OWASP TOP10

Sistemi elektronskog placanja
Projekat

A1 Injection

- Validacija podataka na frontend-u - prilikom popunjavanja formi
- Validacija pristiglih podataka formi na backend-u
- SQL upiti su parametrizovani (Hibernate) - zastita od SLQ injection

A2 Weak authentication and session managment

- Aplikacija nema korisnike te ne postoji briga o sesijama korisnika. Kupovina se vrsi prebacivanjem kontrole na PayPal koji generise novi url za kupovinu iako je korisnik vec ulogovan.

A3 XSS

- Upotrebom JSOUP.clean(...) podaci koji dolaze na backend se ciste od potencijalnih tagova koji mogu izazvati XSS

A4 Insecure direct object references

- (/foo=1234)
- Aplikacija ne sadrzi apije koje je moguce na ovaj nacin eksploatisati

A5 Security misconfiguration

- Knowing what server is used to determine known vulnerabilities
- U zavisnosti od servera na koji bi se aplikacija pustila istrazili bi moguce ranjivosti

A6 Sensitive Data Exposure

- Upotreba HTTS protokola kako bi se enkriptovali podaci od klijenta ka serveru
- Korisnickim podacima vezanim za postupak placanja rukuje PayPal

A7 Missing function level access control

- Aplikacija ne sadrzi korisnicke uloge pa ne postoji mogucnost eksploatisanja informacija koje ne pripadaju odredjenoj ulozi

A8 CSRF

- Paypal redirektuje na nasu aplikaciju prilikom kupovine kreirajuci specifican url za tu kupovinu bilo da je korisnik ulogovan na Paypal ili ne, tako da ne moze doci do CSRF

A9 Using components with known vulnerabilities

- Za komponente koje koristimo (bower komponente i paypali sdk) nismo pronasli opasnosti,

A10 Unvalidated redirects and forwards

- Nikad ne dolazi do redirekcije ili forward-a
- Na frontend-u nevalidni url-ovi uvek vracajau na pocetnu (default) stranicu