UNIVERZA V LJUBLJANI

FAKULTETA ZA RAČUNALNIŠTVO IN INFORMATIKO

Spletna trgovina

Poročilo seminarske naloge pri predmetu
Elektronsko poslovanje

Študenti
Matic Novak (63130164)
Jakob Košir (63130115)

Mentor
David Jelenc

Ljubljana, 12. januar 2016

Kazalo

Poglavje 1

Uvod

V seminarski nalogi sva se osredotočila predvsem na varno programiranje. Strežniški del spletne trgovine sva razvila v programskem jeziku php, pogled pa v tehnologijah html, css in javascript. Razvila sva tudi Android aplikacijo, ki preko rest api-ja dostopa do izdelkov na strežniku in jih ustrezno prikaže na mobilni napravi.

Poglavje 2

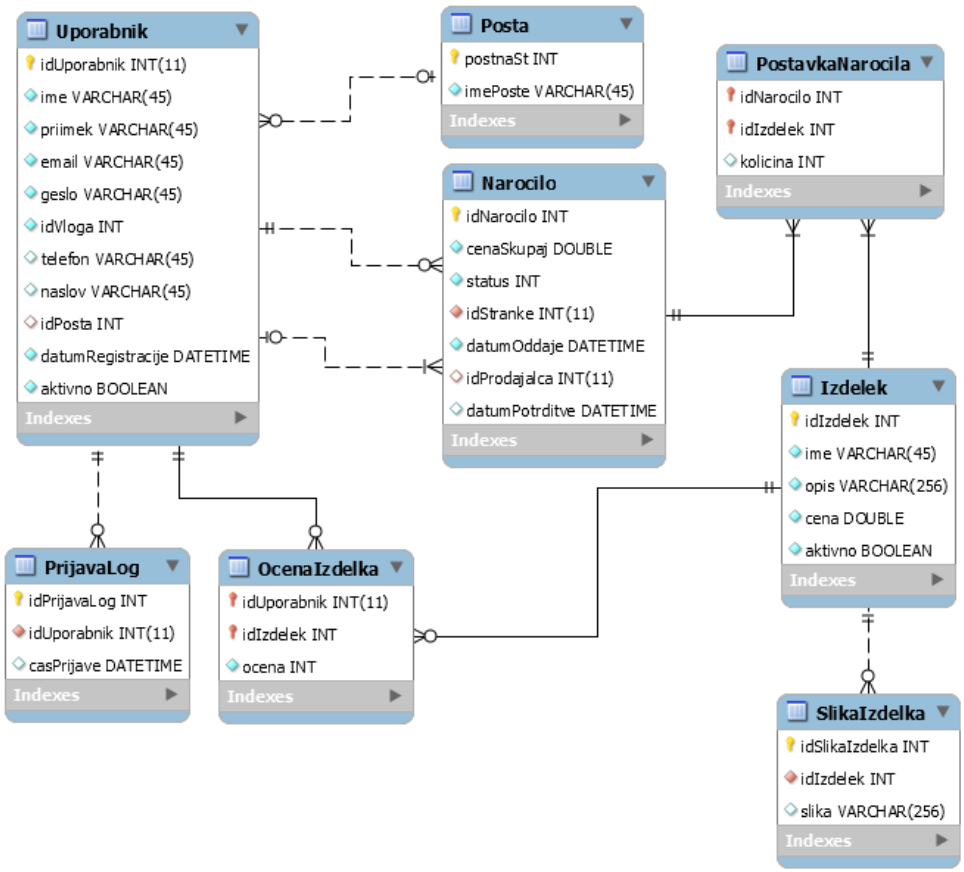
Navedba realiziranih storitev

Implementirala sva vse razširjene storitve, ki se tičejo varnosti in uporabniškega vmesnika: vodenje dnevnika uporabnikov, registracija s captcho, potrditveni e-mail ob registraciji, uporabniški vmesnik s html-jem, css-om in ajax-om, ocenjevanje artiklov, iskanje po artiklih, slike artiklov.

Poglavje 3

Podatkovni model

Podatkovni model sestavlja 8 tabel. Tabela Uporabnik hrani vse uporabnike, ki uporabljajo portal (administratorje, prodajalce in stranke). Da je model normaliziran, poštne številke in pošte hraniva v svoji tabeli. Tabela PrijavaLog služi za vodenje dnevnika uporabnikov. Tabela Izdelek hrani podatke o artiklih v trgovini. Vsak izmed njih ima lahko več slik in več ocen različnih uporabnikov, zato sta to še dve ločeni tabeli. V tabeli Narocilo hranimo vsa naročila, tabela PostavkaNarocila pa hrani vse postavke vseh narocil. Brez nje bi imeli povezavo "many to many"med naročili in izdelki, tako pa model ne bi bil normaliziran.
Vse atribute se da smiselno interpretirati iz njihovih imen. Mogoče bi omenila zgolj gesla, ki se hranijo v tabeli Uporabnik. Pred zapisom v bazo se nad nizom kliče php funkcija password_hash, ki geslo v več iteracijah izračunov spremeni v izvleček. Tako ne more priti do razkritij gesel, če nepooblaščeni osebi uspe pridi do baze.



Slika 3.1: ER diagram podatkovne baze

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.

Kot elementarni način za zagotavljanje pravilnosti podatkov izvajava validacijo vseh obrazcev z regularnimi izrazi. V primeru, da uporabnik ne zadosti zahtevam, se ga na to opozori, podatki pa se sploh ne pošljejo na strežnik. Seveda se da podatke poslati na strežnik tudi mimo obrazcev, zato prejete podatke še enkrat validirava na strani strežnika.

Vse prejete podatke najprej prečistiva z vgrajenimi php funkcijami in s tem preprečiva SQL INJECTION in XSS napade:
($filter\_input(INPUT\_POST, data, FILTER\_SANITIZE\_SPECIAL\_CHARS)$

Dodatno poskrbiva za varnost pri registraciji uporabnika, saj mora pravilno prepisati znake s CAPTCHE. Preprečiva, da bi registracijo opravljal nek zlonamerni program.

Prodajalec in Administrator sta posebni vlogi v spletni trgovini, ki imata nadzor nad zaupnimi podatki. Za prijavo v omenjenih vloga zahtevava, da se uporabnik predstavi z ustreznim (veljavnim) certifikatom X.509.

Poglavje 5

Izjava o avtorstvu seminarske naloge

Spodaj podpisani *Matic Novak*, vpisna številka *63130164*, 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:

- izdelava certifikatov in programske logike za prijavo z njimi
- preusmeritev na zavarovani kanal (HTTPS)
- prijava in odjava v/iz sistem(a)
- registracija uporabnika s CAPTCHO
- pošiljanje potrditvenega e-maila
- vodenje dnevnika uporabnikov
- urejanje uporabniških podatkov
- upravljanje s prodajalci in strankami
- izdelava rest storitve za izdelke
- izdelava Android aplikacije

Podpis: Matic Novak, l.r.

Spodaj podpisana *Jakob Košir*, vpisna številka *63130115*, 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:

- celotno upravljanje z izdeki
- ocenjevanje izdelkov
- iskanje po izdelkih
- predstavitev artiklov s slikami
- košarica z Ajax-om
- celotno upravljanje z naročili

Podpis: Jakob Košir, l.r.

Poglavje 6

Zaključek

Seminarska naloga nama je bila všeč, predvsem zato, ker je bil tokrat povdarek na varnosti aplikacije in ne samo na njenih funkcionalnostih. Zavedava se, kaj vse se lahko zgodi s podatki, če ne poskrbimo za ustrezno varnost in težo posledic. Prvič sva implementirala prijavo s spletnimi certifikati, kar štejeva kot zelo uporabno znanje.

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 12. januar 2016). Dostopno na naslovu: http://www.ipsec-howto.org/t1.html