UNIVERZA V LJUBLJANI

FAKULTETA ZA RAČUNALNIŠTVO IN INFORMATIKO

# E-Trgovina

Poročilo seminarske naloge pri predmetu
Elektronsko poslovanje

**Študenti**
Uroš Gril (63170105)

**Mentor**
David Jelenc

Ljubljana, 10. januar 2022

# Kazalo


1 Uvod 2

2 Navedba realiziranih storitev 3

3 Podatkovni model 4

4 Varnost sistema 6

5 Izjava o avtorstvu seminarske naloge 7

6 Literatura 8

# Poglavje 1

# Uvod

Podana je naloga izdelati model spletne prodajalne z uporabo tehnologij Linux, Apache, SUPB MySQL, PHP, SSL, certifikatov X.509 in mobilne platforme Android. Potrebno je realizirati štiri različne tipe uporabnikov, vsakega s svojimi pravicami in omejitvami. Da se ne bi omejitve kršile, je potrebno paziti tudi na posebne vrste napadov na spletne strani, npr. SQL Injection in XSS napad.

# Poglavje 2

# Navedba realiziranih storitev

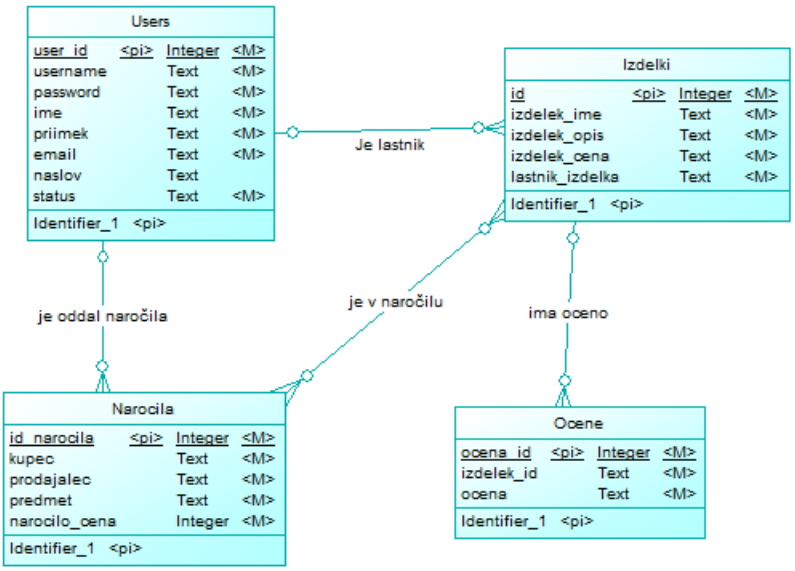
Od razširjenih storitev sta implementirani ocenjevanje izdelkov ter CAPTCHA. Ocenjevanje je prisotno pri vseh izdelkih z manjšo napako. Ko se izvede, stran prikaže "Error", vendar se ob ponovnem obisku strani z izdelki ocena upošteva. Kar pomeni da funkcijonalnost v celoti deluje kot bi morala, čeprav se ob njej pojavi error. CAPTCHA pa je prisotna pri ustvarjanju uporabnika. Če je ne izpolnimo, uporabnika ne moremo registrirati.

Ob obveznih storitev pa ni v celoti implementirano naročilo. Storitev je implementirana do točke ko se stranki izstavi predračun, vendar pa naročilo/potrditev naročila še nista implementirani. V celoti ni implementirana tudi urejanje računov s strani Administratorja in Prodajalca. Trenutno imata oba moč urejati vse račune, ne glede na njihovo omejitev. Ta omejitev manjka pri obeh, drugače je pa storitev implementirana. Deaktivacija računa se mi zdi trivialna, npr. uporabniku se zamenja geslo. Za naše pogoje menim da je to dovolj, saj sedaj ta uporabnik ne more več dostopati do spletne strani. Taka metoda se lahko pojavi tudi v praksi. Potreben je še popravek da se z X.509 certifikati prijavljata le administrator ter trgovec, trenutno je implementirano da ga potrebujejo vsi. Implementirana pa ni tudi aplikacija Android.

# Poglavje 3

# Podatkovni model

V podatkovnem modelu so 4 tabele. Vse so dokaj trivialne. Tabela Ocene vsebuje ocene izdelkov ter id izdelka, ki ga ocenjuje. Narocila vsebujejo ID narocnika (kupec), ID prodajalca, predmet ki bo kupljen ter ceno. Tabela Izdelki vsebuje osnovne podatke o izdelkih. Ime izdelka, opis, ceno ter prodajalca (lastnika izdelka). Edina netrivialna tabela pa so Users, kjer se v tabeli nahajajo vsi trije možni uporabniki. Administrator, Prodajalec in Kupec. Loči se jih po atributu status. Poleg tega se navajajo njihovi username, password, ime, priimek, email in naslov. Naslov ni obvezen atribut, saj ga Administrator in Prodajalec ne potrebujeta.


Users
user_id <pi> Integer <M>
username Text <M>
password Text <M>
ime Text <M>
priimek Text <M>
email Text <M>
naslov Text
status Text <M>
Identifier_1 <pi>
Izdelki
id <pi> Integer <M>
izdelek_ime Text <M>
izdelek_opis Text <M>
izdelek_cena Text <M>
lastnik_izdelka Text <M>
Identifier_1 <pi>
Je lastnik
je oddal naročila
je v naročilu
ima oceno
Narocila
id_narocila <pi> Integer <M>
kupec Text <M>
prodajalec Text <M>
predmet Text <M>
narocilo_cena Integer <M>
Identifier_1 <pi>
Ocene
ocena_id <pi> Integer <M>
izdelek_id Text <M>
ocena Text <M>
Identifier_1 <pi>

# Poglavje 4

# Varnost sistema

**Shranjevanje gesel** - gesla se shranjujejo v bazi, in ko se do njih dostopa se le te preverja preko hash vrednosti.

**Registracija z uporabo CAPTCHA** - prepreči robotske vnose pri registriranju nove stranke.

**Preprečevanje SQL Inject** - Vnosna polja se ne poganjajo direktno preko SQL-la, ampak se vežejo na spremenljivke - kar prepreči SQL inject.

**Preverjanje certifikatov** - V trgovino lahko vstopajo le posamezniki, ki imajo Certifikat, ki ga izdaja spletna stran.

# Poglavje 5

# Izjava o avtorstvu seminarske naloge

Spodaj podpisani *Uroš Gril*, vpisna številka *63170105*, sem (so)avtor seminarske naloge z naslovom *E-Trgovina*. S svojim podpisom zagotavljam, da sem izdelal ali bil soudeležen pri izdelavi naslednjih sklopov seminarske naloge:

- Prijavo in odjava Administratorja, Prodajalca, Stranke
- Implementacija Certifikatne Agencije in izdaja Certifikatov
- Posodobitev gesla in lastnih atributov strank
- Ustvarjanje in posodobitev računa Prodajalec s strani Administratorja
- Ustvarjanje in posodobitev računa Stranka s strani Prodajalca
- Funkcionalnost Nakupovanje pri Stranki
- Namestitev zavarovanega kanala https
- Registracija novih uporabnikov
- Poprava prijave, da je odporna na SQL Injection
- realizacija GET/POST metod
- Filtriranje registracije strank s CAPTCHA
- Ocenjevanje izdelkov
- Smiselna organizacija in izvedba vmesnika s pomočjo CSS

Podpis: Uroš Gril, l.r.

# Literatura


[1] Yank K. *Build Your Own Database-Driven Website Using PHP & MySQL*. SitePoint, 2003. ISBN-10: 0-957-92181-0.

[2] Michele D.; Jon P. *Learning PHP and MySQL*. O'Rielly, 2006. ISBN-10: 0-596-10110-4.

[3] Tim C.; Joyce P.; Clark M. *PHP5 and MySQL Bible*. Wiley Publishing, Inc., 2004. ISBN-10: 0-7645-5746-7

[4] Red Hat Software inc. *Linux Complete Command Reference*. Sams Publishing, 1997. ISBN-10: 0-672-31104-6.

[5] Ralf Spennberg. *IPsec HOWTO* (online). 2003. (citirano 10. januar 2022). Dostopno na naslovu: http://www.ipsec-howto.org/t1.html