UNIVERZA V LJUBLJANI

FAKULTETA ZA RAČUNALNIŠTVO IN INFORMATIKO

Izdelava spletne trgovine TopShop

Poročilo seminarske naloge pri predmetu
Elektronsko poslovanje

Študenti
Robert Barachini (63150045)
Aleksandar Hristov (63150112)
Jernej Vrhunc (63150316)

Mentor
David Jelenc

Ljubljana, 13. januar 2019

Kazalo

Poglavje 1

Uvod

Cilj projekta in seminarske naloge je bila izdelava spletne trgovine z uporabo spletnih tehnologij in učenje uporabe dobrih varnostnih standardov. Aplikacijo smo razvijali v Linux operacijskem sistemu (Ubuntu virtualka in Ubuntu dual boot). Na sistem smo namestili Apache srežnik, ki servira PHP datoteke in jih s pomočjo MySQL podatkovne baze napolni s podatki. Naši rešitvi smo dodali še SSL/TLS protokol za varno izmenjavo podatkov preko omrežja. Za uporabniške račune z več pravicami pa smo s pomočjo svoje certifikatne agencije izdelali X.509 certifikate. Uporabili smo tudi tehnologije JavaScript in BootStrap za izgradnjo dinamične spletne strani z modernim izgledom, ki je uporabna na poljuni napravi (preverili smo delovanje v braskalniku na majhnem zaslonu - tablici, na navadnem brskalniku - Mozilla in na pametnem telefonu - emulator Android). Poleg spletne aplikacije smo v AndroidStudio v Kotlinu izdelali tudi Android aplikacijo, ki preko REST API-ja komunicira s strežnikom. REST klice smo testirali z orodjem Postman. Pri izgradnji baze pa nam je koristilo orodje MySQL Workbench.

Poglavje 2

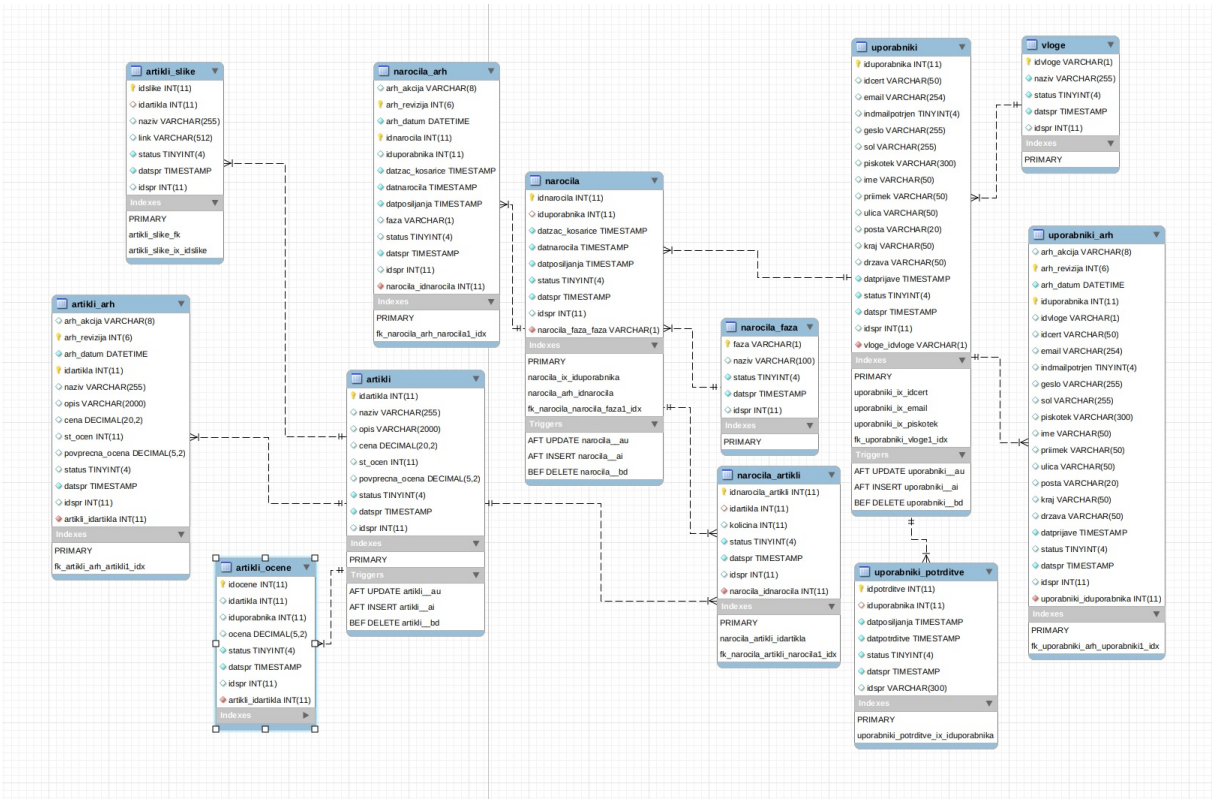
Navedba realiziranih storitev

V okviru hranjenja dnevnikov smo realizirali rešitev v obliki arhivskih tabel, ki so vezane na triggerje njihovih osnovnih objektov na bazi. V bazi se za vse uporabnike (ne le za administratorja in prodajalce), artikle in naročila vodijo arhivske tabele, kjer se preko triggerjev beleži celotna zgodovina operacij nad temi objekti in se potemtakem lahko rekonstruira celoten postopek izvajanja. Pri registraciji uporabljamo tudi Googlovo storitev CAPTCHA. Ob registraciji se pošlje tudi potrditveni e-mail. Uporabniški vmesnih smo oplemenitili z uporabo CSS, Bootstrap in JavaScript, ter dinamično izvajanje s tehnologijo AJAX. Artikle lahko tudi ocenjujemo. Za vsak artikel se beležijo ocene uporabnikov, število ocen in povprečno oceno izdelka. Vsak artikel podpira dodajanje in prikaz več slik, ki se hranijo na filesystemu. Slike lahko dodajamo in brišemo. Za bolj napredne mobilne rešitve je zmanjkalo časa, smo pa naredili zelo obsežno ogrodje spletnega odjemalca, ki omogoča, da bi poleti naredili svojo spletno trgovino, ki bi jo uporabili za različne namene. Prav tako je v ozadju že pripravljeno beleženje vseh uporabnikov (tudi anonimnih), saj se na bazi lahko hrani piškotke za vsakega uporabnika in tudi uporavnike anonimnega tipa, kar pomeni, da je en brskalnik en anonimni uporabnik. Z uporabo te funkcionalnosti bi lahko anonimni uporabnik brez prijave dodajal izdelke v košarico, pri prijavi v obstoječi uporabniški račun pa bi se vsebina košarice prenesla prijavljenemu uporabniku. Takšno napredno funkcionalnost podpirajo nekatere največje spletne trgovine. Prav tako smo realizirali celoten REST API in bazo, ter backend na ločenih nivojih, kar omogoča lažjo menjavo med tehnologijami, če bi se tako odločili.

Poglavje 3

Podatkovni model

Spodnja slika prikazuje naš podatkovni model. Arhivske tabele so prikazane na desni strani. V njih se piše preko triggerjev.



Slika 3.1: Slika EER diagrama

Poglavje 4

Varnost sistema

Na nivoju komunikacije PHP vmesnika z bazo smo povsod uporabili Prepared Statemente in BindParam logiko. To onemogoča napad SQL injection. Napad XSS preprečujemo tako, da filtriramo znake iz vnosa s pomočjo funkcionalnosti htmlspecialchars(strip_tags()). Prav tako smo dodali certifikate za varen dostop in komuniciranje preko SSL/TLS (HTTPS). Naprednim uporabnikom je omogočen vstop s certifikatom X.509, kar dodatno poveča varnost. Za anonimnega uporabnika je omogočeno preklapljanje med HTTP in HTTPS stranmi, pri prijavi in registraciji pa se zahteva HTTPS za varen dostop. Uporabniki tipa Administrator in Prodajalec dostopajo do podatkov preko HTTPS. Pri registraciji smo prav tako implementiranje potrjevanje računov z uporabo potrditvenega e-mail sporočila in pa uporabo CAPTCHA.

Poglavje 5

Izjava o avtorstvu seminarske naloge

Spodaj podpisani *Robert Barachini*, vpisna številka *63150045*, sem (so)avtor seminarske naloge z naslovom *Izdelava spletne trgovine TopShop*. S svojim podpisom zagotavljam, da sem izdelal ali bil soudeležen pri izdelavi naslednjih sklopov seminarske naloge:

- Izdelava logike za bazo in inicializacijske skripte
- Izdelava ERR modela za bazo
- Postavitev začetnega projekta in nastavitev datotek ter osnovne logike delovanja strežnika
- Postavitev in voednje GIT repozitorija
- Celoten REST API za komuniciranje med backendom in bazo
- Kreiranje certifikatne agencije in certifikatov
- Izdelava Android aplikacije
- Beleženje arhivskih tabel
- Pisanje poročila

Podpis: Robert Barachini, l.r.

Spodaj podpisana *Aleksandar Hristov*, vpisna številka *63150112*, sem (so)avtor seminarske naloge z naslovom *Izdelava spletne trgovine TopShop*. S svojim podpisom zagotavljam, da sem izdelal ali bil soudeležen pri izdelavi naslednjih sklopov seminarske naloge:

- Stranka/Anonimni GUI
- Preklapljanje med zavarovanim kanalom in javnim za Stranko in Anonimnim
- Implementacija artiklov s slikami, celotna košarica in checkout, pregled preteklih narocil, ce so stornirani, oddani, potrjeni oziroma zavrnjeni. Spremembe na strani (kjer je to smiselno) so implementirane z Ajax klici. Uporaba CSS in JS.
- Registracija strank s CAPTCHO
- Registracija strank s potrditvenim emailom
- Binarni search

Podpis: Aleksandar Hristov, l.r.

Spodaj podpisana *Jernej Vrhunc*, vpisna številka *63150316*, sem (so)avtor seminarske naloge z naslovom *Izdelava spletne trgovine TopShop*. S svojim podpisom zagotavljam, da sem izdelal ali bil soudeležen pri izdelavi naslednjih sklopov seminarske naloge:

- Vmesnik za administratorja. Prijavljen uporabnik, ki ima vlogo administratorja('A') lahko dostopa do administratorske konzole dostopne na 'localhost/admin'. Na konzoli ima vpogled v vse obstoječe prodajalce(vloga: 'P') in lahko s klikom na njih dostopa na vpogled njihovih podatkov(ime, priimke, ulica, kraj, posta, drzava, email) in jih tudi spreminja. S klikom na gumb 'Dodaj prodajalca' lahko doda novega prodajalca. Prav tako lahko prodajalca aktivira oziroma deaktivira.

- Vmesnik za prodajalca: prijavljen uporabnik, ki ima vlogo prodajalca('P') lahko dostopa do konzole prodajalca dostopne na 'localhost/prodajalec. Na konzoli ima vpogled v vse obstoječe stranke(vloga: 'S') in lahko s klikom na njih dostopa na vpogled njihovih podatkov(ime, priimke, ulica, kraj, posta, drzava, email) in jih tudi spreminja. Prav tako ima na konzoli vpogled v vse obstoječe artikle in lahko s klikom na njih dostopa na vpogled njihovih podatkov(naziv, opis, cena) in jih tudi spreminja. Dostopa lahko tudi do dodajanje slike posameznemu artiklu. Vse stranke kot tudi artikle lahko aktivira in deaktivira. Ima pregled nad neobdelanimi naročili uporabnikov, ki jih lahko sprejme oziroma zavrne. Vsa že obdelana naročila se prikažejo v 'Zgodovini naročil'.

- Profil stranke: vsaki prijavljeni stranki je mogoče dostopati do svojega profila na 'localhost/profil'. Tam lahko ureja svoje podatke (ime, priimke, ulica, kraj, posta, drzava, email). Omogočeno je tudi spreminjanje gesla, registarcijo, prijavo in odjavo. na 'localhost/registracija' je možna registracija novega uporabnika. Za generiranje gesla smo uporabili random generirano sol. na 'localhost/prijava' je možna prijava uporabnika. Preveri se ali se email ujema s katerim iz baze in ali je geslo pravilno. Če je postopek prijave uspešen se uporabniku dodeli piškotek. Ob kliku na gumb 'Odjava' se uporabniku piškotek odvzame.

- Filtriranje artiklov na prvi strani - filtriranje artiklov glede na njihov status(Aktiviran, Deaktiviran)

Podpis: Jernej Vrhunc, l.r.

Poglavje 6

Zaključek

Med delom na projektu smo se naučili zelo veliko zanimivih stvari, ki jih bomo lahko koristno uporabili kasneje, ko se bomo spopadali z novimi problemi in iskali nove rešitve v produkcijskem okolju. Projekt je bil dober trening skupinskega dela in naučili smo se deliti naloge in komunicirati v prid kakovostnega razvoja. Uporabljali smo sistem za nadzorovanje verzij (GIT) in orodje Discord za komunikacijo. Dokumentacijo smo shranjevali v obliki deljenih datotek na Google Drive. Prepričani smo da nam bo pridobljeno znanje koristilo pri novih projektih.

Literatura

[1] David Jelenc *Prosojnice z vaj*. Spletna učilnica, 2018/2019.

[2] *PHP Documentation* (online). 2018/2019. (citirano 13. januar 2019). Dostopno na naslovu: http://php.net/docs.php

[3] *Various StackOverflow pages* (online). 2018/2019. (citirano 13. januar 2019). Dostopno na naslovu: https://stackoverflow.com/