

	Modul Správa používateľov	Verzia :	1.3
		Dátum vydania :	03.05.2016
	Správa používateľov	Zodpovedný :	Tomáš Chovaňák

1.1 SPRÁVA POUŽÍVATEĽOV

Tento modul zabezpečuje čo najjednoduchšiu a bezpečnú autorizáciu a autentifikáciu používateľov na portáli Open Science. Tiež zabezpečuje vytváranie profilov používateľov a správu týchto profilov.

1.1.1 Registrácia používateľa a prihlásenie

Riešiteľ: Helmut Posch, Martin Žalondek

Analýza

Úlohou bolo implementovať registráciu a následné prihlásenie používateľov. Registráciou používateľa sa myslí vytvorenie účtu a umožnenie sa prihlásiť (autentifikovať totožnosť) pomocou používateľského mena / emailu a hesla. Prihlásením používateľovi umožníme vstup k verejne nedostupnej časti portálu, kde bude môcť pracovať s datasetmi na rozšírenej úrovni.

Potrebná je aj integrácia so sociálnymi sieťami. Rozhodli sme sa integrovať sociálne siete Facebook, Google (nie len sociálnu sieť Google+ ale akýkoľvek účet od Google), Twitter a LinkedIn. Pre tieto sociálne siete sme sa rozhodli na základe ich popularity alebo ako v prípade LinkedIn-u podobnosti záujmovej oblasti používateľov.

Riešenie

Riešenie všeobecného problému autentifikácie používateľa sme rozdelili na niekoľko častí.

1. Registrácia používateľa cez náš portál

Prvým krokom k vytvoreniu účtu na našom portály je registrácia. Od používateľa požadujeme nasledujúce povinné údaje:

- *používateľské meno* - každý používateľ musí mať unikátne bez ohľadu na veľkosť písmen, min. dĺžka 2 znaky
- *e-mailová adresa* - min. 5 znakov, musí byť unikátna
- *heslo* - min. 4 znaky

a nasledujúce dobrovoľné údaje:

- *meno* - krstné meno dlhé aspoň 2 znaky
- *priezvisko* - dlhé aspoň 2 znaky.

Rozhodli sme sa implementovať dvojnásobné zadávanie hesla pre overenie, aby sa predišlo chybe pri zlom zadaní hesla.

Po odoslaní formuláru overíme popísané obmedzenia a na zadanú e-mailovú adresu odošleme e-mail s adresou, pomocou ktorej si používateľ účet aktivuje. Aktivačný kľúč vygenerujeme podľa používateľského mena a náhodne pridávaného reťazca. Tento kľúč uložíme k používateľovi aby bol kedykoľvek prístupný. Ak by

	Modul Správa používateľov	Verzia :	1.3
		Dátum vydania :	03.05.2016
	Správa používateľov	Zodpovedný :	Tomáš Chovaňák

sa snažil používateľ prihlásiť so správnymi prihlasovacími údajmi na neaktívovaný účet, portál ho upozorní a ponúkne mu preposlanie e-mailu s aktivačnou adresou. Takýto postup aplikujeme aj pri situácii keď by sa používateľ chcel opätovne registrovať s rovnakou e-mailovou adresou.

V prípade, že formulár nespĺňa požiadavky je zobrazený s predvyplnenými údajmi a zrozumiteľnou chybovou hláškou opäť.

Po aktivácii používateľského účtu sa zobrazí používateľovi prihlasovací formulár s informáciou, že sa môže prihlásiť.

2. Prihlásenie a odhlásenie používateľa cez náš portál

Prihlásenie používateľa prebieha zadaním používateľského mena alebo e-mailovej adresy s heslom. Pokiaľ sú vo formulári správne vyplnené údaje, overí sa ich existencia v databáze. Najprv sa vyhľadáva používateľ podľa dvojice používateľské meno, heslo a ak hľadanie je neúspešné, tak podľa dvojice e-mailová adresa, heslo.

Ak používateľ zadá správne meno alebo e-mailovú adresu a nesprávne heslo, zaznamenáme zlý pokus k prihláseniu pomocou počítača. Dovolíme používateľovi 4-krát zadať nesprávne heslo a pri 4. pokuse mu resetujeme heslo a pošleme mu ho na e-mail. Z tohoto pramení bezpečnostné riziko zámerného blokovania účtov a dokonca zahlietia e-mailovej adresy používateľa. Takýto útok môže vykonať robot, ktorý bude mať informáciu o tom, aké používateľské mená na portály existujú tak, že sa bude donekonečna skúšať prihlásiť so zlým heslom. Preto v budúcnosti plánujeme doimplementovať maximálny počet resetovaní hesla alebo zaviesť kontrolu proti robotom pomocou vykonania úlohy, ktorú vie pochopiť iba človek (napr. CAPTCHA).

Pri zhode dvojice používateľské meno / e-mailová adresa a heslo používateľa prihlásime a resetujeme mu počítačlo zlých prihlásení.

Používateľovi sa môže stať, že zabudne heslo na svoj účet. Preto sme implementovali funkcionality, keď používateľ môže zadať e-mailovú adresu, s ktorou je registrovaný na našom portáli a pošleme mu resetované heslo, s ktorým sa môže prihlásiť. Hrozí tu podobné bezpečnostné riziko ako v prípade veľkého množstva neúspešných pokusov o prihlásenie.

3. Registrácia a prihlásenie používateľa cez sociálnu sieť

Náš portál umožňuje prihlásenie používateľov prostredníctvom účtov na sociálnych sieťach Facebook, Twitter, LinkedIn, Google. Využili sme na to verejne dostupnú knižnicu *python-social-auth*. Táto knižnica podporuje autentifikáciu pomocou protokolou *OAuth2*, preto pre takto registrovaného používateľa nepotrebujeme ukladať jeho heslo do našej databázy.

Po kliknutí na tlačidlo prihlásenia je používateľ vyzvaný k povoleniu prístupu našej aplikácie k jeho profilu na danej sieti. Jedná sa o prístup k jeho prihlasovaciemu menu a emailovej adresy, ktoré sú potrebné na identifikáciu používateľa v našej databáze. Sociálna sieť Twitter však neposkytuje emailovú adresu. Pre náš systém to neznamená veľký problém, pretože používateľa vieme jednoznačne identifikovať pomocou jeho používateľského mena, ktoré vieme získať. Ak by pri prvom prihlásení cez sociálnu sieť nastal prípad, že používateľské meno zo sociálnej siete sa zhodne s nejakým v našej databáze, upravíme ho tak, aby bolo unikátne.

	Modul Správa používateľov	Verzia :	1.3
		Dátum vydania :	03.05.2016
	Správa používateľov	Zodpovedný :	Tomáš Chovaňák

4. Popis implementácie

K implementácií registrácie a prihlásenia je použitý modul frameworku Django na správu používateľov. Poskytuje nám triedu pre správu používateľa (trieda *User*), metódu pre overenie správnosti používateľského mena a hesla, prihlásenie a odhlásenie používateľa. Ďalšie potrebné atribúty a metódy pre našu správu používateľov sme implementovali v triede *django.contrib.auth.AbstractUser*, od tejto triedy je odvodený django *User* a teda dedí všetky tieto metódy a atribúty.

Implementovať odoslanie emailu z lokálneho serveru sa nepodarilo. Táto a s ňou spojená funkcionálna je možná iba z produkčného servera. Na lokálnom serveri nám aplikácia vracia chybu "Error 13 Permission denied", ktorú sa nám aktuálne nepodarilo vyriešiť. V budúcnosti je možné pokúsiť sa nakonfigurovať vlastný SMTP server na lokálnom serveri.

1.1.2 Verejný profil, súkromný profil a jeho správa

Riešiteľ : Rania Daabousová, Milan Gajdoš

Analýza

Úlohou bolo implementovať profil používateľa a správu profilu používateľa.

Riešenie

Celkový koncept profilu používateľa sa logicky rozdeľuje na 3 časti:

1. Používateľský profil - súkromný


Súkromný používateľský profil slúži na zobrazenie informácií o používateľovi dostupných ostatným používateľom. Obsahuje dve logicky oddelené časti: osobné údaje používateľa a používateľove datasety (Datasety, ktoré používateľ nahral na náš portál). Časť s osobnými údajmi používateľa obsahuje údaje :

- *používateľské meno*
- *meno*
- *priezvisko*
- *e-mailová adresa*
- *profilový obrázok*

Pokiaľ ide o používateľa registrovaného cez náš portál tak sa v profile vyplnia údaje zadané používateľom pri registrácii. Používateľ prihlásený cez sociálnu sieť má vyplnené údaje získane zo sociálnej siete.

Časť používateľove datasety obsahuje zoznam datasetov nahraných používateľom. O každom datasete sú zobrazené informácie:

- *meno*
- *veľkosť*
- *dátum nahrania datasetu*

	Modul Správa používateľov	Verzia :	1.3
		Dátum vydania :	03.05.2016
	Správa používateľov	Zodpovedný :	Tomáš Chovaňák

Používateľovi je v tejto časti súkromného profilu umožnené priamo datasety vymazať.

2. Používateľský profil - verejný

Verejný používateľský profil slúži na zobrazenie základných informácií o používateľovi. Obsahuje tri logicky oddelené časti: osobné údaje používateľa, používateľove datasety (Datasety, ktoré používateľ nahral na náš portál) a kontakt.

Časť s osobnými údajmi používateľa obsahuje údaje zadané používateľom pri registrácii. Avšak používateľov email je na verejnom profile zverejnený iba v prípade súhlasu s jeho zverejnením, ktorý používateľ dáva pri registrácii.

Časť používateľove datasety obsahuje zoznam datasetov nahraných používateľom.

V časti kontakt je možné používateľa kontaktovať, napísať mu správu, ktorá sa pošle na jeho email. Používateľov prihlásených do portálu cez sociálne siete nie je možné kontaktovať.

3. Správa používateľského profilu

Správa používateľského profilu je možná zo súkromného profilu, po kliknutí na odkaz ktorý presmeruje užívateľa na obrazovku s editáciou profilu. Správa profilu je obmedzená len pre registrovaných užívateľov.

Používateľovi je umožnené upravovať len vybrané údaje z časti profilu: osobné údaje používateľa. Medzi vybrané údaje patria:

- *meno*
- *priezvisko*
- *heslo*
- *Profilový obrázok*