

UNIVERZA V LJUBLJANI
FAKULTETA ZA RAČUNALNIŠTVO IN INFORMATIKO

EP-store

Poročilo seminarske naloge pri predmetu
Elektronsko poslovanje

Študenti

Tilen Golob (04043349)

Žan Djordjević Štebih (04041512)

Rok Silič (04042903)

Mentor

David Jelenc

Ljubljana, 22. januar 2017

Kazalo

1	Uvod	2
2	Navedba realiziranih storitev	3
3	Podatkovni model	4
4	Varnost sistema	6
5	Izjava o avtorstvu seminarske naloge	7
6	Zaključek	10

Poglavje 1

Uvod

V seminarski nalogi pri predmetu Elektronsko poslovanje smo avtorji imeli nalogo izdelati varno spletno trgovino. Odločili smo se za izdelavo trgovine z imeno EP-Store, pri tem smo si pomagali s programskimi jeziki, ki smo jih spoznali na vajah predmeta. Tako smo za izdelavo uporabili PHP, HTML, CSS in Javo. Cilj naloge bil izdelava izdelava spletne trgovine EP-Store po navodilih in pogojih izdelave.

Nihče od avtorjev se v preteklosti ni še srečal s tako velikim projektom zato je bil naš začetni korak zgraditi dobro ogrodje spletni strani ter učinkovito podatkovno bazo v kateri se bodo hranili atributi iz spletne strani. Programsko bazo smo izdelali v MySQL in jo hranili v MySQL Workbenchu, medtem ko smo ostale stvari izdelali v virtualki, ki smo jo uporabljali na vajah znotraj okolja NetBeans.

Poglavje 2

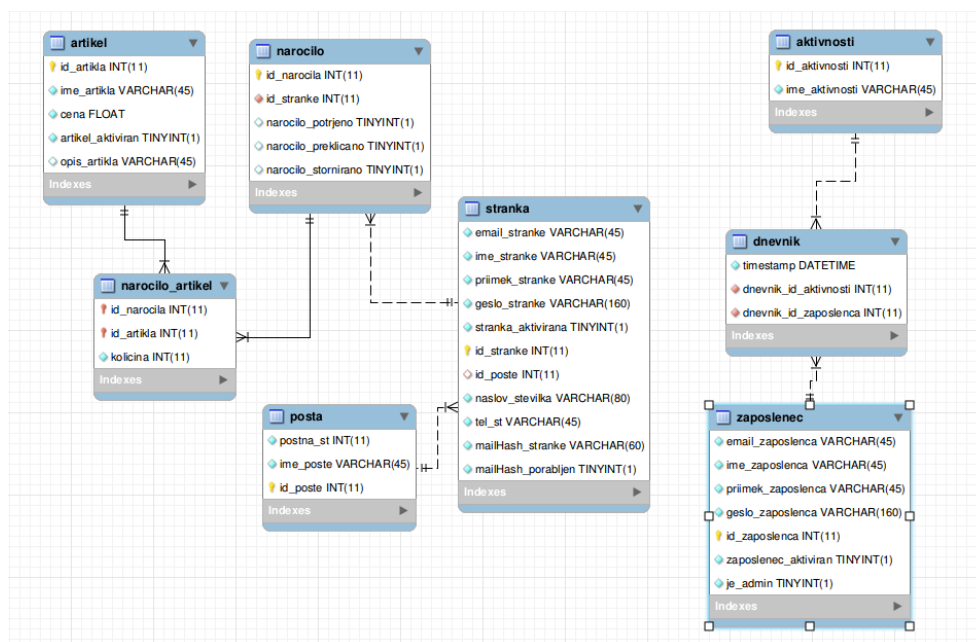
Navedba realiziranih storitev

Implementirali smo naslednje razširjene storitve:

- Varnost:
 - Vodenje dnevnika uporabnikov Administrator in prodajalec: Ob pomembnejših interakcijah s strani zaposlenih se v podatkovno bazo, v tabelo dnevnik, zapišejo vrednosti kateri uporabnik je izvedel dogodek, kaj je bil dogodek in kdaj se je zgodil dogodek.
 - Registracija strank z uporabo filtriranja CAPTCHA: Captcha preverjanje preko Google reCAPTCHA. V primeru da CAPTCHA ni izpolnjena se uporabnika ne spusti do dejanskega obrazca za oddajo.
 - Registracija strank z uporabo potrditvenega e-maila: Pošiljanje potrditvenih e-mailov poteka preko programa smtp, ki pošilja novo registriranim uporabnikom preko ustvarjenega google računa sporočila ob registraciji. Sporočilo vsebuje povezavo do strani, na kateri se postopek registracije zaključi. Ob registraciji se poleg ostalih atributov stranke v bazo zapiše še naključna vrednost in parameter, ki nam pove, če se je stranka uspešno registrirala preko e-maila. V primeru, da se še ni aktivirala je vrednost parametra nastavljena na 0, takoj ko pa aktivira svoj uporabniški račun se nastavi na 1, da se ne more ponovno aktivirati v primeru, ko je uporabniški račun deaktiviran s strani prodajalca.
- Uporabniški vmesnik:
 - Smiselna organizacija in izvedba uporabniškega vmesnika s pomočjo tehnologij CSS.

Poglavje 3

Podatkovni model



Slika 3.1: Logični model

Naš podatkovni model je sestavljen iz šestih tabel:

- Stranka,
 - Atribut mailHash je naključna vrednost, ki se zapiše in nato uporabi pri potrditvi uporabniškega računa, skozi postopek pošiljanja potrditvega maila.
- artikel,
- naročilo,
- naročilo-artikel,

- pošta,
- zaposlenec,
 - Tako za administratorje, kot za prodalce (razlikuje se le vrednost atributa je-admin).
- dnevnik,
- aktivnosti.

Vsi primarni ključi tabel (id-ji) se samodejno povečujejo.

Poglavje 4

Varnost sistema

Za vsa vnosna polja, smo uporabili HTML QuickForm2 - Pear. Za vsako vnosno polje je seveda napisano lastno preverjanje vnesenih podatkov, nakoncu pa se izvede še 'RecursiveFilter: htmlspecialchars ter trim'. Pri spremembi količine v košarici je uporabljena drugačna rešitev, vendar se dovoljuje le uporaba številčnih vrednosti. Omenjene stvari preprečujejo napade XSS.

Prav tako se pri delu z bazo, uporablja knjižnjica PDO (:string). Omenjena zadeva preprečuje napade SQL Injection.

Povsod razen na začetni strani in pri podrobnostih artiklov je prisiljena uporaba protokola HTTPS, pa še to le ob predpostavki, da do prej omenjenih dveh strani dostopa anonimni uporabnik, sicer vse poteka po HTTPS protokolu. To preprečuje prenos občutljivih podatkov po nezaščitenem kanalu.

Vsa gesla v podatkovni bazi so pretvorjena oz. shranjena v obliki hash. Geslo se takoj ob oddanem zahtevku za registracijo uporabnika, pretvori s funkcijo 'password-hash'. Ob vpisu uporabnika se s funkcijo 'password-verify' neposredno preverja, če gre pri vpisu in v bazo zapisanem geslu za par.

Poglavje 5

Izjava o avtorstvu seminarske naloge

Spodaj podpisani *Tilen Golob*, vpisna številka *04043349*, sem (so)avtor seminarske naloge z naslovom *EP-store*. S svojim podpisom zagotavljam, da sem izdelal ali bil soudeležen pri izdelavi naslednjih sklopov seminarske naloge:

- spletna aplikacija
- mobilna aplikacija

Podpis: Tilen Golob, l.r.

Spodaj podpisana *Žan Djordjević Štebih*, vpisna številka *04041512*, sem (so)avtor seminarske naloge z naslovom *EP-store*. S svojim podpisom zagotavljam, da sem izdelal ali bil soudeležen pri izdelavi naslednjih sklopov seminarske naloge:

- spletna aplikacija
- mobilna aplikacija

Podpis: Žan Djordjević Štebih, l.r.

Spodaj podpisana *Rok Silič*, vpisna številka *04042903*, sem (so)avtor seminarske naloge z naslovom *EP-store*. S svojim podpisom zagotavljam, da sem izdelal ali bil soudeležen pri izdelavi naslednjih sklopov seminarske naloge:

- spletna aplikacija
- mobilna aplikacija

Podpis: Rok Silič, l.r.

Poglavje 6

Zaključek

Skozi proces izdelave naloge smo se avtorji spoznali z izdelavo lastne certifikatne agencije in potrdil, izdelavo Android aplikacije za mobilne telefone z programskim jezikom Java ter izdelave spletne strani s programskimi jeziki PHP, HTML, CSS. Ob izdelavi smo si pomagali z orodjem Git in programom Dropbox s katerima smo skozi proces izdelave hranili trenutne rešitve naloge. Tako smo avtorji lahko istočasno delali na seminarski nalogi. Kot možne nadgradnje naloge obstoječe rešitve avtorji vidimo vključitev programskega jezika JavaScript in njegovih knjižnic s čimer bi obstoječi rešitvi dodali dinamičnost.