

Projektna dokumentacija – ak. god. 2016./2017. - V1.1

Zajednička funkcionalnost svim projektima

1. **Neregistrirani korisnik** - je korisnik koji nema korisnički račun na sustavu. Članom sustava može postati u slučaju registracije na sustav kod registracije obavezno se unose osobni podaci o korisniku, lozinka, potvrda lozinke i element da li želi koristiti prijavu u dva koraka. Korisnik se smatra registriranim tek nakon aktivacije računa putem aktivacijske poruke elektroničke pošte (link za aktivaciju vrijedi 5 sati). Svaki neregistrirani korisnik prilikom prve posjete stranici mora prihvatiti uvjete korištenja koji se odnose na bilježenje podataka u kolačiće i to se bilježi u kolačić (koji traje 3 dana) tako da nije potrebno svaki puta potvrđivati.
2. **Registrirani korisnik** - je korisnik koji ima kreiran i aktiviran korisnički račun. Prijava se sastoj od jednog ili dva koraka (ovisno o odabiru prilikom registracije ili kasnijom promjenom u profilu). Prvi korak prijave je unos korisničkog imena i lozinke. U slučaju tri neuspješna unosa (za redom), korisniku se zaključava pristup sustavu; u tom slučaju se aktiviranje korisničkog računa obavlja od strane administratora sustava. Ako je prvi korak ispravan i ako je uključena prijava u dva koraka slijedi drugi korak gdje se korisniku na mail šalje jedinstveni kod prijave koji vrijedi 5 minuta. Kada unese ispravan kod korisnik je prijavljen. U slučaju uspješne prijave na sustav, kreira se korisnička sesija koja traje do isteka vremena podešenog od strane administratora ili do odjave korisnika sa sustava. Registrirani korisnik ima sva prava koja ima neregistrirani korisnik. Kolačić koji evidentira prihvaćanje uvjeta o korištenju kolačića vrijedi mjesec dana od datuma registriranja za registriranog korisnika nakon toga ga je potrebno obnoviti.
3. **Moderator** - ima sva prava koja ima i registrirani korisnik.
4. **Kod svih uloga** – na svakom dijelu projekta gdje postoji kreiranje novih objekata (npr. kategorije, korisnici, itd.) mora se napraviti i ažuriranje i pregled.
5. **Administrator** - ima sva prava koja imaju sve prethodno definirane uloga na sustavu te uz to ima CRUD (unos, ažuriranje, pregled) kontrole (vlastito rješenje, pojedinačno za svaku tablicu) na svim podacima u sustavu. Također ima mogućnost uvid u log sustava (pogledaj točku 9) kao i pretraživanje istog prema datumu (vremenski interval), tipu log zapisa i korisniku.
6. **Straničenje** - svaki ispis podataka veći od 10 mora imati straničenje. Poželjno je da se broj zapisa po stranici može konfigurirati putem uloge administratora.
7. **Statistika** - Sve statistike moraju imati pregled za ispis, sa gumbom za print (koji otvara print dijalog u browseru) (te gumbom za generiranje PDF dokumenta – za dodatne bodove). Sve statistike koje se prikazuju moraju imati mogućnost sortiranja po prikazanim kolonama (minimalno dvije kolone). **Obavezno prikazivanje statističkih podataka u obliku barem jedne vrste grafa** (prema odabiru, zabranjeno

korištenje gotovih rješenja (PHP i JavaScript), obavezno korištenje JavaScripta i Canvasa, a moguće korištenje AJAX-a).

8. **Relativne putanje** - rješenje projekta mora koristiti relativne putanje.
9. **Dnevnik rada** - svaki zahtjev treba biti zapisan u dnevnik rada tzv. log aplikacije (tko, kada, što radio i sl.). Obavezno zapisivanje osnovnih informacija o radu sustava u log (tip prijava/odjava (korisnik, vrijeme), tip rad s bazom (korisnik, upit, vrijeme), tip ostale radnje (korisnik, vrijeme, radnja)). Administrator može pogledati u traženom razdoblju razne izvještaje (kronologija rada svih ili izabranog pojedinca, frekvencija rada osoba i sl.)
10. **Pretraživanje i sortiranje** - svaki tabelarni prikaz mora imati omogućeno pretraživanje i sortiranje po minimalno dva stupca.

Opće upute

11. **Autentikacija** - treba biti provedena vlastitom metodom s bazom podataka. Potrebna je validacija podataka na korisničkoj i poslužiteljskoj strani. Osigurati sigurnost i zaštititi od automata kod registracije korisnika. Poželjno je da se pamte podaci zadnje uspješne prijave (korisničko ime). Detaljnije upute o prijavi opisane su u točki 2.
12. **Lozinke** – potrebno je sve lozinke u bazu podataka spremati u dva stupca. Prvi u čitljivom obliku i drugi u kriptiranom obliku korištenjem SHA1 ili SHA256 algoritma za izračunavanja sažetka (eng. hash) i primjenom soli (eng. salt). Čitljiv oblik se koristi samo iz praktičnih razloga ako zaboravite definiranu lozinku.
13. **HTTPS** – prijava mora ići preko sigurne linije tj. preko HTTPS protokola. Ostatak projekta ne mora biti preko HTTPS-a.
14. **Zaštita XSS i SQL ubacivanje (eng. SQL inject)** – za dodatne bodove napravite osnovu zaštitu u cijelom projektu za XSS koristeći filter_input kod unosa i htmlspecialchars kod ispisa i zaštitu za SQL ubacivanja korištenjem pripremljenih upita (eng. prepare statements).
15. **Korisničko sučelje** - treba biti realizirano uz pomoć AJAX-a koji će preuzimati podatke s poslužitelja (preporučujemo XML ili JSON, varijanta s HTML-om donosi manje bodova). jQuery može se koristiti kod određenih dijelova projekta, veće korištenje donosi više bodova. Za preglede kataloga podataka i ostale preglede potrebno je primjenjivati stranicenje (pogledaj točku 6). Poželjna je personalizacija i pomoć/olakšanje rada korisnika (npr. više CSS-ova).
16. **Podaci u bazi podataka** - glavni katalozi podataka (npr. korisnici, obiteljska stabla, nekretnine, vozila, dijelovi, oprema i sl.) trebaju sadržavati više od 20 pojedinačnih elemenata. Ostale tablice podataka trebaju imati više 30 pojedinačnih elemenata.
17. **Virtualno vrijeme** - rad aplikacije temelji se na virtualnom vremenu koje polazi od stvarnog vremena na poslužitelju koje se korigira za određeni pomak vremena. Jedinica vremena kod pomaka je 1 sat. Administrator aplikacije jedini može obaviti

usklađivanje vremena, npr. treba pomaknuti za 7 dana naprijed pa je pomak 148 sati. Kod pomaka u nazad za 7 dana (prošlost) radi se o -148 sati. Nakon što administrator obavi usklađivanje vremena, sve aktivnosti vežu se uz novo virtualno vrijeme. Preporučuju se posebna funkcija kojom će se dobivati virtualno vrijeme i koja će se koristiti kod svih vremenskih uspoređivanja. Redoslijed koraka je sljedeći:

- podešavanje pomaka vremena obavlja se upisom adrese http://barka.foi.hr/WebDiP/pomak_vremena/vrijeme.html.
 - preuzimanje pomaka vremena obavlja se čitanjem podataka s adrese http://barka.foi.hr/WebDiP/pomak_vremena/pomak.php?format=xml ili http://barka.foi.hr/WebDiP/pomak_vremena/pomak.php?format=json. To je xml ili json datoteka jednostavne strukture. Preuzimanje podataka za pomak vremena treba obaviti prema XML ili JSON formatu, a zatim aplikacija treba spremiti pomak vremena, u bazu podataka ili datoteku. To se obavlja samo po zahtjevu administratora.
 - postavljanje virtualnog vremena na bazi stvarnog vremena na poslužitelju i pomaka vremena. To se obavlja samo po zahtjevu administratora. Od sada aplikacija radi s virtualnim vremenom.
18. **Instalacija** - rješenje treba biti instalirano na računalu **barka.foi.hr**. Pristup ostalim studentima treba biti zabranjen!
19. **Podaci** - se pohranjuju u MySQL bazu podataka pod nazivom WebDiP2016xnn (nn je broj studenta 01 <= nn <= 300). Za studente će biti kreirane potrebne baze podataka i dodijeljene potrebne privilegije za rad s bazom podataka. Studenti će dobiti potrebne informacije za bazu podataka.
20. **Direktorij** - na kojem je smješteno projektno rješenje treba biti WebDiP2016xnn (nn je broj studenta 01 <= nn <= 300) u direktoriju /var/www/WebDiP/2016_projekti. Studenti će dobiti poruku s potrebnim informacijama za smještaj projektnog rješenja. Na direktoriju projektnog rješenja smiju se nalaziti samo skripte i ostali podaci vezani uz projektno rješenje.
21. **Direktorij privatno** - treba biti zaštićen .htaccess datotekom pri čemu u njoj treba postojati korisnik s istim korisničkim imenom i lozinkom kao i pristup do baze podataka (pogledaj točku 16). Skripta privatno/korisnici.php treba ispisati sve korisnike, njihove lozinke u čitljivom obliku i vrstu. Pristup do skripte nije ograničen na korisnike aplikacije.
22. **Dokumentacija** - Naziv datoteke treba biti dokumentacija.html i njoj se pristupa iz početne stranice projektnog rješenja. Dokumentacija projektnog rješenja sastoji se od:
- a. opis projektnog zadatka
 - b. opis projektnog rješenja
 - c. bitne odrednice projektnog rješenja (ERA model)
 - d. popis i **opis** skripata, mapa mjesta, navigacijski dijagram

- e. popis i **opis** korištenih tehnologija i alata
 - f. popis i **opis** vanjskih (tuđih) modula/biblioteka i njihovo korištenje u skriptama i sl.
23. **O autoru** – Naziv datoteke treba biti o_autoru.html i njoj se pristupa sa početne stranice projektnog rješenja. Stranica mora imati sliku (kao u indeksu), ime, prezime, broj indeksa i mail (sa linkom koji otvara slanje maila). Ostatak stranice sadrži podatke prema želji.

Pristup obrani projekta

- prijaviti se na jedan od objavljenih termina za obranu projekta
- instalirati rješenje projekta na računalo **barka.foi.hr** prema prethodnim uputama
- donijeti sa sobom prijenosno računalo na kojem će se izvršavati projekt. Računalo treba imati instalirano minimalno 2 preglednika (Chrome, IE, Firefox, Opera,...) jer će se paralelno izvršavati kroz 2 preglednika. Računalo treba imati instaliranu programsku podršku za pristup Eduroam bežičnoj mreži i **osigurati da radi za vaše korisničke podatke.**
- potrebno je **popuniti cijeli** obrazac za projekt, ispisati ga, potpisati i donijeti na obranu projektnog rješenja. Student koji ne popuni obrazac do početka obrane izgubiti će dio ostvarenih bodova.
- potrebno je **popuniti cijeli (samoprocjena)** obrazac za ocjenjivanje projekta, ispisati ga, potpisati i donijeti na obranu projektnog rješenja. Student koji ne popuni obrazac do početka obrane izgubiti će dio ostvarenih bodova.
- cjelovito projektno rješenje i dokumentacija (struktura direktorija) uključujući eksport baze podataka u datoteku pod nazivom WebDiP2016xnn.sql (nn je broj studenta $01 \leq nn \leq 300$) trebaju biti spremljeni u zip datoteku i donijeti na samu obranu. Studenti će predati unaprijed pripremljen zip dokument na **Moodle** nakon uspješne obrane projektnog rješenja.
- pripremiti scenarij svoje prezentacije rješenja tijekom koje će se proći svi bitni elementi. Nastavnik će postavljati pitanja za određene elemente kada je to potrebno.
- doći minimalno 10 min prije termina pred kabinet nastavnika i pripremiti računalo za rad
- nakon obrane dok su još u kabinetu ponovo zabraniti pristup projektu ostalim studentima te ga NE SMIJU više otključavati!