UNIVERZA V LJUBLJANI

FAKULTETA ZA RAČUNALNIŠTVO IN INFORMATIKO

Spletna prodajalna

Poročilo seminarske naloge pri predmetu
Elektronsko poslovanje

Študenti
Klemen Klemar (63170143)
Bojan Ilic (63170362)
Matic Pirnat (63170230)

Mentor
David Jelenc

Ljubljana, 20. december 2020

Kazalo

Poglavje 1

Uvod

Za seminarsko nalogo smo pripravili spletno prodajalno z uporabo tehnologij Linux, Apache, SUPB MySQL, PHP, SSL, certifikatov X.509 in mobilne platforme Android. Za organizacijsko arhitekturo našega projekta smo uporabili MVC pristop. Za izpolnjevanje obrazcev smo uporabljali Pear QuickForm2. Slike smo pretvorili v *base64* in shranili v podatkovno bazo. Aplikacijo smo ustrezno zavarovali pred potencialnimi grožnjami kot so: SQL Injection in XSS napadi

Poglavje 2

Navedba realiziranih storitev

Pri našli alikaciji smo imlepmentirali naslednje razširjene storitve:

- Registracija strank z uporabo filtriranja CAPTCHA.
- Predstavitev artiklov s slikami. Slike slike smo shranili v SUPB. Implementacija podpira dodajanje in brisanje slik ter možnost dodajanja več slik za vsak artikel.
- Implementacija iskanja po artiklih. Iskalnik podpira binarno iskanje.
- Implementacija ocenjevanja artiklov prijavljenega uporabnika ter predstavitev njihove povprečne ocene pri njihovem ogledu. Ocene so prestavljene z zvezdicami.
- Prijava in odjava v mobilni aplikaciji.
- Pregled profilnih podatkov (ime, priimek, email, geslo, naslov ipd.) ter možnost njihovega spreminjanja v mobilni aplikaciji

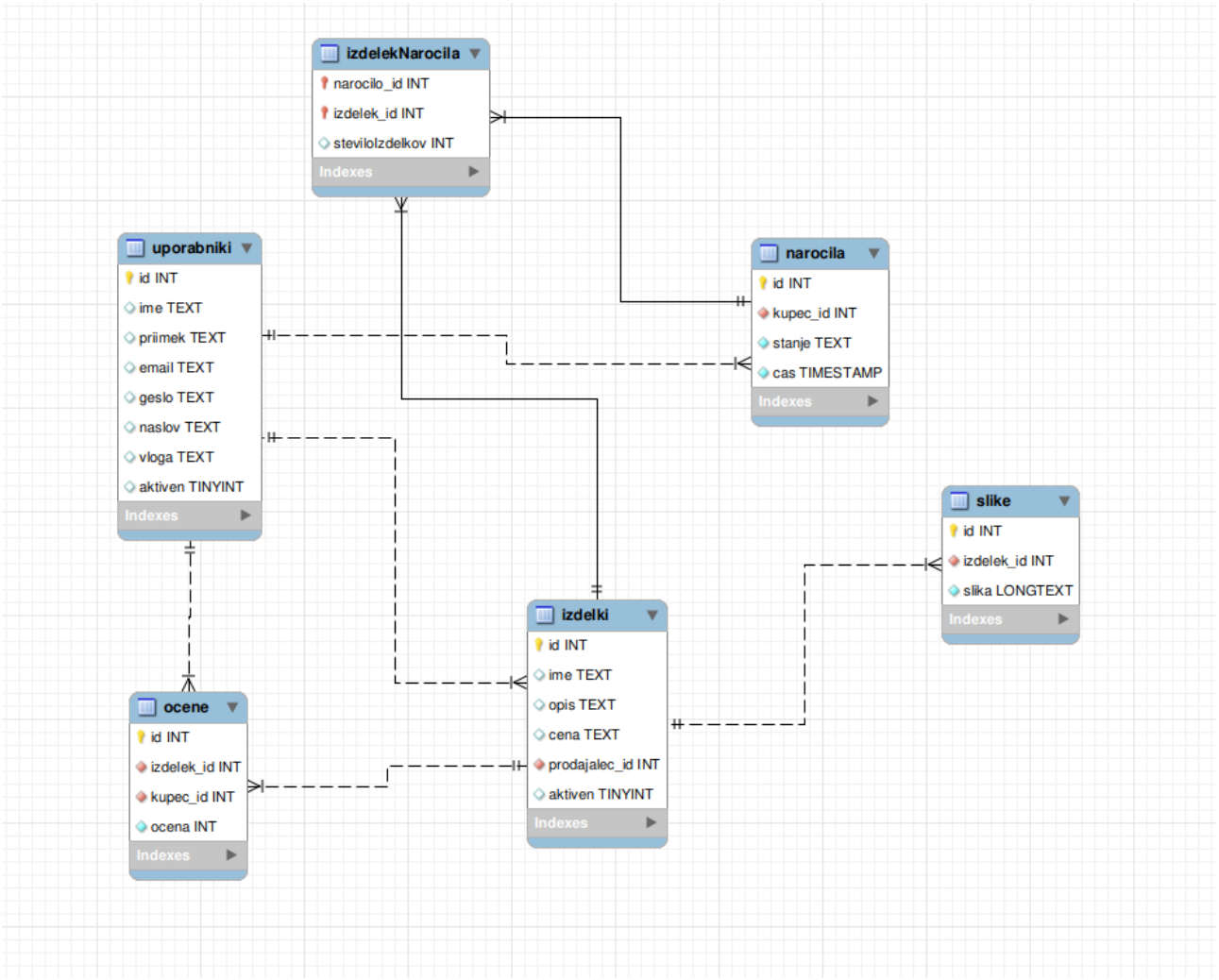
Poglavje 3

Podatkovni model

Naša podatkovna baza **uporabniki** vsebuje naslednje tabele:

- uporabniki - hrani uporabnike: administratorja, prodajalce in stranke.
- izdelki - hrani izdelke ter id prodajalca, ki ga je vpisal v bazo.
- narocila - hrani naročila, trenutno stanje obdelave ter čas oddaje naročila.
- izdelekNarocila - predstavlja *vmesno* tabelo med izedlki in narocili, torej za vsak id izdelka (izdelek_id), hrani id naročila (narocilo_id), ter količino tega izdelka v tem naročilu (steviloIzdelkov).
- ocene - hrani ocene izdelka. Za vsakega uporabnika (kupec_id) se hrani njegova ocena (ocena) za izdelek (izdelek_id).
- slike - hrani slike izdelka. Za vsak izdelek (izdelek_id) se hrani njegova slika (slika_id).

Naslov smo zaradi lažje obravnave hranili kot en atribut.



Slika 3.1: Slika podatkovne baze

Poglavje 4

Varnost sistema

4.1 Preklapljanje na zavarovan kanal

Spletna trgovina je anonimnim uporabnikom dostopna tudi preko nezavarovanega kanala, ampak ima le omejeno funkcionalnost. Preko nezavarovanega kanala lahko anonimni uporabniki le brskajo po izdelkih in jih dodajajo v košarico. Takoj, ko se pa želijo prijaviti ali registrirati, da bi zaključili nakup, pa se povezava preusmeri na zavarovan kanal.

4.2 Shranjevanje gesel

Vsa gesla so pred vpisom v podatkovno bazo šifrirana z algoritmom MD5 in uporabo soli. To smo implementirali z vgrajeno funkcijo *crypt()*. Gesla se preverjajo tako, da se vnos najprej filtrira, potem kriptira na enak način, kot pri registraciji, potem se pa zgoščena vrednost primerja s tisto, ki je v podatkovni bazi.

4.3 Registracija strank z uporabo filtriranja CAPTCHA

Pri registraciji nove stranke, smo za preprečevanje robotskih vnosov uporabili CAPTCHA_Numeral znotraj QuickForm2 obrazca iz knjznice Pear. Uporabnik mora za registracijo rešiti preprost račun.

4.4 Preprečevanje injekcije kode SQL

Vse vhode, ki jih strežnik pridobi z zahtevama POST in GET, smo prefiltrirali s pomočjo funkcije *filter_input()*.

4.5 Prijava in odjava na spletni aplikaciji

Kot omenjeno že zgoraj, je prijava dostopna le preko zavarovanega kanala. Osebje, torej prodajalci in admin, pa se za prijavo potrebujejo še overiti s pomočjo certifikata X.509. Za uspešen vpis mora biti poleg pravilnega gesla tudi vpisan email enak tistemu, kot je na certifikatu.

4.6 Prijava na Android aplikaciji

Na aplikacijo se lahko prijavljajo samo uporabniki tipa stranka. Preveri se njihov vnos email naslov in gesla. Email in geslo se nato preko POST zahteve pošljeta na strežnik, kjer se geslo kriptira in preveri, ali je zgoščena vrednost enaka tisti, ki je zapisana v podatkovni bazi. Če je, strežink odgovori z odgovorom 200 OK, če pa je geslo napačno pa z odgovorom 401 Unauthorized. V primeru, da je uporabnik neaktiven, pa strežnik pošlje odgovor 403 Forbidden.

Poglavje 5

Izjava o avtorstvu seminarske naloge

Spodaj podpisani *Klemen Klemar*, vpisna številka *63170143*, sem (so)avtor seminarske naloge z naslovom *Spletna prodajalna*. S svojim podpisom zagotavljam, da sem izdelal ali bil soudeležen pri izdelavi naslednjih sklopov seminarske naloge:

- Vzpostavitev lastne certifikalne agencije in strežniškega digitalnega potrdila
- Konfiguracija strežnika Apache
- Generiranje uporabniških certifikatov X.509
- Administrator: Prijava s certifikatom X.509 in odjava
- Šifriranje gesel ter API za preverjanje prijave
- Administrator: Posodobitev lastnega gesla in ostalih atributov
- Administrator: Ustvarjanje, aktiviranje in deaktiviranje računa Prodajalec ter posodobitev njegovih atributov
- Prodajalec: Prijava s certifikatom X.509 in odjava
- Prodajalec: Posodobitev lastnega gesla in ostalih atributov
- Prodajalec: Ustvarjanje, aktiviranje in deaktiviranje artiklov in posodabljanje njihovih atributov
- Prodajalec: Ustvarjanje, aktiviranje računov Stranka in posodabljanje njihovih atributov
- Stranka: Prijava in odjava
- Stranka: Posodobitev lastnega gesla in ostalih atributov
- Stranka: Dodajanje in odstranjevanje artiklov v košarico ter spreminjanje količine v košarici
- Anonimni odjemalec: Registracija preko spletnega vmesnika

- Preklapljanje med zavarovanim in nezavarovanim kanalom
- Registriranje strank z uporabo filtriranja CAPTCHA
- Implementacija iskanja po artiklih z binarnim iskanjem
- Implementacija ocenjevanja artiklov

Podpis: Klemen Klemar, l.r.

Spodaj podpisana *Bojan Ilic*, vpisna številka *63170362*, sem (so)avtor seminarske naloge z naslovom *Spletna prodajalna*. S svojim podpisom zagotavljam, da sem izdelal ali bil soudeležen pri izdelavi naslednjih sklopov seminarske naloge:

- Planiranje in ustvarjanje podatkovne baze
- Ustvarjanje naročil ter operacij nad njihovimi atributi
- Pregled naročil s strani stranke
- Pregled neobdelani, potrjenih, preklicanih in storniranih naročil s strani prodajalca
- Obdelava naročil v podatkovni bazi: potrjevanje, preklic, storniranje
- Ustvarjanje slik ter operacij nad njihovimi atributi
- Implementacija dodajanja in brisanja slik
- Razhroščevanje in popravki pri implementaciji prikaza izdelkov
- Razhroščevanje in popravki pri implementaciji košarice
- Kreiranje REST API-ja za izdekle in uporabnike
- Ustvarjanje ocen ter operacij nad njihovimi atributi
- Sodelovanje pri implementaciji ocenjevanja
- Sodelovanje pri varnostnih storitvah aplikacije
- Izdelava poročila

Podpis: Bojan Ilic, l.r.

Spodaj podpisana *Matic Pirnat*, vpisna številka *63170230*, sem (so)avtor seminarske naloge z naslovom *Spletna prodajalna*. S svojim podpisom zagotavljam, da sem izdelal ali bil soudeležen pri izdelavi naslednjih sklopov seminarske naloge:

- Android: Prikaz vseh izdelkov
- Android: Prikaz podrobnosti izdelka
- Android: Prijava
- Android: Povezava z bazo
- Android: Prikaz in urejanje profila

Podpis: Matic Pirnat, 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 20. december 2020). Dostopno na naslovu: http://www.ipsec-howto.org/t1.html