WordPress

Da bi se davateljima usluga olakšala implementacija AAI@EduHr autentikacije u sustavu WordPress, razvijen je poseban dodatak (engl. plugin) pod nazivom *WP AAI@EduHr Auth*.

Dodatak *WP AAI@EduHr Auth* u sustavu WordPress omogućuje jednostavnu zamjenu standardnog WordPress autentikacijskog mehanizma s AAI@EduHr autentikacijom. Dodatak se može konfigurirati tako da dopusti prijavu samo određenim korisnicima ili može dopustiti prijavu svim korisnicima koji se autenticiraju preko AAI@EduHr sustava. Također, moguće je ograničiti prijave po određenim ustanovama. Dodatak se može koristiti u testnom ili produkcijskom AAI@EduHr okruženju.

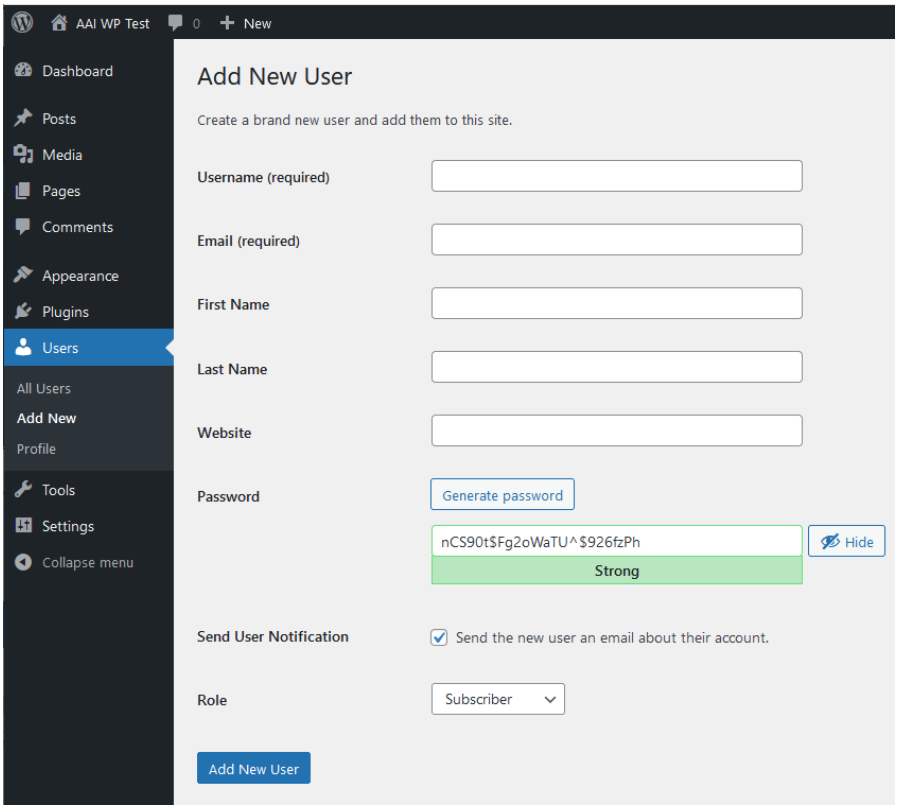
Dodatak je napisan poštujući WordPress standarde za pisanje dodataka, pa se u bilo kojem trenutku može omogućiti i onemogućiti. Iako se sustav WordPress redovno nadograđuje, ne očekuju se velike promjene u načinu rada s korisničkim računima, pa bi se dodatak trebao moći koristiti i na budućim verzijama sustava WordPress.

> Dodatak *WP AAI@EduHr Auth* je '*open source*' i dostupan je kao git repozitorij na poveznici: https://github.com/cicnavi/wp-aaieduhr-auth. Za sve izazove i probleme s dodatkom potrebno je otvoriti 'issue' na spomenutorm repozitoriju ili se obratiti originalnom autoru.

WordPress i korisnički računi

WordPress ima ugrađenu podršku za upravljanje korisničkim računima. Da bismo mogli uspješno zamijeniti ugrađeno upravljanje korisnicima s AAI@EduHr autentikacijom, ukratko ćemo se upoznati s postojećim mogućnostima povezanim s korisnicima i autentikacijom koje nudi WordPress.

Prilikom instalacije sustava WordPress definira se glavni administratorski korisnički račun. Nakon što se prijavimo pomoću glavnog administratorskog računa, možemo ručno dodavati nove korisnike kojima se želi omogućiti prijava na stranice. Forma za dodavanje novih korisnika izgleda ovako:

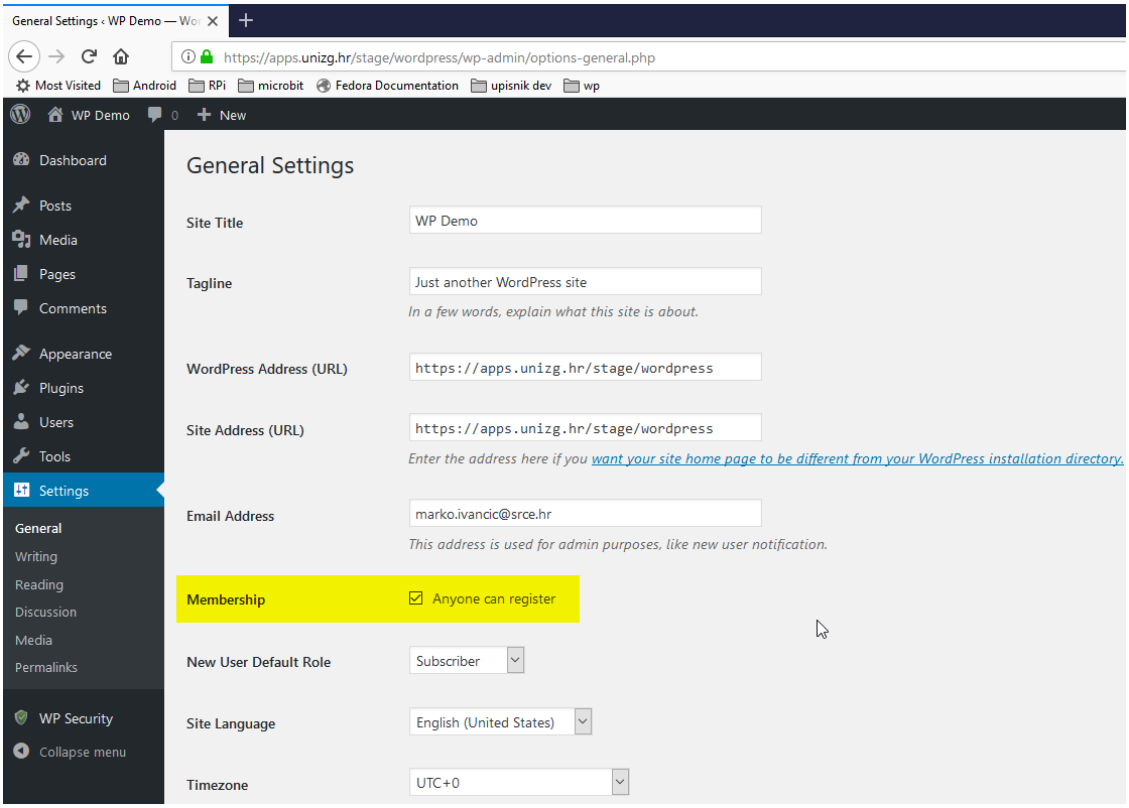


Na formi je moguće postaviti lozinku za korisnika. Nakon što administrator doda korisnika, korisniku može sam javiti početnu lozinku ili može odabrati opciju slanja e-maila u kojem će biti obavijest o otvorenom računu. Korisnik će nakon toga moći postaviti svoju novu lozinku za buduće korištenje. Kod stvaranja korisnika administrator može postaviti i ulogu za korisnika. Dostupne uloge su:

- *Super Admin* – osoba s potpunim pristupom administraciji na mrežnoj razini (kad stranica ima više podstranica)
- *Administrator* – osoba s pristupom administraciji određene stranice
- Editor – osoba koja može objaviti svoje članke ili članke drugih osoba
- *Author* – osoba koja može objaviti svoje članke

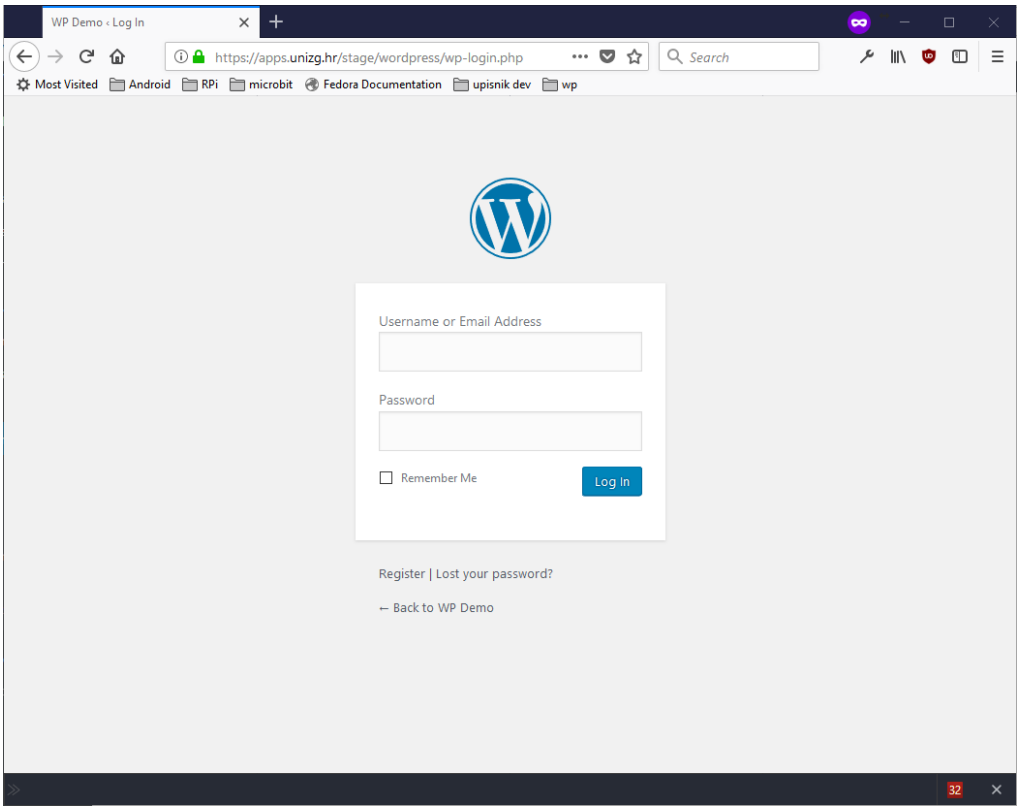
- *Contributor* – osoba koja može pisati članke, ali ih ne može objaviti
- *Subscriber* – osoba koja samo može uređivati svoj profil.

Uz ručno dodavanje, moguće je dopustiti i da korisnici sami naprave korisnički račun (da se registriraju na stranicu). Opcija za omogućavanje registracije nalazi se u *Settings > General.*

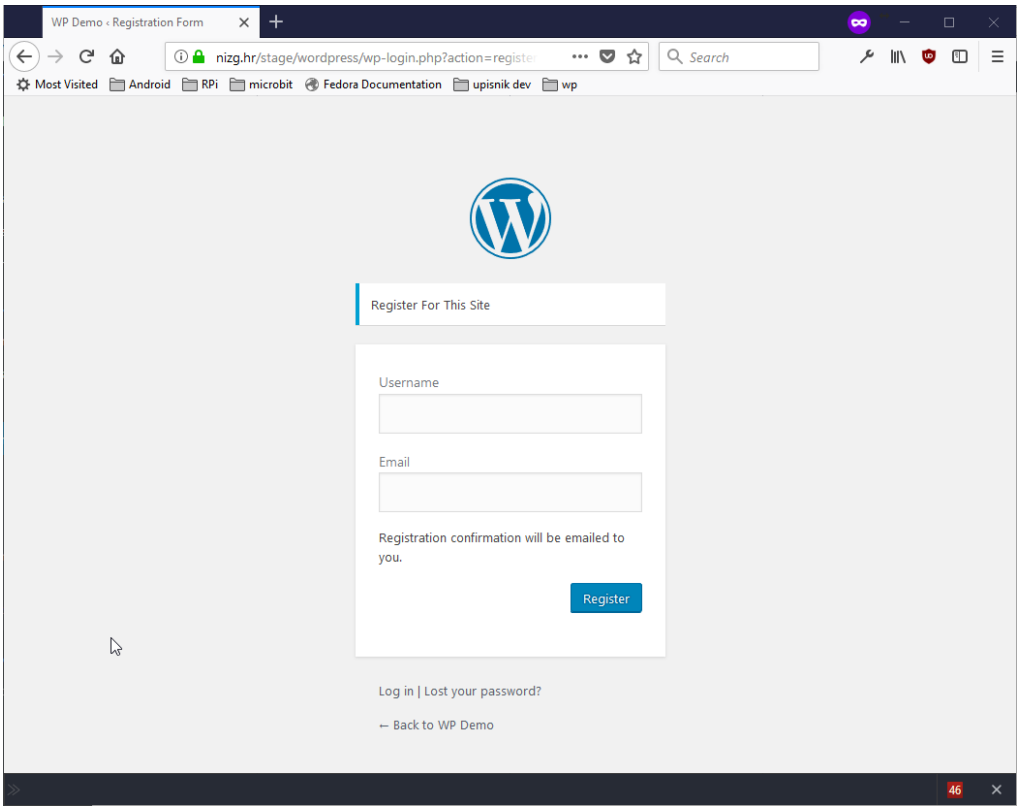


Kada se korisnici sami registriraju, prema početnim postavkama dobit će ulogu *Subscriber*, što je najslabija uloga za prijavljene korisnike u sustavu WordPress.

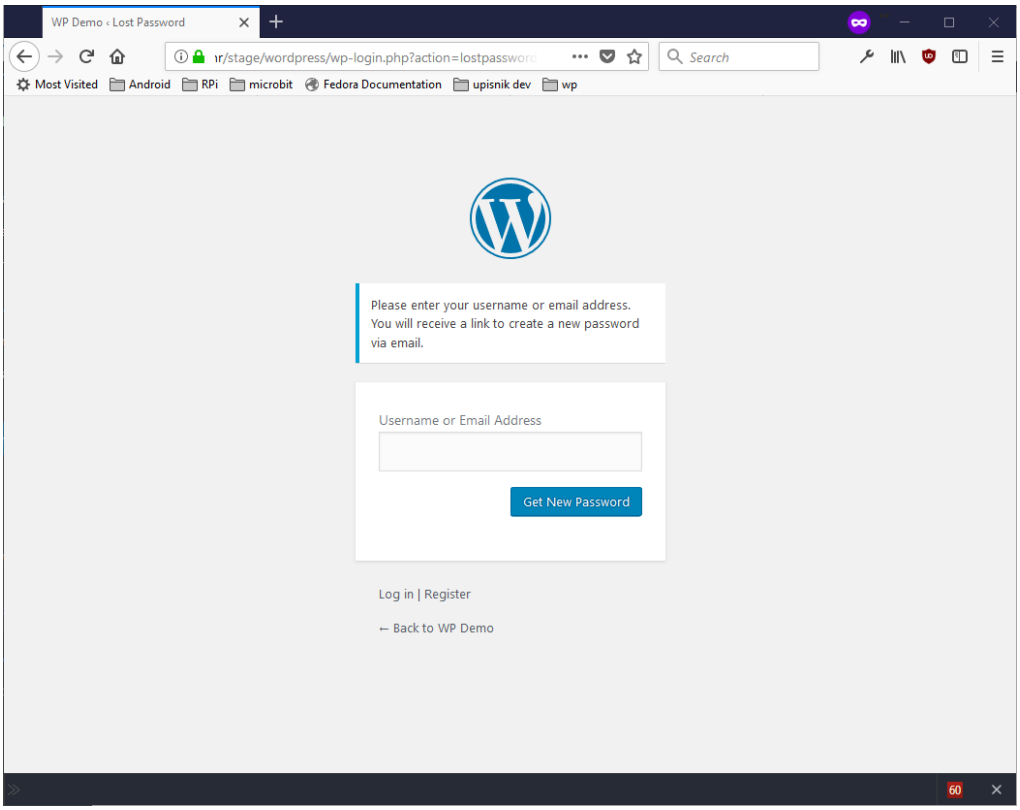
Korisnici koji imaju korisnički račun mogu se prijaviti preko poveznice *{wordpress-instalacija}/wp-login.php*, a forma izgleda ovako:



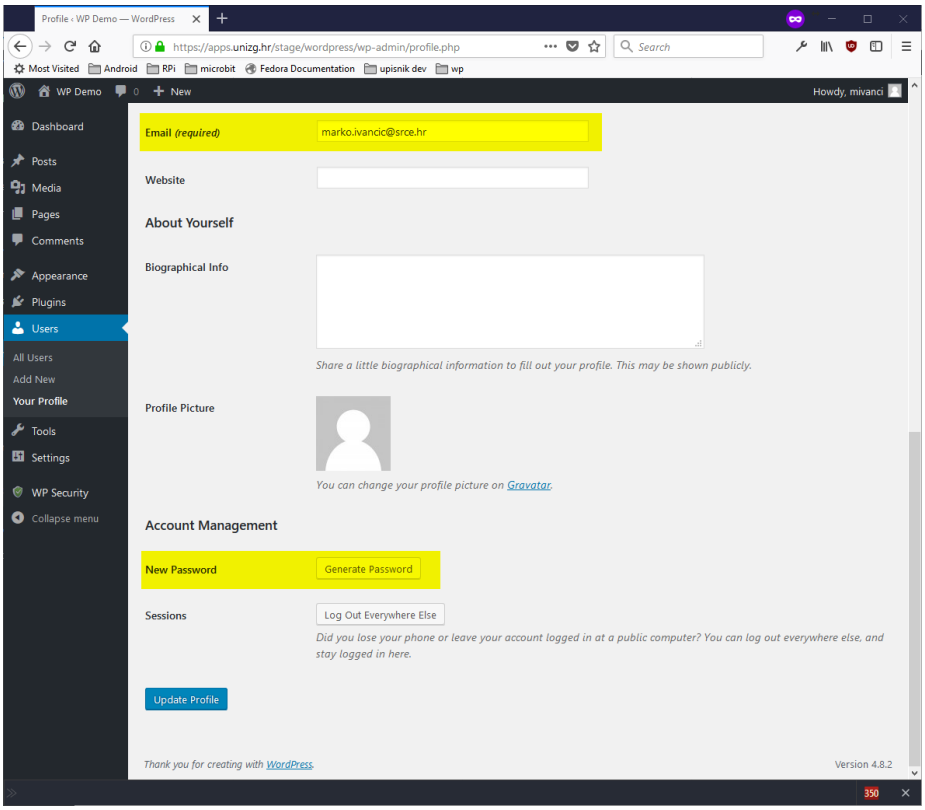
Ako je omogućena registracija, korisnici se mogu registrirati na stranice preko poveznice *{wordpress-instalacija}/wp-login.php?action=register*, a forma izgleda ovako:



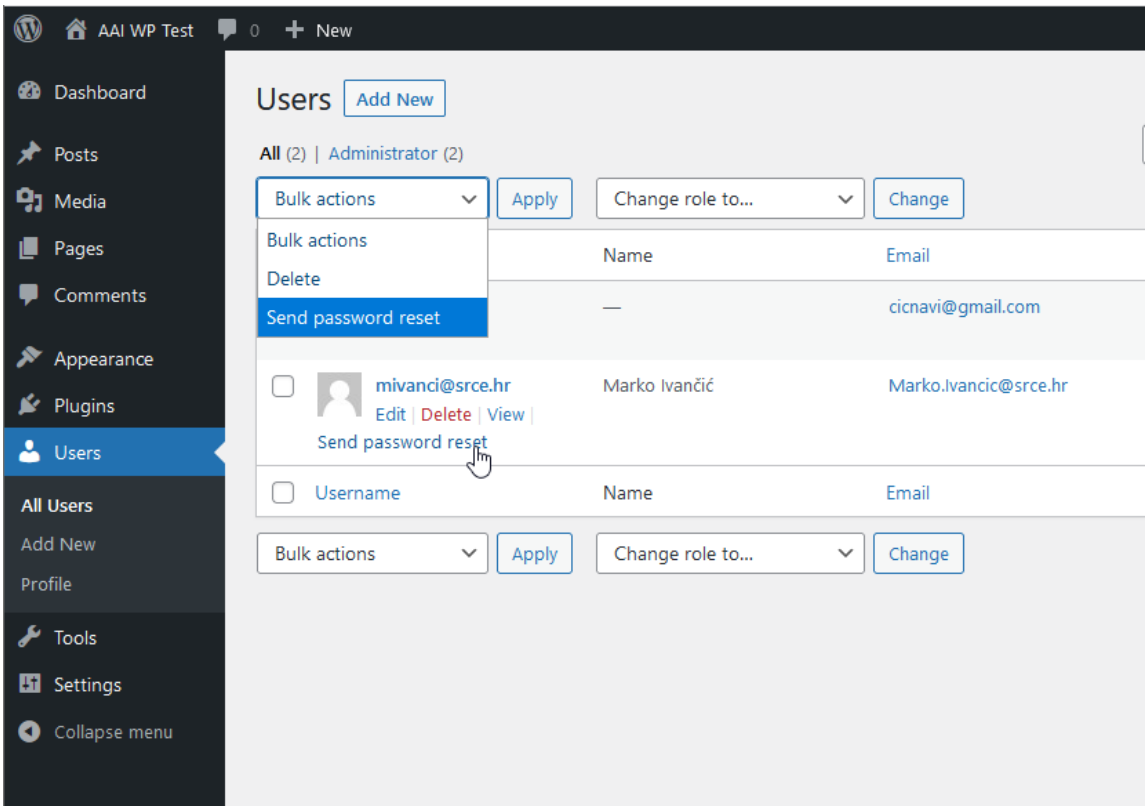
Korisnici imaju mogućnost resetiranja lozinke u slučaju da su je zaboravili. Korisnici to mogu učiniti preko poveznice *{wordpress-instalacija}/wp-login.php?action=lostpassword*, a forma izgleda ovako:



Kada se korisnici prijave na stranicu, u svom korisničkom profilu mogu mijenjati e-mail adresu i mogu generirati novu lozinku (uz ostale opcije):



Prilikom ažuriranja korisnika administratori mogu zatražiti resetiranje lozinke preko opcije "Send password reset".



Generalno gledajući, osnovne podatke koje sustav WordPress zahtijeva za korisničke račune su:

- korisničko ime (engl. *username)*
- e-mail
- lozinka
- uloga (ako nije dana, početna uloga bit će *Subscriber*).

Što se tiče baze podataka, svi podaci o korisnicima spremaju se u tablice *'users'* i *'usermeta'*.

Dakle, ako u WordPress želimo uvesti autentikaciju pomoću AAI@EduHr sustava, moramo onemogućiti skoro sve ugrađene funkcionalnosti u vezi s kreiranjem korisničkih računa i prijave korisnika na stranice. Budući da sustav WordPress ovisi o lokalnim korisničkim računima, morat ćemo ih i dalje koristiti iako imamo aktivnu AAI@EduHr autentikaciju.

Na sreću, sustav WordPress je relativno lako proširiv preko dodataka, pa smo za tu potrebu napravili dodatak *WP AAI@EduHr Auth* koji može na standardni način omogućiti autentikaciju preko AAI@EduHr sustava te sam stvoriti i koristiti lokalne WordPress korisničke račune.

Preduvjeti za rad dodatka *WP AAI@EduHr Auth*

Da bi se mogao koristiti dodatak *WP AAI@EduHr Auth*, na poslužitelju na kojem će se koristiti WordPress s AAI@EduHr autentikacijom potrebno je instalirati programski alat *simpleSAMLphp*. Također, potrebno je imati registriran resurs u sustavu AAI@EduHr. Upute kako instalirati simpleSAMLphp i kako registrirati resurs dostupne su na stranici: http://www.aaiedu.hr/za-davatelje-usluga/za-web-aplikacije/kako-implementirati-autentikaciju-putem-sustava-aaieduhr-u-php .

Prilikom registracije resursa, prilikom odabira korisničkih atributa koji će se isporučivati usluzi, preporučamo odabrati sljedeće atribute:

- hrEduPersonUniqueID (korisnička oznaka - obavezno)
- mail (e-mail - opcionalno, ali poželjno)
- givenName (ime - opcionalno)
- sn (prezime - opcionalno)

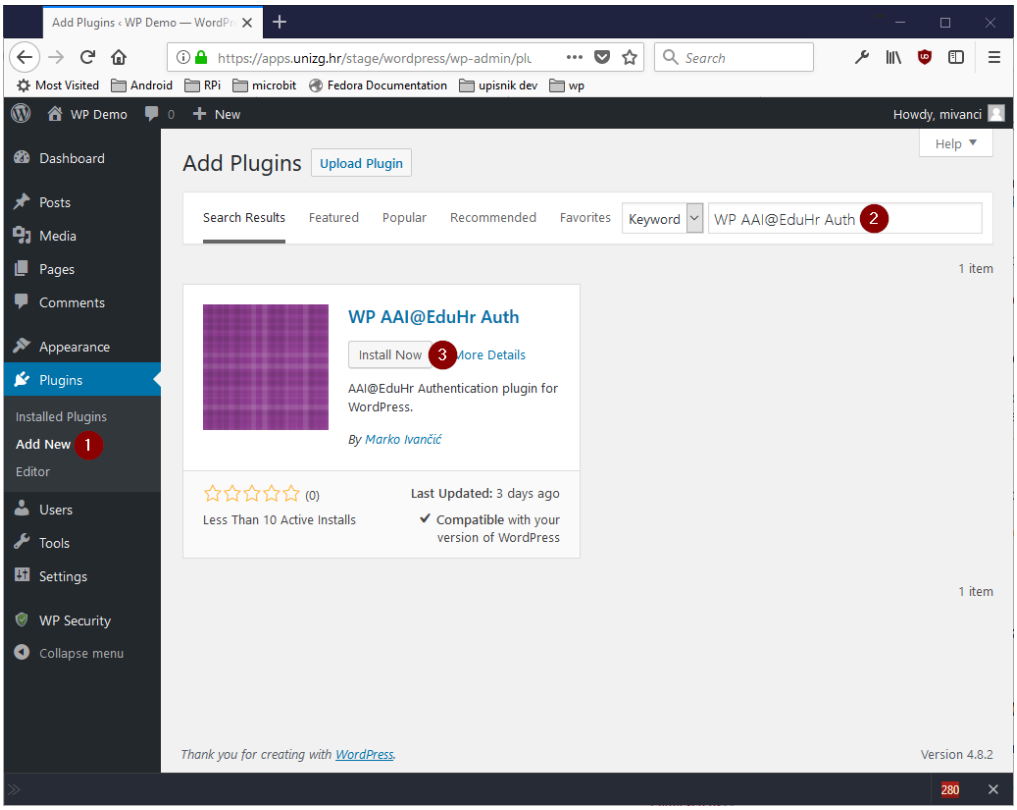
Naime, da bi se mogao napraviti novi korisnički račun u sustavu WordPress, obavezno se moraju postaviti korisnička oznaka i e-mail. Opcionalno, mogu se postaviti ime i prezime.

Da bi dodatak WP AAI@EduHr Auth mogao raditi, prilikom autentikacije obavezno mora dobiti korisnički atribut 'hrEduPersonUniqueID', kojeg će iskoristiti za provjeru postojanja ili kreiranja korisničkog računa u sustavu WordPress. Ako prilikom autentikacije dodatak ne dobije atribut 'mail', atribut 'hrEduPersonUniqueID' će se iskoristiti za definiranje korisničke oznake i e-maila.

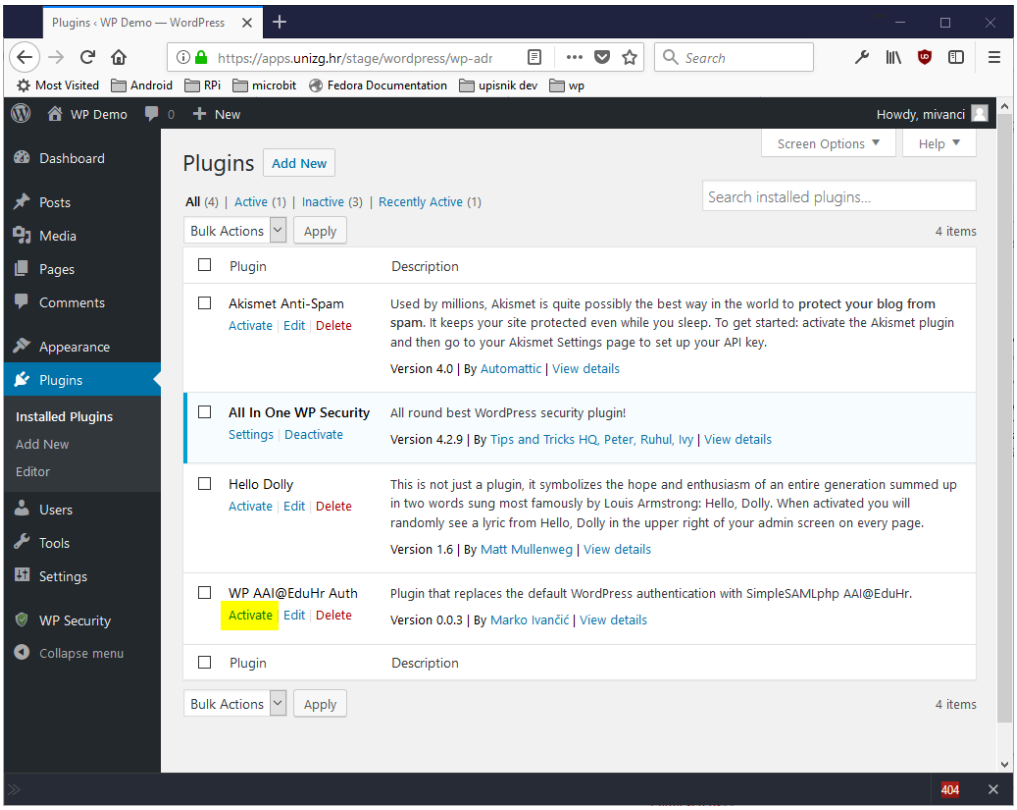
Instalacija dodatka *WP AAI@EduHR Auth*

Dodatak *WP AAI@EduHr Auth* dostupan je kao WordPress dodatak te ga se može preuzeti na standardni način iz službenog WordPress repozitorija dodataka.

Dakle, u kontrolnoj ploči možemo kliknuti na *Plugins* > *Add New*. U tražilicu možemo unijeti naziv dodatka *'WP AAI@EduHr Auth'*. Nakon toga možemo kliknuti na gumbić *'Install Now'*.

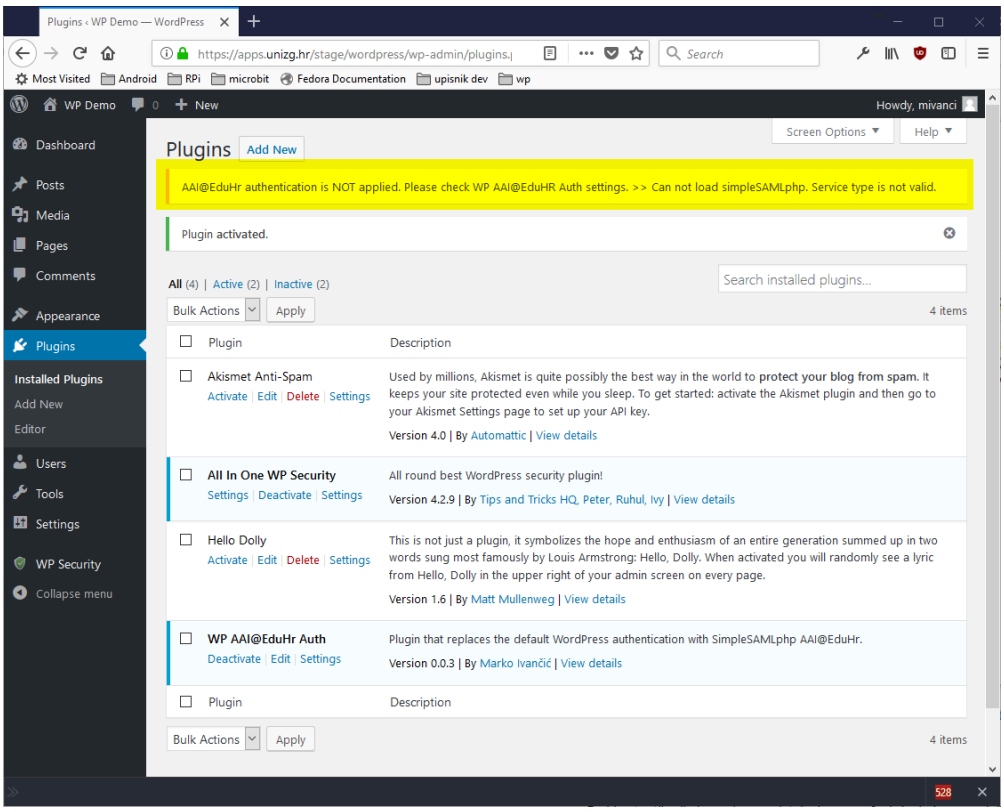


Nakon instalacije možemo otići na *Plugins* > *Installed Plugins*. Na listi instaliranih dodataka potrebno je pronaći dodatak *WP AAI@EduHr Auth* i aktivirati ga klikom na gumbić *Activate*.

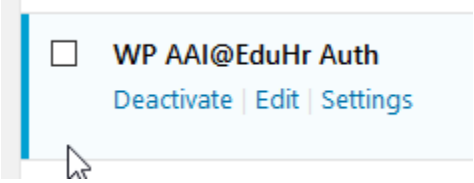


Postavke dodatka *WP AAI@EduHr Auth*

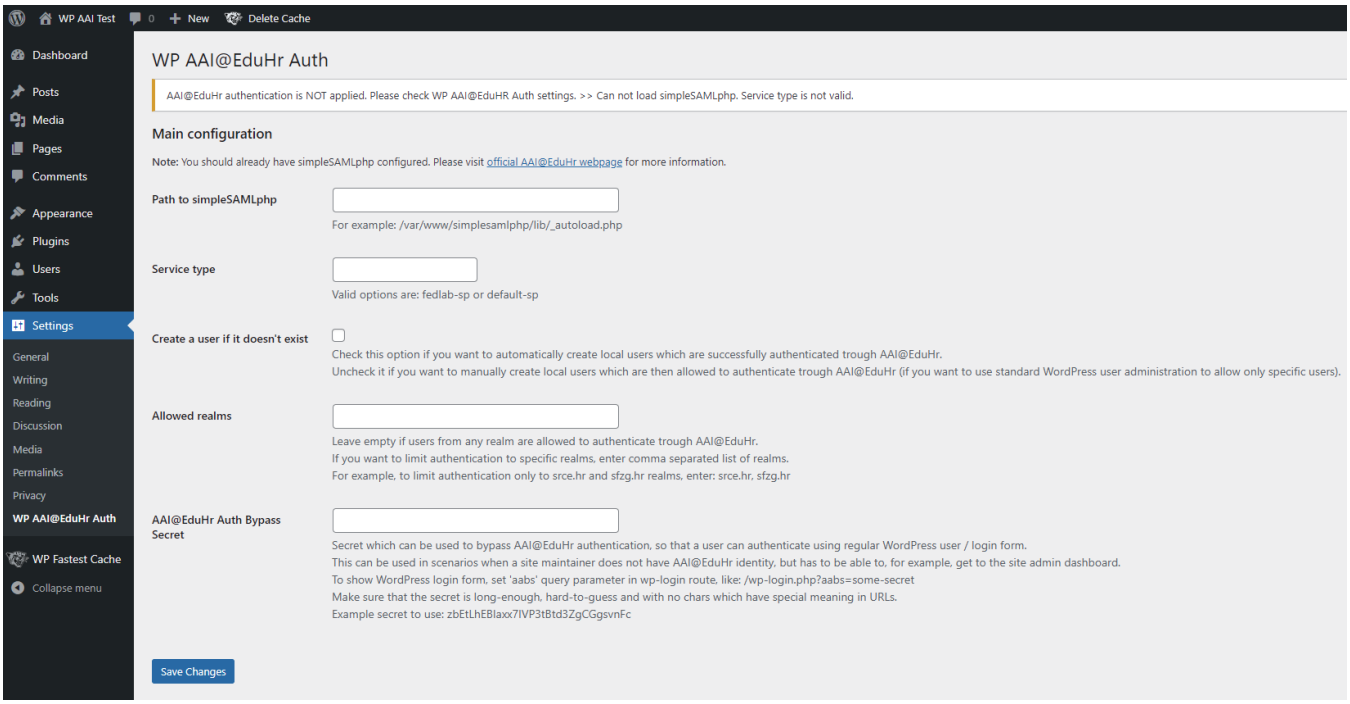
Nakon aktivacije potrebno je unijeti postavke dodatka. Sve dok se postavke ne unesu, neće biti moguće koristiti AAI@EduHr autentikaciju. Na vrhu kontrolne ploče vidljiv je status o tome je li AAI@EduHr autentikacija aktivna ili ne. Budući da trenutačno nismo unijeli postavke, vidimo da AAI@EduHr autentikacija još uvijek nije aktivirana:



Da bismo došli do stranice s postavkama, možemo kliknuti na gumbić *'Settings'* koji se nalazi ispod naziva samog dodatka:



Također možemo otići na *'Settings'* > *'WP AAI@EduHr Auth'*:



Prva postavka koju moramo unijeti je putanja do alata simpleSAMLphp (engl. *Path to simpleSAMLphp*). U našem slučaju putanja za učitavanje alata simpleSAMLphp je /var/www/projects/aai/ssp-aai/simplesamlphp-aai-1.18.8-aai/lib/_autoload.php.

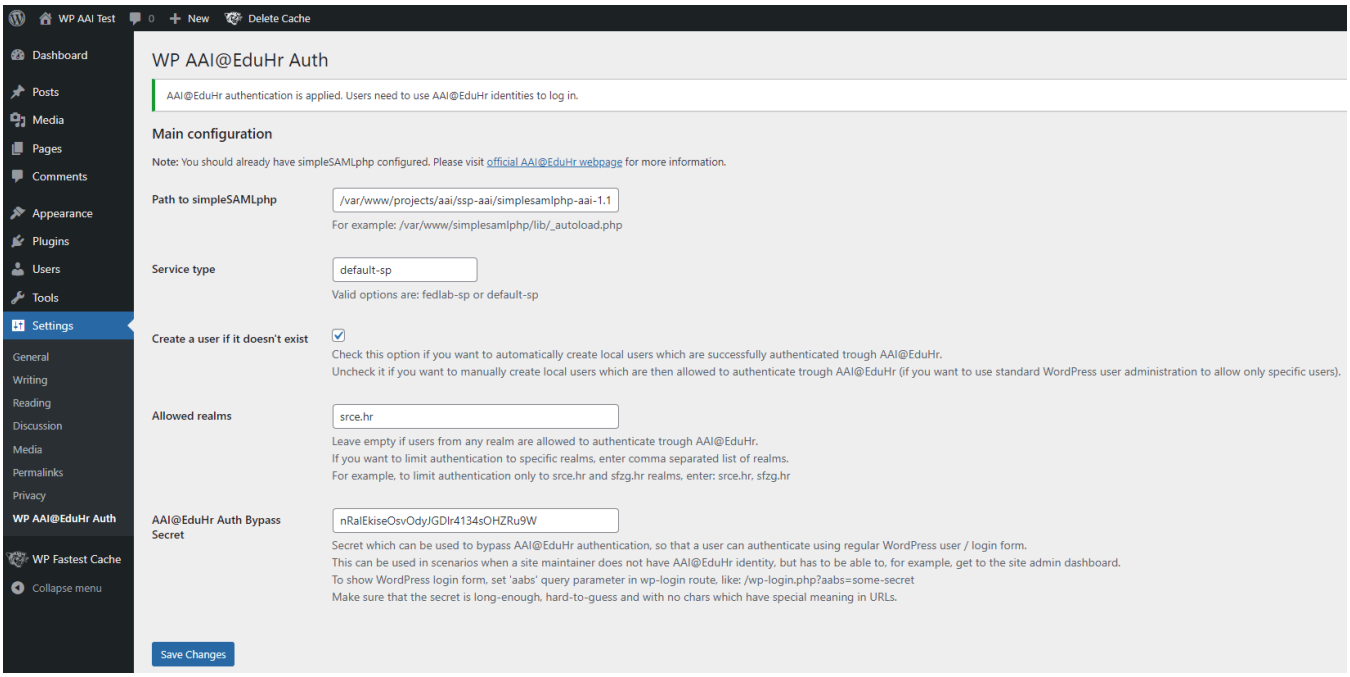
Druga postavka koju moramo unijeti je tip servisa (engl. *Service type*). Moguće opcije su *'fedlab-sp'* ili *'default-sp'*. Opcija *'fedlab-sp'* označava testni autentikacijski servis, a *'default-sp'* označava produkcijski autentikacijski servis. U našem slučaju unijet ćemo *'default-sp'*.

Dalje, možemo odabrati da li želimo automatski stvoriti lokalne korisničke račune ili ćemo sami definirati koji korisnički računi će se moći prijaviti na stranice. Ako odaberemo automatsko stvaranje korisničkih računa, dodatak *WP AAI@EduHr Auth* će sam stvoriti lokalni korisnički račun za sve korisnike koji se uspješno autenticiraju preko AAI@EduHr sustava, a do te prijave nisu imali lokalni korisnički račun. Ako ne odaberemo opciju za automatsko stvaranje korisničkih računa, morat ćemo ručno dodati svakog korisnika preko forme koja se nalazi na *'Users'* > *'Add New'*. U tom slučaju za svakog korisnika kojeg ručno dodajemo, kao korisničko ime moramo navesti korisničku oznaku iz AAI@EduHr sustava.

Dalje, preko postavke *'Allowed realms'* možemo ograničiti prijave na korisnike samo s određenih ustanova. Ako tu postavku ostavimo praznom, korisnici s bilo koje ustanove moći će se prijaviti na stranice. Ako želimo postaviti ograničenje na određene ustanove, možemo unijeti listu LDAP domena ustanova odvojenih zarezom (popis matičnih ustanova s naznakom LDAP domene dostupan je na stranici: http://www.aaiedu.hr/statistika-i-stanje-sustava/maticne-ustanove/popis). Na primjer, ako želimo ograničiti prijave samo na korisnike s ustanova Sveučilišni računski centar i Sveučilište u Zagrebu, unijeli bismo: *sr ce.hr, unizg.hr*.

Dalje, za omogućavanje prijave za korisnike koji ne posjeduju AAI@EduHr elektronički identitet, moguće je popuniti opciju '*AAI@EduHr Auth Bypass Secret* '. Ako se u to polje unese tajni string, on će se moći iskoristiti za pristup standardnom WordPress sučelju za prijavu lokalnih korisnika. Ova opcija se može iskoristiti u scenariju kada osobe održavatelji WordPress sjedišta nisu sa ustanove koja je vlasnik web sjedišta. Tajni string se može iskoristiti definiranjem 'aabs' parametra prilikom pristupa wp-login.php formi, npr.: *{wordpress-instalacija}/wp-login.php?aabs=some-secret*

Nakon spremanja postavki pojavit će se obavijest da je AAI@EduHr autentikacija sada aktivna (ako su postavke ispravne).



Onemogućene WordPress funkcionalnosti

Nakon aktiviranja dodatka *WP AAI@EduHr Auth*, određene WordPress funkcionalnosti povezane s korisnicima bit će onemogućene:

- Više neće biti moguće koristiti standardni link za registraciju *korisnika {wordpress-instalacija}/wp-login.php?action=register*. Ako netko pokuša otvoriti tu stranicu, dodatak *WP AAI@EduHr Auth* javit će poruku da je registracija na stranicu onemogućena.
- Akcija vraćanja izgubljene lozinke koja se mogla obaviti na stranici *{wordpress-instalacija}/wp-login.php?action=lostpassword* također je onemogućena.
- Nadalje, kod dodavanja novog korisnika kroz standardno WordPress sučelje više nije moguće definirati korisničku lozinku niti je kod uređivanja postojećeg korisničkog profila moguće mijenjati korisničke lozinke. Dodatak *WP AAI@EduHr Auth* generirat će slučajne lozinke (iako se te lozinke neće koristiti).

Deaktivacija dodatka *WP AAI@EduHr Auth*

Iako je redovna praksa da aplikacije koje jednom počnu koristiti AAI@EduHr autentikaciju nastave raditi na taj način do kraja svog životnog vijeka, dodatak *WP AAI@EduHr Auth* može se deaktivirati u bilo kojem trenutku. U slučaju da to odlučite, treba imati na umu nekoliko stvari.

- Svi lokalni korisnički računi koji su stvoreni dok se koristio dodatak *WP AAI@EduHr Auth* ostat će evidentirani u sustavu WordPress.
- Sve prethodno spomenute onemogućene akcije ponovno će postati aktivne, što znači da će korisnici ponovno moći koristiti standardne akcije za vraćanje i resetiranje lozinke te za prijavu i registraciju na stranicu.
- U slučaju deaktiviranja dodatka treba razmotriti da li treba određene AAI@EduHr korisnike obrisati iz sustava WordPress kako si ne bi mogli resetirati lozinke i na taj si način ponovno omogućiti pristup stranici.

Poveznice

Dodatak *WP AAI@EduHr Auth* napisan je pod licencijom GPL-3.0+, a trenutačno je dostupan na engleskom i hrvatskom jeziku.

Službena stranica dodatka je: https://wordpress.org/plugins/wp-aaieduhr-auth/.

Git repozitorij dostupan je na adresi: https://github.com/cicnavi/wp-aaieduhr-auth.

SVN repozitorij dostupan je na adresi: https://plugins.svn.wordpress.org/wp-aaieduhr-auth/.

Pozivamo vas da isprobate dodatak i da nam javite svoja iskustva. Također, programere pozivamo da pogledaju izvorni kod i da sudjeluju u daljnjem razvoju dodatka. Možete koristiti mogućnosti koje nude spomenuti repozitoriji ili se možete javiti direktno autoru na e-mail. Svi prijedlozi su dobrodošli.