UNIVERZA V LJUBLJANI

FAKULTETA ZA RAČUNALNIŠTVO IN INFORMATIKO

EP Seminarska naloga - Spletna trgovina

Poročilo seminarske naloge pri predmetu
Elektronsko poslovanje

Študenti
Igor Žibert (63140300)

Mentor
David Jelenc

Ljubljana, 14. januar 2018

Kazalo

1 Uvod 2

2 Navedba realiziranih storitev 3

3 Podatkovni model 4

4 Varnost sistema 6

5 Izjava o avtorstvu seminarske naloge 7

Poglavje 1

Uvod

Tema seminarske naloge je izdelava spletne trgovine, preko katere imajo uporabniki možnost nakupovanja določenih izdelkov. Moja spletna trgovina uporablja za izdelke različna piva, katera lahko kupijo s pomočjo kreditne kartice. Prodajalcem je omogočen pregled nad vsemi oddanimi naročili, katera lahko sprejmejo ali zavrnejo. Lahko tudi spreminjajo podatke o uporabnikih in prekličejo njihove račune. Administratorju je omogočeno vse, razen da lahko zraven še spreminja račune prodajalcev.

Uporabljene tehnologije za realizacijo naloge so:

- Operacijski sistem Linux
- Strežnik HTTP Apache
- Podatkovna baza MYSQL
- Programski jezik PHP
- Protokol SSL
- Certifikati X.509
- Ogrodje Laravel
- Integrirano razvojno okolje Android Studio

Poglavje 2

Navedba realiziranih storitev

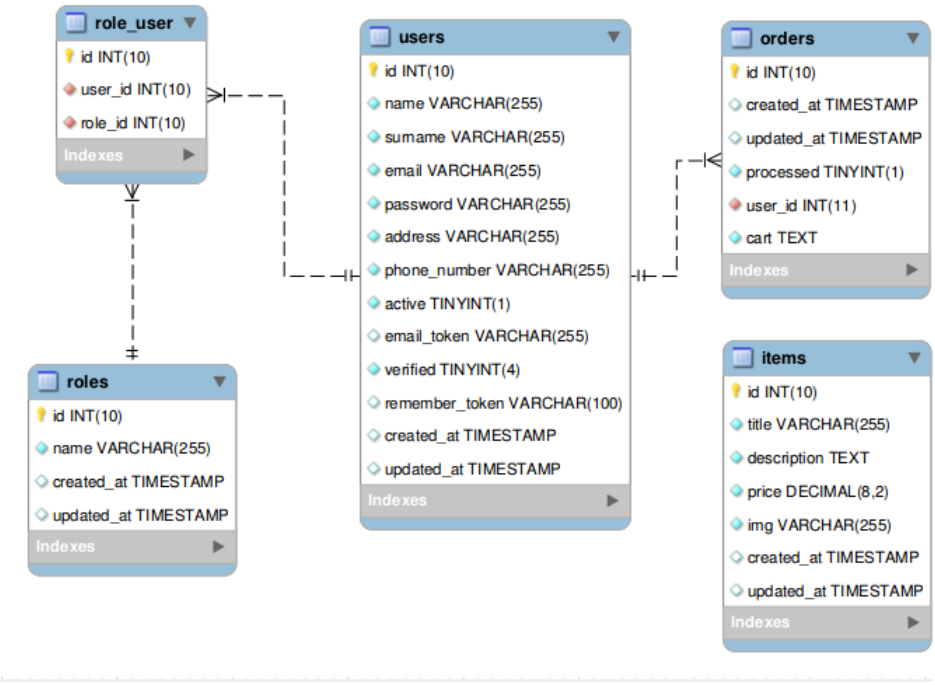
Implementiral sem sledeče razširjene storitve:

- Implementiral sem razširjeno storitev za varnost pri registraciji strank z uporabo filtriranja CAPTCHA. Pri registraciji se mora uporabnik validirati preko Google sistema reCAPTCHA s klikom na okence. Na strežniški strani se potlej preveri, ali je uporabnik prestal test in vrne primeren odgovor.
- Za varnost je bilo poskrbljeno tudi z aktivacijo upor. računov z uporabo potrditvenega e-maila preko protocola SMTP. Aplikacija se poveže na Gmail račun, s katerega se pošlje e-mail z aktivacijskem naslovom novemu uporabniku.
- Delno implementirana je 'Smiselna organizacija in izvedba uporabniškega vmesnika s pomočjo tehnologij kot so sta CSS in JavaScript'. Spletna stran uporablja Bootstrap 3.3.7 za izboljšavo uporabniške izkušnje na enostaven način. Uporablja se tudi ogrodje CSS Font Awesome, s katerim prikažem razne smiselne ikone, za hitrejšo navigacijo uporabnika. Vsa avtorska koda za oblikovanje se nahaja v CSS, JavaScript na odjemalčevi strani se pa uporablja zgolj za eno funkcijo. AJAX implementracije ni, saj ni bila potrebna.
- Prav tako je delno implementirana predstavitev artiklov s slikami. Slike se shranejujejo na datotečni sistem in se servirajo odjemalcu. Omogočeno je dodajanje in spreminjanje slike, ampak ne podpira več slik hkrati.

Splošne storitev, ki ni bila v celoti realizirana se tiče certifikatov. Strežnik ima svoj certifikat, s pomočjo katerega tudi zahteva povezave tipa HTTPS pri registraciji, prijavi in nakupu. Ne podpira pa overjanja uporabnikov s pomočjo osebnih certifikatov.

Poglavje 3

Podatkovni model



Slika 3.1: *
EER model podatkovne baze.

Tabele, ki jih uporabljam, so:

- Users, ki predstavlja uporabnike. Poleg trivialnih atributov uporablja tudi atribute 'verified' in 'email_token'. Uporabljata se pri implementaciji potrjevanja uporabnikov preko poslane e-pošte. Ko se uporabnik uspešno potrdi, se mu vrednost 'verified' spremeni na 1 in omogoči dostop do računa.
- Items, ki predstavlja artikle spletne trgovine. Atribut 'img' se tukaj nastavi na lokacijo slike na datotečnem sistemu.

- Orders, ki predstavlja oddana naročila uporabnikov. Uporabnik je predstavljen s tujim ključem in ima lahko več naročil. Netrivialni atribut je tukaj cart, ki predstavlja nakupovalno košarico uporabnika. Namesto dodatnih tabel se kar cela košarica zgradi 'in-memory' v obliki JSON objekta in serializira v tabelo. Ob branju naročila, se nad košarico uporabi metoda 'unserialize', ki zgradi privotni JSON objekt.
- Roles, ki predstavlja eno izmed treh vlog, 'Customer','Staff' ali 'Admin'.
- In tabelo Roles-User, ki povezuje uporabnika z določeno vlogo. En uporabnik ima lahko več vlog hkrati.

.

Poglavje 4

Varnost sistema

Laravel ima že v osnovi implementirane varnostne rešitve. Ogrodje pri izpisu s pomočjo značk ' <vsebina> ' uporablja php funkcijo 'htmlentities()' za preprečitev XSS napadov. Ta funkcija na vhod sprejme niz znakov, v izhodu pa pretvori vse značke HTML v entitete HTML. Npr. značka '<script>' se prevede v 'lt;scriptgt:'. Zaradi pretvorbe znakov '<' in '>' v entitete se brskalniku onemogoči uporaba teh znakov kot elemente HTML

Prav tako uporabljam Laravel-ov Eloquent ORM (Object-Relation Mapping), ki pa ustrezno priredi vnešene podatke pri delu z bazo. Na primer, vhod 'SELECT * FROM users WHERE email = 'jason@example.com' or 1=1' bi brez primerne zaščite izpisal vse podatke iz tabele users. Eloquent pa poskrbi, da se ta niz pretvori v 'SELECT * FROM users WHERE email = 'jason@example.com or 1=1'. Ker noben poštni naslov ni enak 'jason@example.com or 1=1', bi ta poizvedba vrnila 0 rezultatov.

Za preverjanje, ali ima uporabnik dovoljenje, da obišče določeno stran sem pa implementiral funkcijo, ki preverja katere vloge ima uporabnik. Če uporabnik nima vloge, ki bi mu to dovoljevala, se mu dostop prepreči.

Poglavje 5

Izjava o avtorstvu seminarske naloge

Spodaj podpisani *Igor Žibert*, vpisna številka *63140300*, sem avtor seminarske naloge z naslovom *EP Seminarska naloga - Spletna trgovina*. S svojim podpisom zagotavljam, da sem izdelal vse sklope seminarske naloge.