao i token iz svog pretraživača. Zbog pomenute pretnje moramo korisnika obučavati i skrenuti mu pažnju kako bi morao da se ponaša kako ne bi na naivan način ugrozio svoju bezbednost na internetu, kao i bezbednost same aplikacije.

Kako koristimo Spring kao back-end on ima uključenu CSRF zaštitu u samoj Java konfiguraciji. (OVO JOS PROVERITI)