UNIVERZA V LJUBLJANI

FAKULTETA ZA RAČUNALNIŠTVO IN INFORMATIKO

Spletna trgovina

Poročilo seminarske naloge pri predmetu
Elektronsko poslovanje

Študenti
Matevž Fabjančič (63150086)
Andraž Povše (63150224)

Mentor
David Jelenc

Ljubljana, 11. januar 2018

Kazalo

Poglavje 1

Uvod

V uvodu podajte kratko predstavitev teme seminarske naloge ter navedite seznam uporabljene tehnologije.

PHP, MySQL, Bootstrap, QuickForms2 (treba instalirat), MVC arhitektura –

Poglavje 2

Navedba realiziranih storitev

Navedite, katere razširjene storitve ste implementirali. Če ste katero storitev implementirali le deloma, opišite, kako daleč ste z implementacijo prišli.

Prav tako navedite, če katero od obveznih storitev niste implementirali v celoti.

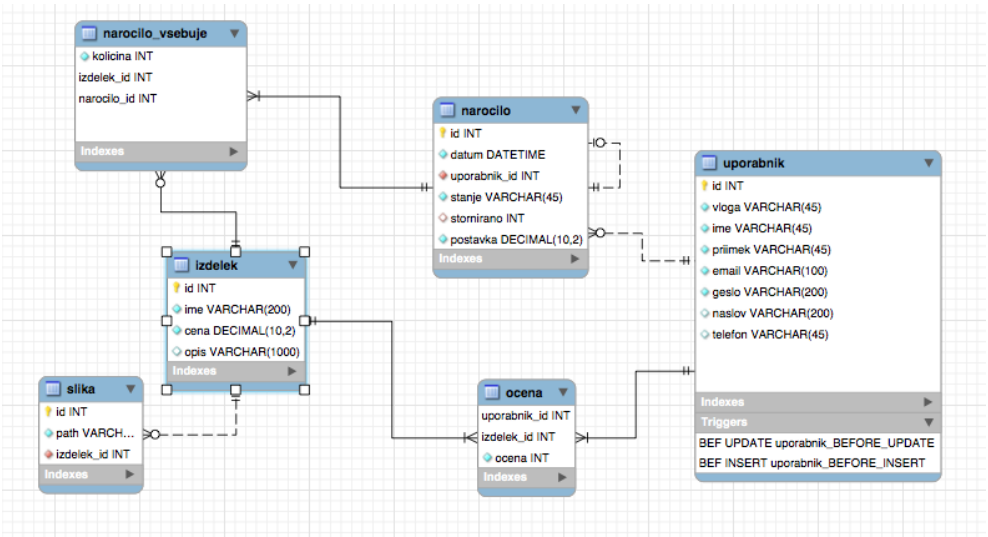
Poglavje 3

Podatkovni model

Podajte sliko logičnega podatkovnega modela (denimo iz programa MySQL Workbench) ter navedite in kratko opišite uporabljene tabele. Če katera vsebuje netrivialne atribute, jih pojasnite.

V podatkovni bazi sva ustvarila naslednje tabele:

- Uporabnik. Tabela vsebuje stranke, prodajalce in administratorje.
- Narocilo. Tabela vsebuje narocila.
- Izdelek. Tabela vsebuje izdelke z imenom, ceno in opisom.
- Slika. Tabela vsebuje tuji kljuc do izdelka in pot do slike v datotecnem sistemu.
- Ocena. Tabela vsebuje tuji kljuc do osebe, izdelka in podano oceno.
- Narocilo_vsebuje. Tabela vsebuje tuji kljuc do izdelka, narocila in kolicino narocenega izdelka.



Slika 3.1: Slika logicnega modela

Poglavje 4

Varnost sistema

Opišite implementirane mehanizme za nadzor dostopa ter ostale kontrole, ki ste jih implementirali. Pri vsake navedite, kaj je njen namen oz. katere varnostne grožnje preprečuje.

4.1 Preprečevanje injekcije kode SQL

Z uporabo izključno pripravljenih poizvedb (angl. Prepared statements) in preverjanja uporabniških vnosov, kot je opisano v odseku 4.3, se nevarnosti injekcije kode SQL odpravijo.

4.2 Shranjevanje gesel

Geslo, ki po zavarovanem kanalu ob registraciji pride v strežniško okolje, se z uporabo vgrajene funkcije password_hash() pretvori v zgoščeno vrednost. Funkcija se izvede s privzetimi parametri; uporabi se zgoščevalni algoritem bcrypt, kot sol pa se uporabi naključno proizvedena vrednost. Namen uporabe naključne soli je ta, da so v primeru enakih gesel uporabnikov zgoščene vrednosti različne. Cena (oz. računska zahtevnost zgoščevanja) je prav tako ostala na privzeti vrednosti 10. Ta parameter napadalcu, ki bi poznal zgoščene vrednosti gesel, dodatno oteži iskanje dejanskega gesla.

Zgoščena vrednost gesla se nato zapiše v podatkovno bazo. Ob prijavi se geslo, ki ga poda uporabnik, primerja z zgoščeno vrednostjo v podatkovni bazi. Pri tem se uporabi vgrajena funkcija password_verify().

4.3 Preverjanje uporabnikovih vnosov

Z vnosi uporabnikov vedno ravnajo razredi tipa Controller. V vsaki funkciji, ki ima opravka s potencialno zlonamernim vnosom uporabnika, se ta preveri. Za preverjanje se uporabi vgrajena funkcija filter_input_array(). Pravila so podana v ločeni tabeli (v večini primerov imenovani $rules).

4.4 Prijava in odjava

Kontrola prijave in odjave je centralizirana v razredu UporabnikiController. Ko je prijava uspešna (po postopku opisanem v odseku 4.2, se ponovno nastavi identifikator seje, v sejo pa se zapiše tudi ID uporabnika in njegova vloga.

Prijava je mogoča na dveh naslovih:

- /prijava

  Če se uporabnik prijavi na tem naslovu, se v sejo vedno zapiše vloga *stranka*. Takrat se tudi prodajalci in administrator postavijo v vlogo stranke.

- /x509login

  Na tem naslovu se od uporabnika zahteva overitev z digitalnim potrdilom. Ob prijavi se v sejo shrani dejanska vloga uporabnika. Ko se nekdo overi z digitalnim potrdilom, ki vsebuje lastnikov elektronski naslov, se uporabnik prijavi le v tisti račun, ki uporablja enak elektronski naslov.

4.5 Preverjanje vlog

V razredih, izpeljanih iz razreda AbstractController, se pred izvedbami funkcij za urejanje stanja trgovine po potrebi preveri vloga uporabnika. To preverjanje je implementirano v funkciji preveriVlogo().

```php
<?php
    static $VLOGE = [
        'stranka' => 3,
        'prodajalec' => 2,
        'administrator' => 0
    ];

    /**
     * V primeru da je podana vloga nadrejena prijavljeni vlogi
     * preusmeri na /
     * @param string $vloga vloga
     * @return NULL
     */
    protected static function preveriVlogo($vloga = 'prodajalec') {
        if (isset($_SESSION['vloga']) &&
            self::$VLOGE[$_SESSION['vloga']] <= self::$VLOGE[$vloga]) {
            return;
        } else {
            ViewHelper::alert('Prepovedan dostop', '/');
        }
    }
```

Poglavje 5

Izjava o avtorstvu seminarske naloge

Spodaj podpisani *Matevž Fabjančič*, vpisna številka *63150086*, sem (so)avtor seminarske naloge z naslovom *Spletna trgovina*. S svojim podpisom zagotavljam, da sem izdelal ali bil soudeležen pri izdelavi naslednjih sklopov seminarske naloge:

- 4 Varnost sistema

Podpis: Matevž Fabjančič, l.r.

Spodaj podpisana *Andraž Povše*, vpisna številka *63150224*, sem (so)avtor seminarske naloge z naslovom *Spletna trgovina*. S svojim podpisom zagotavljam, da sem izdelal ali bil soudeležen pri izdelavi naslednjih sklopov seminarske naloge:

- Vzorčni sklop 1
- Vzorčni sklop 2

Podpis: Andraž Povše, l.r.

Poglavje 6

Dodatno vzorčno poglavje

Besedilo poglavja.

6.1 Dodatni vzorčni odsek ena

Besedilo odseka.

6.2 Dodatni vzorčni odsek dva

Besedilo odseka.

6.3 Dodatni vzorčni odsek tri

Besedilo odseka.

N	Vsebina
1	Vrstica 1
2	Vrstica 2
...	...

Tabela 6.1: Tabela vrednosti vzorcev

Besedilo odseka.
Besedilo odseka.

Slika 6.1: Slika določenega vzorca

Poglavje 7

Zaključek

Zaključek.

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 11. januar 2018). Dostopno na naslovu: http://www.ipsec-howto.org/t1.html

Dodatek A

Naslov dodatka

Po potrebi.