UNIVERZA V LJUBLJANI

FAKULTETA ZA RAČUNALNIŠTVO IN INFORMATIKO

Spletna trgovina: Movie shop

Poročilo seminarske naloge pri predmetu
Elektronsko poslovanje

Študenti
Gašper Kočjaž (63120162)

Mentor
David Jelenc

Ljubljana, 30. junij 2020

Kazalo

Poglavje 1

Uvod

V sklopu vaj pri predmetu Elektronsko poslovanje, sem implementiral spletno trgovino za prodajo filmov. Implementacija temelji na sistemu XUbuntu 18.04, ki teče na priskrbljeni virtualki in strežniku Apache.

Pri delu sem uporabil namenske programe kot so NetBeans, MySQLWorkbench in AndroidStudio.

Seznam uporabljenih tehnologij:

- Linux & Apache
- PHP
- HTML & CSS
- MySQL
- SSL & certifikat X.509
- mobilna platforma Android

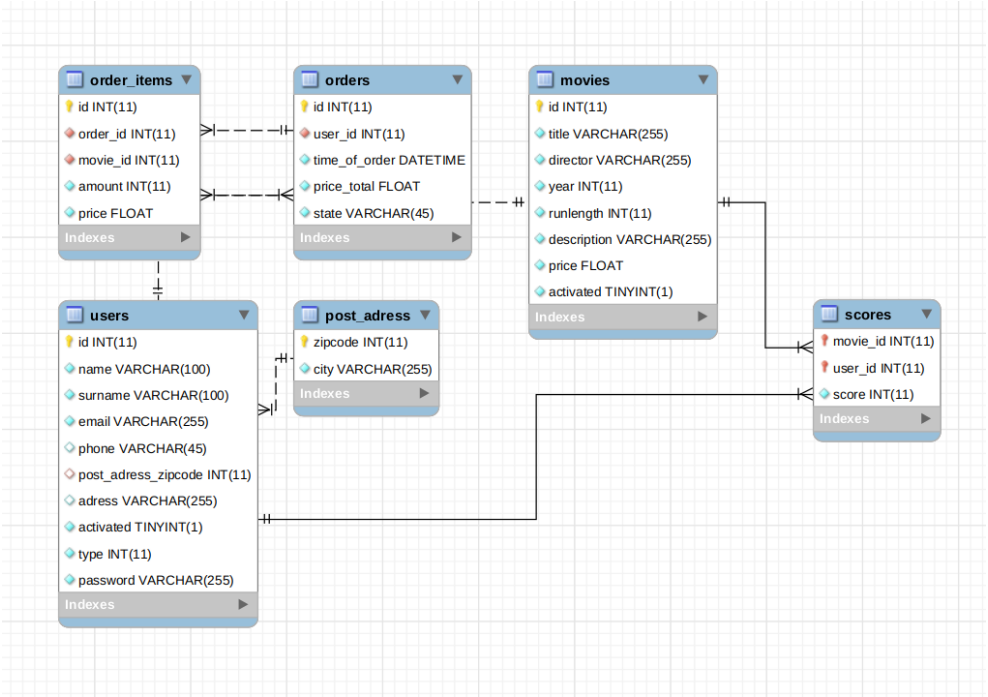
Poglavje 2

Navedba realiziranih storitev

Od razširjenih storitev sem implementiral **ocenjevanje artiklov** in **izgradnja uporabniškega vmesnika z uporabo CSS**.

Poglavje 3

Podatkovni model



Slika 3.1: Diagram podatkovnega modela

- **movies**:

  Tabela *movies* se nanaša na artikle oz. filme in hrani za to potrebne atribute kot so naslov filma, režiser, cena itd. Atribut *activated* pa pove ali je film aktiviran, torej ali je strankam na voljo za ogled oz. nakup.

- **scores**:

  V tabeli *scores* hranimo evidenco ocen, ki so jih podali uporabniki filmom. Posamezna ocena je identificirana po ID-ju filma in ID-ju uporabnika, ki je ocenil film. Nato lahko iz shranjenih ocen izračunamo povprečno oceno za določen film.

- **users**:

  Tabela hrani podatke o registriranih uporabnikih, ki se glede na vlogo (*type*) delijo na stranke, prodajalce in administratorja. Zaradi lažjega preverjanja hierarhije med uporabniki sem *type* definiral kot INT, ki lahko zavzame vrednosti 0 (stranka), 1 (prodajalec), ali 2 (administrator). Prav tako imajo uporabniki atribut *activated*, ki je prvotno nastavljen na FALSE, saj mora uporabnika po registraciji najprej potrditi avtorizirana oseba (prodajalec/administrator) - prav tako je uporabnik lahko deaktiviran.

  Za stranke hranimo še kontaktne podatke v obliki telefonske številke, poštne številke (tuj ključ iz tabele *post_adress*) in naslova bivanja.

  V *password* so varno shranjena zašifrirana uporabniška gesla.

- **post_adress**:

  Vsebuje številko pošte (ki se hrani v tabeli *users*) in ime mesta.

- **orders**:

  Vsako naročilo beleži ID uporabnika (tuj ključ *user_id*), ki je oddal naročilo ter čas in znesek. Hranimo tudi stanje naročila, ki je lahko neobdelano, potrjeno, preklicano ali stornirano.

- **order_items**:

  Predstavlja posamezen artikel (*movie_id*) v naročilu (*order_id*), za katerega beležimo naročeno količino in znesek.

Poglavje 4

Varnost sistema

Dostop do spletne strani in njenih funkcionalnosti je odvisen od vloge uporabnika (anonimni uporabnik, stranka, prodajalec/administrator), zato sem preverjal ustreznost vloge uporabnika in le-tega preusmeril ob neustreznem poskusu dostopa do "naprednih" funkcionalnosti. Poskrbel sem za ustrezno hrambo/šifriranje gesel z uporabo funkcij *password_hash()* in *password_verify()*, ter implementiral prijavo z uporabo X.509 certifikatov za prodajalce in administratorja.

Implementiral sem preklapljanje med nezavarovanim in zavarovanim kanalom pri interakciji z anonimnim uporabnikom oz. stranko, ter omejil prodajalce/administratorja na uporabo zavarovanega kanala po uspešni avtorizaciji z X.509 certifikatom.

Injekcijo SQL kode sem preprečil z uporabo pripravljenih poizvedb, ki jih omogoča PDO. Prav tako sem filtriral vse uporabniške vnose, ki so se prenesli na bazo, z uporabo funkcije *filter_input_array()*, da bi preprečil nepravilne interakcije z podatkovno bazo.

Za preprečevanje XSS napadov sem izvajal validacijo in filtriranje podatkov z uporabo filtrov kot so *FILTER_SANITIZE_SPECIAL_CHARS*, ki poskrbi, da se potencialno nevarni znaki (s katerimi bi izvedli XSS napad) pretvorijo v varno obliko.

Poglavje 5

Izjava o avtorstvu seminarske naloge

Spodaj podpisani *Gašper Kočjaž*, vpisna številka *63120162*, sem avtor seminarske naloge z naslovom *Spletna trgovina: Movie shop*. S svojim podpisom zagotavljam, da sem izdelal ali bil soudeležen pri izdelavi naslednjih sklopov seminarske naloge:

- Vse obvezne storitve
- Navedene razširjene storitve

Podpis: Gašper Kočjaž, l.r.

Poglavje 6

Zaključek

Izdelava seminarske naloge mi je dala dober vpogled v razvoj spletnih aplikacij za elektronsko poslovanje in nove izkušnje z uporabo orodij kot so AndroidStudio. Seveda bi bilo potrebno implementacijo v realnem svetu nadgraditi in še bolje zavarovati, saj gre za delo z občutljivimi podatki. Prav tako bi bilo potrebno dodati dinamičnost z uporabo tehnologij in ogrodij na osnovi JavaScripta, saj bi izboljšali tako privlačnost spletne trgovine in enostavnost uporabe oz. ozdivnost.