

UNIVERZA V LJUBLJANI
FAKULTETA ZA RAČUNALNIŠTVO IN INFORMATIKO

Implementacija spletne prodajalne in odjemalca za Android

Poročilo seminarske naloge pri predmetu
Elektronsko poslovanje

Študenti

Primož Hrovat (63150113)
Miha Mazovec (63150193)

Mentor

David Jelenc

Ljubljana, 14. januar 2018

Kazalo

1	Uvod	2
2	Navedba realiziranih storitev	3
3	Podatkovni model	4
4	Varnost sistema	6
5	Izjava o avtorstvu seminarske naloge	8
6	Zaslonske slike - spletna aplikacija	10
7	Zaslonske slike - Android aplikacija	13
8	Zaključek	15
9	Literatura	16

Poglavje 1

Uvod

Seminarska naloga je predvidevala izdelavo spletne prodajalne, tako spletne kot mobilne aplikacije za Android. Pri izdelavi sva uporabljala tehnologije PHP, točneje ogrodje Laravel, z namenom spoznavanja tega ogrodja za izdelavo spletnih aplikacij. Mobilni odjemalec temelji na operacijskem sistemu Android, ki je trenutno najbolj razširjen OS na svetu.

Poglavje 2

Navedba realiziranih storitev

Aplikacija podpira (implementira) naslednje dodatne razširitve:

1. Splet:

- Vodenje dnevnika uporabnikov Administrator in Prodajalec.
- Registracija strank z uporabo filtriranja CAPTCHA
- Registracija strank z uporabo potrditvenega e-maila
- Manjše nadgradnje na strani uporabniškega vmesnika (CSS, JS)
- Implementacija ocenjevanja artiklov prijavljenega uporabnika ter predstavitev njihove povprečne ocene pri njihovem ogledu.
- Implementacija iskanja po artiklih. Iskalnik naj podpira binarno iskanje.
- Predstavitev artiklov s slikami. Slike lahko shranite v SUPB ali na datotečni sistem.

2. Android:

- Osveževanje zaslonov
- Prijava in odjava registriranega uporabnika
- Pregled artiklov s prijavljenim uporabnikom
- Pregled in spreminjanje uporabnikovih podatkov

Delno je implementiran tudi strežniški del za nakupovanje preko vmesnika mobilne aplikacije (košarica, računi...).

Poglavje 3

Podatkovni model

Na sliki 3.1 je prikazana shema uporabljene podatkovne baze. Baza podpira dodeljevanje več vlog uporabnikom, prav tako lahko za posamezen produkt dodamo več cen, upošteva se vedno zadnja veljavna. To lahko koristimo v primeru, da se cena izdelka spremeni, preteklim nakupom pa ne smemo popravljati zneskov, sicer pride do nekonsistence glavne knjige. Baza je načeloma v 3. normalni obliki, z izjemo uporabnikovega atributa naslov, kjer za potrebe naše trgovine ločevanje atributa na nove povezane tabele (naslov, kraj, država) ne predstavlja večjega smisla. Denormalizacija je izvedena tudi na tabeli 'postavka' in 'racun', kjer bazni prožilci sproti popravljajo ceno/znesek, podobno je pri produktu - povprečna ocena se popravlja z baznimi prožilci. Relacija 'dnevnik' v atributu 'opis' hrani podatke o zahtevah prodajalcev in administratorja, tip pa predstavlja tip zahtevka HTTP. 'Vloga' služi le kot šifrant za različne tipe vlog: 'administrator', 'prodajalec', 'stranka'.

Poglavje 4

Varnost sistema

Za namene varnosti so strani `/admin/*` in `/prodaja/*` dostopne le z uporabo certifikata X.509, potrjenega s strani CA PMCA. PMCA je certifikatna agencija, pripravljena prav za potrebe te spletne aplikacije. Dodatno se pri dostopu `/admin` in vseh podstrani zahteva uporaba administratorskega certifikata (CN=Administrator). Dodatno se preverjanje uporabnika preverja na strani same aplikacije - poišče se ujemanje elektronskega naslova na podanem certifikatu in tistim, zapisanim v bazi. Od uporabnika se nato zahteva še sam vnos gesla, ki si ga lahko uporabnik po volji spremeni, prav tako je omogočeno urejanje ostalih atributov.

Spletni vmesnik za pregled izdelkov je dostopen preko HTTP in HTTPS protokola, dočim se za prijavo in registracijo izvede preusmerjanje na zavarovan kanal. Vse strani prijavljenega uporabnika so zaščitene s protokolom HTTPS, prav tako vse strani in podstrani `/admin` in `/prodaja`.

Vsako preverjanje vnosov s strani uporabnikov je očiščeno html znakov (funkcija `htmlspecialchars()`), vsi parametri, ki se uporabljajo v poizvedbah SQL se obravnavajo kot parametri in ne kot ukazi (uporaba predpripravljenih poizvedb), kar naj bi preprečevalo vrivanje kode SQL (SQL Injection). S pomočjo ogrodja Laravel se uporablja tudi zaščita pred CSRF napadom.

Vsi dostopi do različnih podstrani, ki zahtevajo prijavo so prav tako ščiteni z uporabo sejnih spremenljivk, ki v primeru nepooblaščenega dostopa izvedejo preusmeritev na stran za prijavo. Pri registraciji uporabnika je zahtevana uspešna rešitev CAPTCH, katere odziv se preveri na strežniški strani. V kolikor je odziv ustrezen, se uporabnika doda v podatkovno bazo, nadalje pa se mu pošlje potrditveno elektronsko sporočilo z naključno generiranim nizom. S klikom na povezavo se preveri veljavnost niza in v primeru ujemanja uporabniku dovolimo prijavo v trgovino. Pošiljanje elektronskih sporočil je izvedeno preko storitve Mailgun, ki brezplačno omogoča pošiljanje sporočil samo osebam, ki so izrecno dovolile dostavo. Za potrebe demonstracije, je v kodi trenutno nastavljen fiksni e-naslov, ki ima dostavo dovoljeno (`primoz.hrovat.96@gmail.com`). V praksi se ta storitev proti plačilu lahko uporablja nemoteno. Varovanje registracije novih uporabnikov varuje pred zlonamernimi programi - pajki, ki avtomatsko izpolnjujejo nezaščitene spletne obrazce. S CAPTCHO jim delo vsaj otežimo, s potrditvenim sporočilom pa registracijo sicer izvedemo, ven-

dar nepotrjene uporabnike po določenem času pač iz baze izbrišemo.

Za konsistentnost podatkovne baze skrbijo bazni prožilci ter omejitve tujih ključev.

V Android aplikacijo se lahko prijavi le prej registriran uporabnik, ki za prijavo potrebuje e-mail in geslo. V kolikor se skuša prijaviti z napačnim geslom ali napačnim e-mailom ga aplikacija na to opozori, ko pritisne gumb "Prijava". Ko uporabnik vnese veljaven e-mail in geslo, se pošlje zahtevo na strežnik, ki vrne objekt, če je bila prijava uspešna, sicer vrne "null". Vrnjen objekt se shrani v "ApplicationObject", kateri se preverja na vsaki strani aplikacije. V kolikor se uporabnik odjavi iz aplikacije, se njegov objekt nastavi na "null".

Ob prijavi se uporabniku dodeli seja, ki jo mobilna aplikacija shrani in jo z vsakim naslednjim zahtevkom pošilja strežniku, s čimer se preveri, ali je uporabnik že bil overjen ali ne.

Poglavje 5

Izjava o avtorstvu seminarske naloge

Spodaj podpisani *Primož Hrovat*, vpisna številka 63150113, sem (so)avtor seminarske naloge z naslovom *Implementacija spletne prodajalne in odjemalca za Android*. S svojim podpisom zagotavljam, da sem izdelal ali bil soudeležen pri izdelavi naslednjih sklopov seminarske naloge:

- načrtovanje in izvedba podatkovne baze
- izvedba strežniškega in odjemalskega dela spletne aplikacije za stranko
- izvedba strežniškega in odjemalskega dela spletne aplikacije za prodajalca
- izvedba strežniškega in odjemalskega dela spletne aplikacije za administratorja
- izvedba dodatnih razširitev za spletno aplikacijo (Email, Captcha, dnevnik, CSS, JS, ocenjevanje, iskanje, slike)

Podpis: Primož Hrovat, l.r.

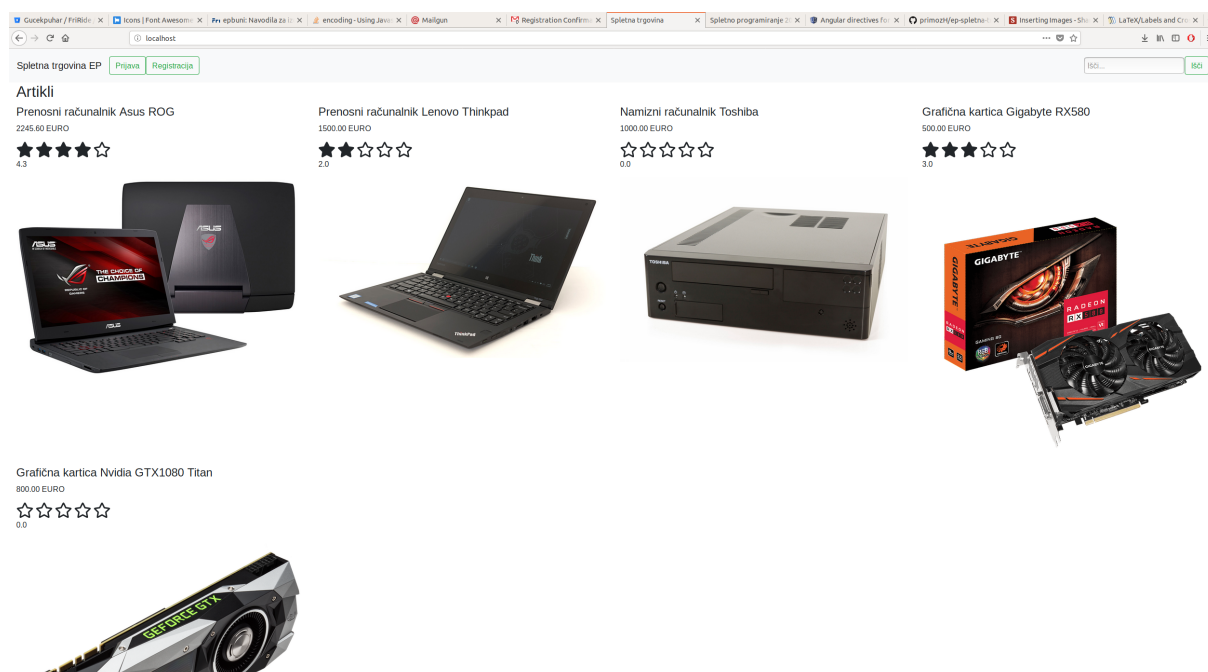
Spodaj podpisana *Miha Mazovec*, vpisna številka 63150193, sem (so)avtor seminarske naloge z naslovom *Implementacija spletne prodajalne in odjemalca za Android*. S svojim podpisom zagotavljam, da sem izdelal ali bil soudeležen pri izdelavi naslednjih sklopov seminarske naloge:

- načrtovanje podatkovne baze
- izvedba strežniškega in odjemalskega dela spletne aplikacije za stranko
- izvedba odjemalskega dela spletne aplikacije za prodajalca
- izvedba odjemalskega dela spletne aplikacije za administratorja
- izvedba mobilne aplikacije Android

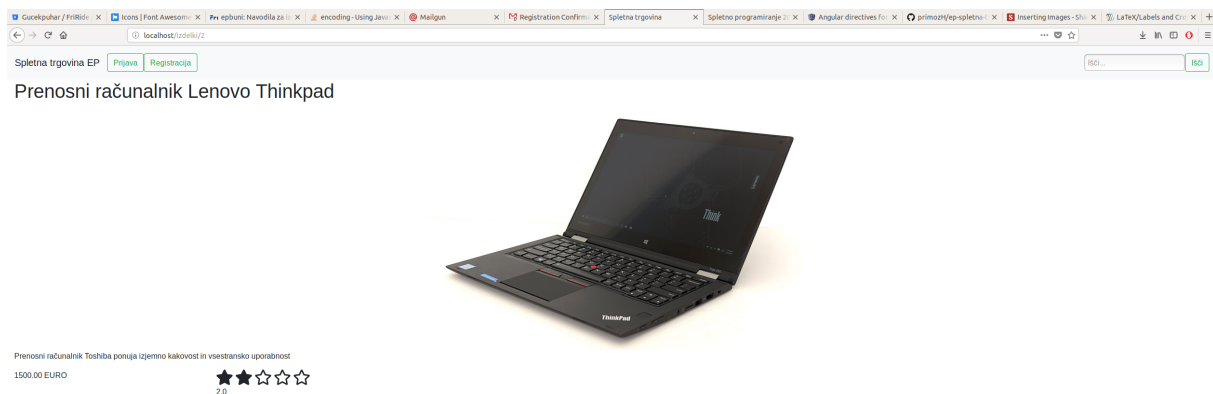
Podpis: Miha Mazovec, l.r.

Poglavje 6

Zaslonske slike - spletna aplikacija



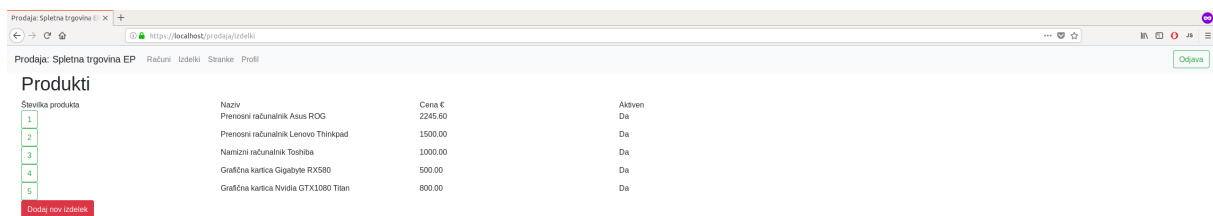
Slika 6.1: Začetna stran



Slika 6.2: Podrobnosti izdelka

Prodaja: Spletna trgovina EP				Zgodovina naročil			
Odporna naročila							
Račun	Id. stranke	Znesek		Datum	Račun št.	Id. stranke	Znesek
3	5	800.00		2018-01-13	1	4	3745.60
6	5	0.00		2018-01-13	2	5	500.00
7	5	0.00		2018-01-13	4	5	2000.00
8	5	0.00		2018-01-13	5	5	500.00
9	5	0.00					
10	5	0.00					
11	5	0.00					
12	5	0.00					
13	5	0.00					
14	5	0.00					
15	5	0.00					
16	5	0.00					
17	5	0.00					
18	5	0.00					
19	5	0.00					
20	5	500.00					
21	5	0.00					
22	5	0.00					
23	5	0.00					
24	5	0.00					
25	5	0.00					
26	5	0.00					
27	5	0.00					
28	5	0.00					
29	5	0.00					
30	5	500.00					
31	5	0.00					
32	5	0.00					
33	5	0.00					

Slika 6.3: Začetna stran - prodaja



Slika 6.4: Nadzorna plošča izdelkov - prodaja

Poglavje 7

Zaslonske slike - Android aplikacija



Slika 7.1: Pregled artiklov



Slika 7.2: Prijavno okno

ep-trgovina-android

Ime: Janez

Priimek: Novak

Email: janez@novak.si


Naslov: Borovnica 12

Tel. st.: 041999999

POSODOBI

Slika 7.3: Podatki uporabnika

ep-trgovina-android



**Prenosni računalnik
Lenovo Thinkpad**

1500.0 € Ocena: 2.0

Prenosni računalnik Toshiba ponuja izjemno kakovost in vsestransko uporabnost

Slika 7.4: Podrobnosti artikla

Poglavje 8

Zaključek

Pri izdelavi seminarske naloge sva naletela na kar precej izzivov, ki sva jih bolj ali manj uspešno tudi rešila. Poseben izziv nama je predstavljalo samo učenje ogrodja Laravel in implementacija mobilnega odjemalca za Android. Laravel sam po sebi kot ogrodje omogoča ogromno nastavitev in opcij, ki se jih je potrebno zavedati in se sprva težko znajdeš že v osnovnem projektu. Pri spoznavanju okolja zelo pomaga obširna uradna dokumentacija, dostopna preko spleta [1]. Operacijski sistem Android je še toliko obsežnejši, kar predstavlja dodaten izziv, v pomoč pa je razvijalsko ogrodje Android Studio in pa uradna dokumentacija [2], prav tako dostopna prek spleta.

Pri izdelavi seminarske naloge sva predvsem začutila utrip razvijalskega življenja in na lastni koži občutila, s kakšnimi problemi se srečujemo v vsakdanjiku neke razvojne ekipe. Od naloge sva odnesla veliko novega in uporabnega znanja, ki nama bo koristilo na nadaljni karierni poti.

Literatura

[1] *Laravel* <https://laravel.com> 15

[2] *Android Developers* <https://developer.android.com/index.html> 15