Testiranje bezbednosti webshop-a

Napraviti webshop za prodaju vaših omiljenih proizvoda (računarska oprema, prehrambeni proizvodi, kozmetika,…). Potrebno je da svaki proizvod pripada nekoj kategoriji (npr. u slučaju računarske opreme jedna kategorija je grafičke kartice, gde je konkretan proizvod koji pripada toj kategoriji nVidia GeForce GTX 980).

WebShop treba da omogući prijavu i registraciju korisnika, gde prijavljeni korisnik može da ima ulogu administratora ili kupca. Korisnik se može registrovati unosom korisničkog imena, lozinke (koje se skladište sa **hash & salt** pristupom) i nekih ličnih podataka ili koristeći **OAuth** protokol upotrebom Facebook ili Google naloga.

Koristeći **RBAC** princip kontrole pristupa, sajt treba da ponudi sledeću funkcionalnost:

* Pregled svih proizvoda po kategorijama (anoniman korisnik, kupac, administrator);
* Manipulacija svoje korpe – dodavanje, uklanjanje i izmena količine proizvoda u korpi (kupac, administrator);
* Checkout – korisnik popunjava podatke za pošiljku i time formira transakciju koja sadrži podatke o narudžbini i prazni korpu korisnika (kupac, administrator);
* Pregled ličnih transakcija – korisnik može da vidi listu svojih prošlih transakcija (korisnik, administrator);
* Pregled svih transakcija – administrator može da vidi sve transakcije (administrator);

Komunikacija između klijenta i servera treba da bude preko **HTTPS**-a.

Nakon što ste izgradili aplikaciju potrebno je formirati izveštaj (dokument od nekoliko strana) gde ćete proći kroz OWASP Top 10 listu i prokomentarisati da li, gde i u kojoj meri vaša aplikacija može da nastrada zbog date grupe propusta. Zatim, treba da definišete odbranu od datog propusta, i da navedete gde tačno u kodu se vi branite od datog problema. Ovo (uz boldovane koncepte iznad) je ono što će se ocenjivati, gde je ostatak aplikacije tu samo da bi mogli da izvršimo bezbednosnu evaluaciju. S’ time na umu potrebno je da detaljno izučite svaku od 10 grupa propusta, da potpuno shvatite o čemu je reč tu, i da vidite u kojoj meri se dati propusti odnose na vaš sistem, nakon čega ćete se zaštiti od problema.

**Napomena:** nije dovoljno izguglati određen propust i otvoriti prvi link, naći paragraf ili dva i uzeti kao da ste sve rešili. Za svaku grupu propusta potrebno je sprovesti ozbiljnije istraživanje, gde ćete sa više izvora pročitati viđenje datog propusta i najzad napraviti vašu zdravorazumsku sintezu problema.