UNIVERZA V LJUBLJANI

FAKULTETA ZA RAČUNALNIŠTVO IN INFORMATIKO

E-TRGOVINA

Poročilo seminarske naloge pri predmetu
Elektronsko poslovanje

Študenti
Tjaša Domadenik (63180086)
Aljaž Jazbec (63180125)

Mentor
David Jelenc

Celje, 20. december 2020

Kazalo

Poglavje 1

Uvod

V okviru seminarske naloge sma implelentirala spletno trgovino z različnimi izdelki. Obseg spletne strani je odvisen od tipa uporabnika (administrator, prodajalec, stranka ter anonimni odjemalec). Poleg same spletne strani pa sva naredila tudi android aplikacijo, ki omogoča pregled izdelkov.

Poglavje 2

Navedba realiziranih storitev

Osnovni del je implementiran v celoti.

2.1 Administrator

Administrator ima nadzor nad vsemi funkcionalnostmi spletne strani. Kreiranje administratorja poteka ročno preko url naslova "localhost/netbeans/seminarska_naloga/index.php /seminarska_naloga/dodajanjeUporabnikov", ki poleg administratorja kreira tudi testne uporabnike.

Funkcionalnosti:

- Prijava omogočena zgolj preko certifikatov X.509.
- Posodabljanje lastnega gesla in ostalih atributov preko zavihka *uredi profil* na spletni strani.
- Lahko ustvari, aktivira, deaktivira, posodablja ter briše račune prodajalcev in strank.
- Vse funkcionalnosti stranke ter prodajalca

2.2 Prodajalec

Prodajalec ima nadzor nad naročili, artikli ter strankami. Posamezna naročila se prodajalcu prikažejo, ko jih stranke oddajo. Ima možnost potrditve ali preklica oddanih naročil, ogleda zgodovine potrjenih naročil in možnost stoniranja le-teh.

Funkcionalnosti:

- Lahko prijavi le preko certifikatov X.509.

- Mogoča posodovitev lastnega gesla in ostalih atributov.
- Ima pregled nad neobdelanimi naročili in njihovimi postavkami.
- Ustvari, aktivira in deaktivira posamezen artikel in mu posodablja atribute.
- Ustvarja, posodablja, briše, aktivira in deaktivira račune stranke.

2.3 Stranka

Stranka ima dostop do trgovine in možnosti nakupovanja. Lahko pregleduje artikle trgovine, jih dodaja in odstranjuje iz košarice ter spreminja količino izdelkov. Po zaključku nakupa vidi povzetek kupljenih izdelkov s predračunom. Po potrditvi naročila gre le-ta v čakalno vrsto neobdelanih naročil. Uporabnik ima dostop do seznama vseh svojih preteklih nakupov. Deluje samo na zavarovanem kanalu (https).

Funkcionalnosti:

- Prijavo in odjava.
- Posodobitev artibutov in gesla.
- Nakupovanje.

2.4 Anonimni odjemalec

Omogočeno mu je pregledovanje artiklov, registracija, delovanje je omogočeno tako na zavarovanem kot tudi nezavarovanem kanalu.

2.5 Vmesnik mobilne aplikacije

Omogoča pregledovanje artiklov v spletni trgovini. Aplikacija s prodajalno komunicira preko REST API-ja. Možno je brskanje po artiklih: seznam vseh artiklov ter ogled podrobnosti izbranega artikla (ob kliku na artikel).

2.6 Ostale zahteve

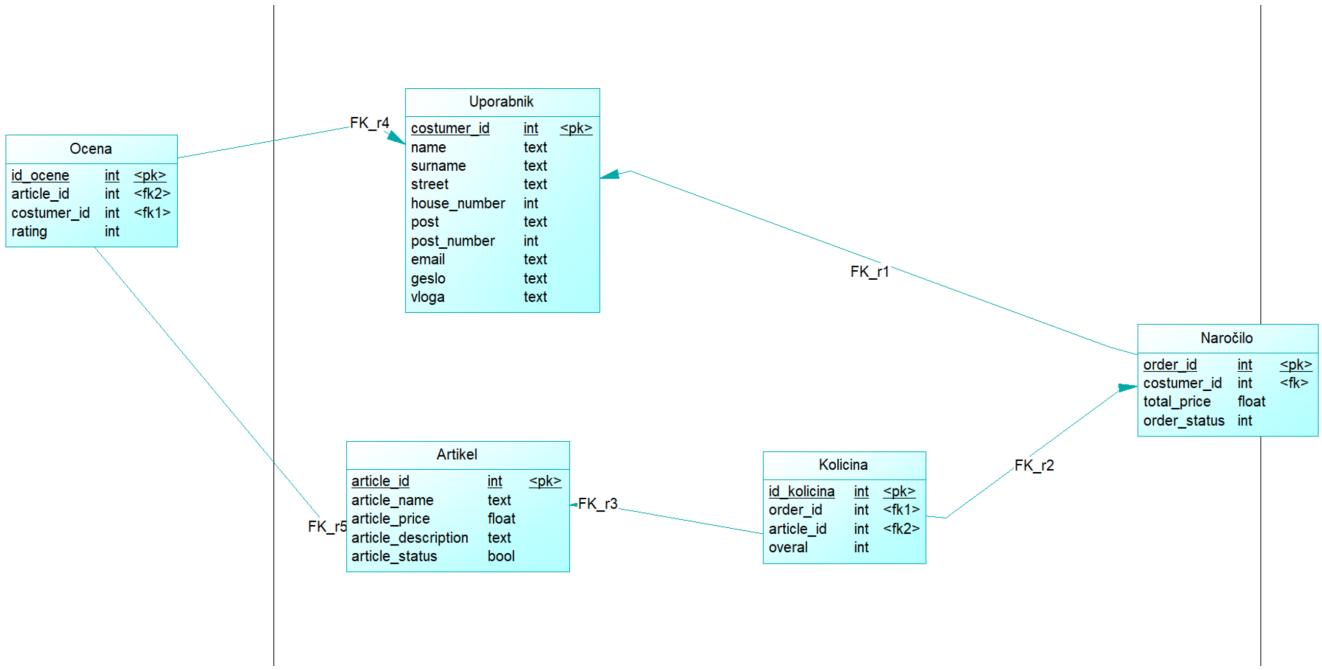
Izdelana je certifikatna agencija in strežniško digitalno potrdilo (nahajajo se v datoteki certs). Nameščeni so v strežnik Apache. Izdelani so tudi osebni certifikati za administratorja in prodajalca, oba sta s certifikatom povezana preko e-mail naslova (baza - certifikat).
Napadi XSS so preprečeni z uporabo funkcije htmlspecialchars() pri vseh izrisih strani (views), SQL injection pa je preprečen z uporabu spremenljivk bind pri vnosih v bazo. Gesla so hranjena ustrezno z šifriranjem. Metode protokola HTTP so realizirane v skladu s priporočili standarda HTTP (zahtevki z metodo GET za lahke operacije, metoda POST za zahtevnejše). Baza je normalizirana do 3NO, spodaj je priložena slika 3.1.

2.7 Razširjene storitve

V celoti sva implementirala varnostne storitve: registracijo z uporabo filtra CAPTCHA ter registracijo strank z uporabo potrditvenega e-maila.
Pri uporabniškem vmesniku je delno implementirana smiselna organizacija in izvedba uporabniškega vmesnika, saj tehnologij AJAX in podobnih nisma uporabljala. Prav tako je delno implementirana predstavitev artiklov s slikami, saj omogoča samo prikaz v naprej shranjenih slik, in sicer prikaz ene ali več slik za posamezen izdelek, ne omogča pa dodajanja in spreminjanja slik. V popolnosti sta implemenitrani zahtevi iskanje po artiklih in ocenjevanje izdelkov.
Pri Naprednih funkcijah mobilne aplikacije sta v celoti implemenitrana prijava in odjava uporabnika ter pregled profilnih podatkov in njihovo posodabljanje.

Poglavje 3

Podatkovni model



Slika 3.1: Slika Podatkovna baza

Uporabljenih je pet tabel. Tabela Ocena se uporablja za shranjevanje ocen uporabnikov o posameznih izdelkih. Tabela Uporabnik vsebuje atribute posameznega uporabnika. V tabeli Naročilo so atributi naročila, preko tabele Količina pa se dostopa do vseh postavk posameznega naročila (atribut overal predstavlja izbrano količino določenega izdelka). V tabeli Artikel so shranjeni osnovni podatki o artiklih.

Poglavje 4

Varnost sistema

Dostop do funkcionalnosti spletne aplikacije je zavarovan na več načinov:

- Za administratorja in uporabnika je potrebna prijava z certifikatom (kar poveča varnost ob prijavi).
- Dostop do posameznih strani je omejen preko sej - npr. stranka nima dostopa do urejanja artiklov.
- Pri registraciji se uporablja filter CAPTCHA, ki onemogoči robotske napade (registracije) na spletno stran.
- Z metodo hmtlspecialchars() se preprečuje XSS napade pri izrisu strani.
- Z uporabo bind spremenljivk pri delu z bazamo se onemogoči možnost napada SQL injection.

Poglavje 5

Izjava o avtorstvu seminarske naloge

Spodaj podpisani *Tjaša Domadenik*, vpisna številka *63180086*, sem (so)avtorica seminarske naloge z naslovom *E-TRGOVINA*. S svojim podpisom zagotavljam, da sem izdelala ali bila soudeležena pri izdelavi naslednjih sklopov seminarske naloge:

- Implementacija osnovnih storitev:
  - vzpostavitev baze
  - upravljanje z uporabniki (prijavljanje, odjavljanje, omogočanje, spremembe atributov, registracija)
  - vmesnik mobilne aplikacije (Android)
  - hramba gesel
  - preprečitev XSS napadov in SQL injection
  - ustrezna raba protokola HTTP

- Razširjene storitve:
  - Uporabniški vmesnik(V1*)
  Napredne funkcije mobilne aplikacije -> A1, A1

Podpis: Tjaša Domadenik, l.r.

Spodaj podpisana *Aljaž Jazbec*, vpisna številka *63180125*, 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:

- Implementacija osnovnih storitev:
  - vzpostavitev baze
  - upravljanje z atributi in naročili
  - košarica
  - zavarovanje kanalov
  - delo s certifikati (ustvarjanje, dodajanje, prijava s certifikatom), preprečitev XSS napadov in SQL injection
  - ustrezna raba protokola HTTP

- Razširjene storitve:
  - Varnostne storitve (V1, V2)
  - Uporabniški vmesnik (V1*, V2*, V3, V4)

Podpis: Aljaž Jazbec, l.r.