

UNIVERZA V LJUBLJANI
FAKULTETA ZA RAČUNALNIŠTVO IN INFORMATIKO

Spletna trgovina

Poročilo seminarske naloge pri predmetu
Elektronsko poslovanje

Študenti

Vanesa Gradišar (63150099)
Nina Ramšak (63150234)
Matic Anžič (63150038)

Mentor

David Jelenc

Ljubljana, 13. januar 2019

Kazalo

1	Uvod	2
2	Navedba realiziranih storitev	3
3	Podatkovni model	4
3.1	Tabele in denormalizacija	4
4	Varnost sistema	6
4.1	Različne vrste napadov	6
4.2	Ustrezna hramba gesel	6
4.3	Prijava in certifikati	6
4.4	Preklop HTTP -> HTTPS	7
4.5	Omejitev dostopa	7
4.6	Dodatno: registracija strank z uporabo reCAPTCHE (Googlov sistem) .	7
5	Izjava o avtorstvu seminarske naloge	8

Poglavje 1

Uvod

V seminarski nalogi smo izdelali model spletne prodajalne z uporabo tehnologij Linux, Apache, SUPB MySQL, PHP, SSL, certifikatov X.509 ter mobilne platforme Android. Nalogo smo gradili po MVC arhitekturnem sistemu, uporabili pa smo tudi Bootstrap knjižnico za izgled.

Poglavje 2

Navedba realiziranih storitev

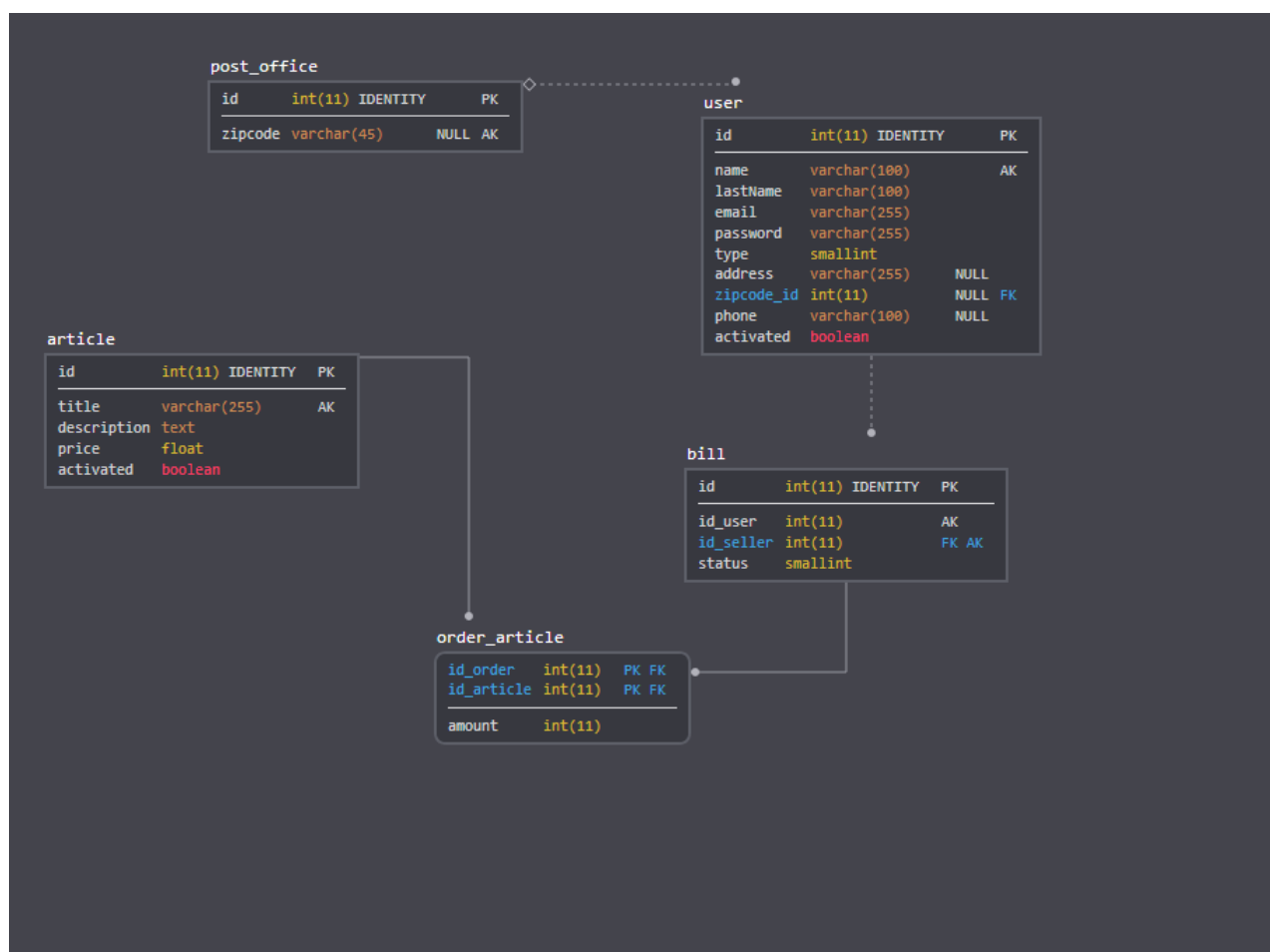
Naša aplikacija ima po večini implementirane zgolj osnovne storitve. Od razširjenih storitev smo implementirali zgolj:

- v poglavju Varnost:
 - registracija strank z uporabo filtriranja reCAPTCHA
- v poglavju uporabniški vmesnik:
 - smiselna organizacija in izvedba uporabniškega vmesnika s pomočjo tehnologij kot so sta CSS in JavaScript (dodano le nekaj stilov - gumbi)

V celoti morda ni poskrbljeno za napade tipa XSS. Uporabili smo OWASP ZAP program za simulacijo programov in odpravili večino pomankljivosti, ki jih je program javil. Vendar ni uspelo v celoti umakniti opozoril glede XSS napada, saj je javljalo pomankljivosti v dveh datotekah, katerih sploh nimamo v repozitoriju.

Poglavje 3

Podatkovni model



3.1 Tabele in denormalizacija

- user: Tabela hrani attribute o uporabniku, atribut tip pa o uporabniku pove, ali je administrator, prodajalec ali stranka. Pri stranki so naslov, poštna številka in telefon obvezni atributi, medtem ko za druge dva tipa niso.

- article: vsebuje ime, opis, ceno in podatek o aktivnosti izdelka.
- bill: hrani id stranke in id prodajalca ter status, ki je lahko oddano naročilo (0), potrjeno (1) ali stornirano (2)
- order_article: povezuje izdelek z naročilom (bill)
- post_office: hrani pošto številko s krajem

Poglavje 4

Varnost sistema

4.1 Različne vrste napadov

- XSS napade smo preprečili z delom kode `'header("X-XSS-Protection: 1; mode=block");'` v vsaki datoteki, ki je vsebovala krmilnik
- s `'header('X-Content-Type-Options: nosniff');'` smo poskrbeli za varnost pred vohljanjem za vsebino (predvsem pri MIME tipih); tudi v datotekah, ki so implementirale krmilnike
- pred napadi injekcije kode SQL pa smo se zaščitili z vnaprej pripravljenimi poizvedbami ('Prepared statements'), tako da ne more priti do tega, da se naokoli prenašajo pomembni podatki o računu/uporabniku
- s pregledi vnosov in filtracijo teh, smo poskrbeli, da so vnosi preverjeni, preden gredo v izvajanje in da tako niso zlonamerni -> to smo naredili s funkcijo `getRules()` v krmilnikih, kjer so prisotni vnosi (registracija, prijava, ...)

4.2 Ustrezna hramba gesel

Gesla v primeru registracije ali urejanja uporabnika oz. svojega uporabniškega profila primerno zaščitimo, preden jih shranimo v bazo. To pa naredimo z vgrajeno funkcijo `password_hash(password, PASSWORD_DEFAULT)` - ta vzame privzeto vrednost (drug argument), uporabi bcrypt algoritem (ki je močan enosmerni zgoševalni algoritem) in tako geslo pretvori v zgoščeno vrednost.

Uporabili smo tudi vgrajeno funkcijo `password_verify()` za preverjanje ujemanja vnešenega gesla in gesla v bazi (pri prijavi).

4.3 Prijava in certifikati

Ko je obiskano mesto `/certificate`, pa se zahteva overitev s certifikatom. Nato je možna prijava administratorju in prodajalcu, ne pa stranki. Certifikati so obravnavani v

config datoteki:

```
<LocationMatch "certificate" >  
SSLVerifyClient require  
SSLCipherSuite HIGH:!aNULL:!MD5  
SSLVerifyDepth 1  
SSLOptions +ExportCertData  
</LocationMatch>
```

4.4 Preklop HTTP -> HTTPS

Za preklop med HTTP in HTTPS kanaloma je poskrbljeno na strežniku Apache. Na https tako preklopi, ko so obiskana naslednja mesta: /login, /registration, /confirmation, /logout.

Urejeno s pogoji:

```
RewriteCond %HTTPS off  
RewriteRule "(certificate|confirmation|login|registration|logout)"  
"https://%HTTP_HOST%REQUEST_URI"
```

4.5 Omejitev dostopa

Dostop smo uporabnikom omejili glede na njihov tip, in sicer sproti v kodi pogledov (views). Pri prijavi se v sejo shranijo vsi podatki o uporabniku, ki trenutno dostopa do aplikacije. Tako smo si pomagali s podatkom \$_SESSION["type"] in glede na to uravnavali, kaj lahko katera vloga vidi. Administrator je uporabnik tipa 0, prodajalec je tipa 1, stranka pa 2.

4.6 Dodatno: registracija strank z uporabo reCAPTCHA (Googlov sistem)

Da bi registracijo preprečili 'robotom', smo poskrbeli za dodatno polje, ki ga je potrebno izpolniti. Potrebno je obkljukati določen kvadrataček in če je sistemu karkoli sumljivo, poda še uganko, kjer je potrebno obkljukati fotografije, ki zadostujejo zahtevi.

Na spletni strani smo tako prevzeli javni in privatni ključ; javni za generiranje reCAPTCHA, privatni pa za pošiljanje POST zahteve - le-ta se skupaj s privatnim ključem in povratno kodo reCAPTCHA (ta se generira, ko oseba reši uganko) pošlje na URL Googla. Nazaj prejmemo odgovor v JSON obliki, kjer je v atributu success razvidno, ali je bila uganka pravilno izpolnjena. Če uganka ni rešena, ali je napačno rešena, mora stranka izpolniti novo.

Poglavje 5

Izjava o avtorstvu seminarske naloge

Spodaj podpisana *Vanesa Gradišar*, vpisna številka 63150099, sem (so)avtorica seminarske naloge z naslovom *Spletna trgovina*. S svojim podpisom zagotavljam, da sem izdelala ali bila soudeležena pri izdelavi naslednjih sklopov seminarske naloge:

- Vzpostavitev lastne certifikatne agencije in strežniškega digitalnega potrdila
- izdelava osebnih certifikatov
- preverjanje vnosov s strani odjemalca, napadi
- normalizacija podatkovne baze
- spletni vmesnik vloge administrator
- spletni vmesnik vloge prodajalec
- spletni vmesnik vloge stranka

Podpis: Vanesa Gradišar, l.r.

Spodaj podpisana *Nina Ramšak*, vpisna številka 63150234, sem (so)avtorica seminarske naloge z naslovom *Spletna trgovina*. S svojim podpisom zagotavljam, da sem izdelala ali bila soudeležena pri izdelavi naslednjih sklopov seminarske naloge:

- Vmesnik mobilne aplikacije (platforma Android)

Podpis: Nina Ramšak, l.r.

Spodaj podpisan *Matic Anžič*, vpisna številka 63150038, 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:

- preverjanje vnosov s strani odjemalca, napadi
- normalizacija podatkovne baze
- preusmerjanje HTTPS in zahtevke za certifikat
- spletni vmesnik vloge administrator
- spletni vmesnik vloge prodajalec
- spletni vmesnik vloge stranka

Podpis: Matic Anžič, l.r.