

UNIVERZA V LJUBLJANI  
FAKULTETA ZA RAČUNALNIŠTVO IN INFORMATIKO

## **Spletna knjigarna - Trgovina abc**

Poročilo seminarske naloge pri predmetu  
Elektronsko poslovanje

### **Študenti**

Tilen Miklavič (63180204)  
Luka Zornada (64170033)  
Rihard Marušič (64170021)

### **Mentor**

David Jelenc

Ljubljana, 21. december 2020

# Kazalo

1	Uvod	2
2	Navedba realiziranih storitev	3
3	Podatkovni model	4
4	Varnost sistema	5
5	Izjava o avtorstvu seminarske naloge	6

# Poglavje 1

## Uvod

Za seminarsko nalogo smo izdelali spletno knjigarno. Namenjena je anonimnim in registriranim kupcem, ter jim ogomoča pregled artiklov in dodajanje le teh v košarico. Ravno tako podpira prijavo in registracijo novih uporabnikov. Spletno knjigarno ravno tako uporabljajo prodajalci, ki imajo pregled nad strankami in lahko z njihovimi podatki upravljajo. Njihova naloga pa je tudi potrjevanje, zavračanje in storniranje računov. Za sistem skrbi sistemski inženir (admin), ki ima pregled nad vsemi trgovci.

## Poglavje 2

### Navedba realiziranih storitev

Implementirali smo registracijo strank z uporabo filtriranja CAPTCHA. Za to smo uporabili Googlovo reCAPTCHA, ki se na strani za registracijo pojavi kot enostaven gumb za potrditev, da uporabnik ni robot.

Implementirali smo tudi registracijo strank z uporabo potrditvenega e-maila. Za to smo uporabili priljubljeno knjižnico PHPMailer. Ob registraciji novega uporabnika, se le temu na vpisan e-poštni naslov pošlje sporočilo z vsemi podatki, ravno tako pa povezava do strani za potrditev e-poštnega naslova. Preden uporabnik potrdi svoj e-mail, je v bazi označen kot neaktiven, ko pa obišče povezavo za potrditev, se spremeni v "aktivnega" kupca.

Implementirali smo smiselno organizacijo in izvedbo uporabniškega vmesnika s pomočjo tehnologij kot so sta CSS in JavaScript. Za to smo uporabili CSS in JS knjižnico Bootstrap, ki nam v večini koristi za smislen celoten estetski izgled strani.

Implementirali smo binarno iskanje...

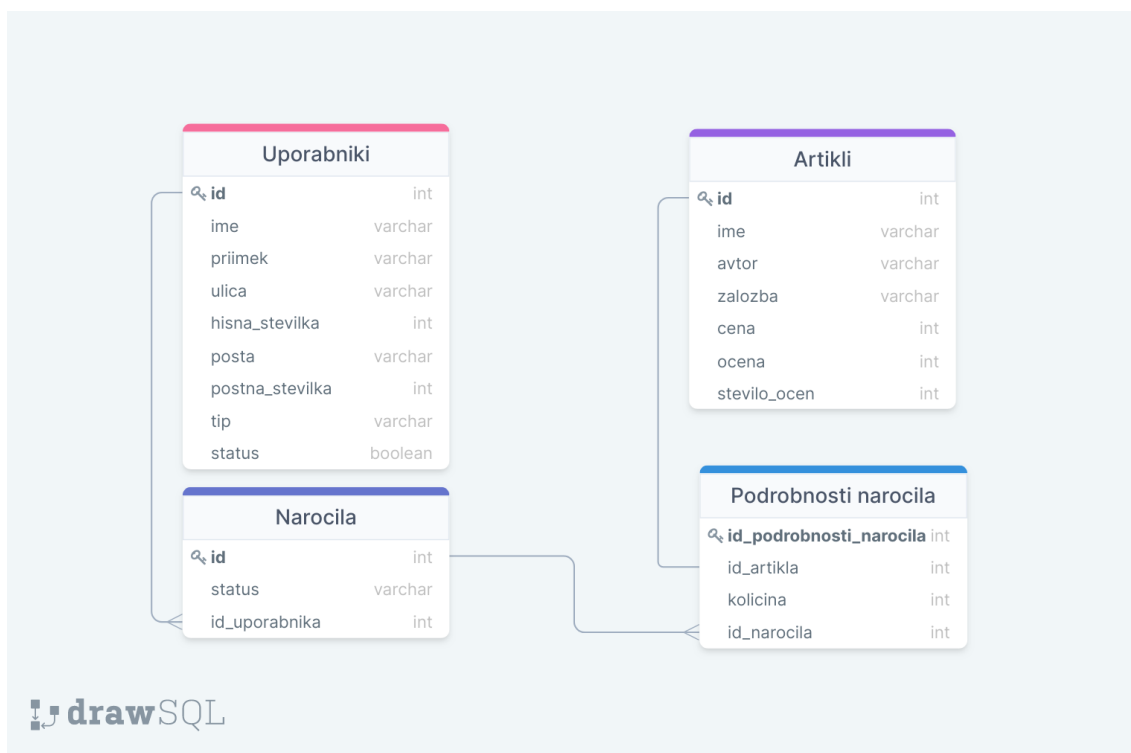
Predstavitev artiklov s slikami...

Implementirali smo ocenjevanje artiklov. Do te funkcionalnosti lahko dostopajo samo prijavljeni uporabniki, ko kliknejo na artikel, da se jim pokažejo podrobnosti. Na tej strani lahko podajo svojo oceno za določen artikel, ta pa se nato shrani v podatkovno bazo. Na strani s pregledom artiklov lahko vsak vidi povprečno oceno posamičnega artikla.

Obvezne storitve, ki je nismo implementirali do konca je Prikaz artiklov v mobilni aplikaciji Android. Razvili smo REST API-je za pregled, urejanje in brisanje artiklov, vendar je bil JSON element, ki ga je Android aplikacija prejela pokvarjen in ga zato ni mogla pretvoriti v Kotlin objekt.

## Poglavje 3

# Podatkovni model



Slika 3.1: Podatkovni model

S podatkovnega modela je razvidno, da smo ustvarili štiri tabele (artikli, uporabniki, narocila, podrobnosti narocila). V tabeli artikli so shranjeni seveda vsi artikli ki se prodajajo v knjigarni, v tabeli uporabniki si shranjeni vsi uporabniki spletne trgovine (admin, prodajalci in stranke), v tabeli narocila so shranjena vsa narocila in v tabeli podrobnosti narocila so shranjeni vsi artikli ki so se pojavili na kakšnem naročilu (vsak zapis v podrobnosti naročila ponazarja eno naročilo in en artikel, ki je na tem naročilu, ravno tako pa nam pove količino tega izdelka na tem določenim naročilom).

## Poglavje 4

### Varnost sistema

Pri brskanju po trgovini je implementirano preklapljanje med varnim in navadnim kanalom. Ko obiščemo stran za prijavo se preklopi na varnostni kanal, pri čemer nas stran vpraša za certifikat. Če se želimo prijaviti kot admin ali prodajalec izberemo ustrezen certifikat, sicer zavrnamo izbiro. Varna povezava se nato obdrži do odjave uporabnika, ko se stran poveže nazaj na navaden kanal.

Prijava v spletno trgovino je zaščitena z uporabniškim imenom in geslom. Ravno tako je prijava v sistem kot prodajalec ali administrator zaščitena s certifikatom.

Vsa gesla se pred vpisom v podatkovno bazo šifrira in se jih nato vedno preverja v funkciji v šifrirani obliki.

S funkcijo `htmlspecialchars()` je naša spletna knjigarna zaščitena pred napadi XSS.

Z uporabo PDO-ja pa je zaščitena tudi pred SQL-injection napadi.

# Poglavje 5

## Izjava o avtorstvu seminarske naloge

Spodaj podpisani *Tilen Miklavič*, vpisna številka 63180204, sem (so)avtor seminarske naloge z naslovom *Spletna knjigarna - Trgovina abc*. S svojim podpisom zagotavljam, da sem izdelal ali bil soudeležen pri izdelavi naslednjih sklopov seminarske naloge:

- Zasnova MySQL podatkovnega modela
- Kreiranje MySQL podatkovnega modela
- Kreiranje vseh tabel v bazi
- Vzpostavljanje lastne certifikatne agencije
- Izdelovanje strežniškega digitalnega potrdila
- Implementacija večinskega dela index.php routerja
- Implementacija večinskega dela database.php datotek za komunikacijo s podatkovno bazo
- Implementacija logike za Prikaz seznama artiklov prijavljeni in neprijavljeni stranki
- Implementacija logike za prikaz podrobnosti artikla prijavljeni in neprijavljeni stranki
- Implementacija logike za prijavo in registracijo stranke
- Implementacija logike za dodajanje artiklov v košarico
- Posodabljanje lastnih atributov vseh uporabnikov
- Posodabljanje atributov drugim uporabnikom
- Ocenjevanja artiklov
- Šifriranje gesel

- Obramba pred napadi XSS
- Obmramba pred napadi SQL injection
- Kreiranje novega artikla za prodajalca
- Urejanje artiklov za prodajalca
- Pregled strank za prodajalca
- Urejanje atributov strank za prodajalca
- Ustvarjanje novih uporabnikov za prodajalca
- Pregled in urejanje prodajalcev za admina
- Ustvarjanje novih prodajalcev za admina
- Shranjevanje trenutne seje za ohranitev prijave in brisanje seje ob odjavi
- Implementiranje filtriranja ob registraciji z CAPTCHA
- Implementiranje potrjevanja strank s potrditvenim emailom
- Implementacija API endpoint-a
- Implementacija kontrolerja za komuniciranje med strežnikom in android aplikacijo
- priprava izgleda in delovanje android aplikacije (nepopolno)

Podpis: Tilen Miklavič, l.r.



Spodaj podpisana *Luka Zornada*, vpisna številka 64170033, sem (so)avtor seminarske naloge z naslovom *Spletna knjigarna - Trgovina abc*. S svojim podpisom zagotavljam, da sem izdelal ali bil soudeležen pri izdelavi naslednjih sklopov seminarske naloge:

- Prijava z ustreznim certifikatom
- Preklop med varnim in navadnim kanalom
- Posodabljanje podatkov izdelkov
- Priprava izgleda in delovanje android aplikacije (nepopolno)

Podpis: Luka Zornada, l.r.

Spodaj podpisana *Rihard Marušič*, vpisna številka 64170021, sem (so)avtor seminar-ske naloge z naslovom *Spletna knjigarna - Trgovina abc*. S svojim podpisom zagotavljam, da sem izdelal ali bil soudeležen pri izdelavi naslednjih sklopov seminarske naloge:

- Vzorčni sklop 1
- Vzorčni sklop 2

Podpis: Rihard Marušič, l.r.