UNIVERZA V LJUBLJANI

FAKULTETA ZA RAČUNALNIŠTVO IN INFORMATIKO

Spletna trgovina

Poročilo seminarske naloge pri predmetu
Elektronsko poslovanje

Študenti
Vanesa Gradišar (63150099)
Matic Anžič (63150038)

Mentor
David Jelenc

Ljubljana, 14. januar 2019

Kazalo

Poglavje 1

Uvod

V seminarski nalogi sva izdelala model spletne prodajalne z uporabo tehnologij Linux, Apache, SUPB MySQL, PHP, SSL, certifikatov X.509 ter mobilne platforme Android. Nalogo sva gradila po MVC arhitekturnem sistemu, uporabila pa sva tudi Bootstrap knjižnico za izgled. Mobilna aplikacija ponuja osnovni storitvi, kjer lahko brskamo po seznamu artiklov, vidimo ceno posameznega artikla in s prehodom na drug pogled preberemo njegov opis.

Poglavje 2

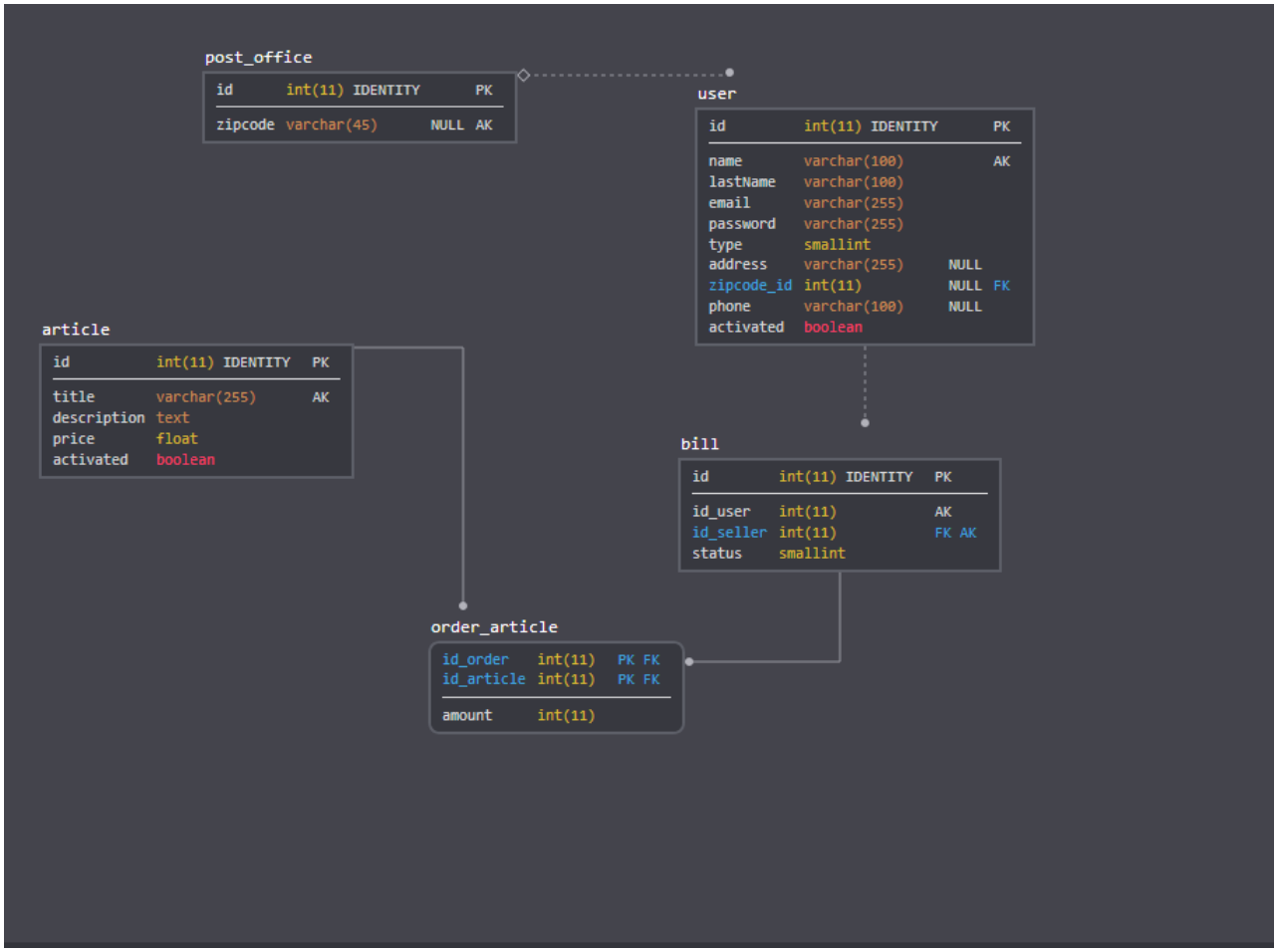
Navedba realiziranih storitev

Naša aplikacija ima po večini implementirane zgolj osnovne storitve.
Od razširjenih storitev sva implementirala 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. Uporabila sva 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 pomanjkljivosti v dveh datotekah, katerih sploh nimamo v repozitoriju.

Poglavje 3

Podatkovni model



3.1 Tabele in denormalizacija

- user: Tabela hrani atribute 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 poštno številko s krajem

Poglavje 4

Varnost sistema

4.1 Različne vrste napadov

- XSS napade sva preprečila z delom kode 'header("X-XSS-Protection: 1; mode=block");' v vsaki datoteki, ki je vsebovala krmilnik
- s 'header('X-Content-Type-Options: nosniff');' sva poskrbela za varnost pred vohljanjem za vsebino (predvsem pri MIME tipih); tudi v datotekah, ki so implementirale krmilnike
- pred napadi injekcije kode SQL pa sva aplikacijo zaščitila 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, sva poskrbela, da so vnosi preverjeni, preden gredo v izvajanje in da tako niso zlonamerni -> to sva naredila s filtri v funkciji 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.
Uporabila sva 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$_{H}OST$%$REQUEST_{U}RI$”

4.5 Omejitev dostopa

Dostop sva uporabnikom omejila 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 sva si pomagala s podatkom $_SESSION["type"] in glede na to uravnavala, kaj lahko katera vloga vidi. Administrator je uporabnik tipa 0, prodajalec je tipa 1, stranka pa 2.

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

Da bi registracijo preprečila ’robotom’, sva poskrbela za dodatno polje, ki ga je potrebno izpolniti. Potrebno je obkljukati določen kvadratek in če je sistemu karkoli sumljivo, poda še uganko, kjer je potrebno obkljukati fotografije, ki zadostujejo zahtevi.
Na spletni strani sva tako prevzela javni in privatni ključ; javni za generiranje reCAPTCHE, privatni pa za pošiljanje POST zahteve - le-ta se skupaj s privatnim ključem in povratno kodo reCAPTCHE (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 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 zahtevek za certifikat
- spletni vmesnik vloge administrator
- spletni vmesnik vloge prodajalec
- spletni vmesnik vloge stranka
- vmesnik mobilne aplikacije (platforma Android)

Podpis: Matic Anžič, l.r.