OWASP TOP 10

A1 Injection

- Validacija podataka na *frontend*-u
- Validacija pomoću *Hibernate* za upis u bazu
- Validacija pristiglih podataka na backend-u

A2 Broken Authentication and Session Management

- *HTTPS* protokol obezbeđuje tajnost podataka
- Aplikacija ne sadrži autentifikaciju korisnika
- Kupovina se vrši prebacivanjem kontrole na banku koja generiše *URL* na koji treba da se redirektuje

A3 Cross-Site Scripting (XSS)

- *XSS* zaštita nije podržana

A4 Insecure Direct Object References

- Nema osetljivih informacija u *URL*-u
- Svi vidljivi *ID*-jevi u *URL*-ovima su nasumično generisani od strane banke

A5 Security Misconfiguration

- Aplikacija ne trči na javnom serveru, stoga nemamo konfiguraciju na istom

A6 Sensitive Data Exposure

- Korišćen je *HTTPS* protokol za enkriptuje podataka između klijenta i servara i između servera i servera

A7 Missing Function Level Access Control

- Aplikacija ne sadrži *ROLLE*

A8 Cross-Site Request Forgery (CSRF)

- Korišćenjem *HTTPS-a* protokola dobili smo kriptovanje zahteva koji smanjuje mogućnost da se ukradu podaci poslati na server
- Podaci se čuvaju u *Cookie-u* ali zato svako plaćanje se vrši na jedinstvenom *URL-u*

A9 Using Components with Known Vulnerabilities

- *Bower* komponente koje smo koristili su dosta zastupljene na drugim projektima gde nema prijavljenih bezbednosnih propusta
- Kosišćene su sveže verzije *bower* komponenta

A10 Unvalidated Redirects and Forwards

- Na *frontend-u* korišćen je *ui-router* kod kog koristimo mehanizam stanja, stoga nemamo redirekciju i *forward* na aplikaciji