SecretWiki

Wersja: testowa

Informacje

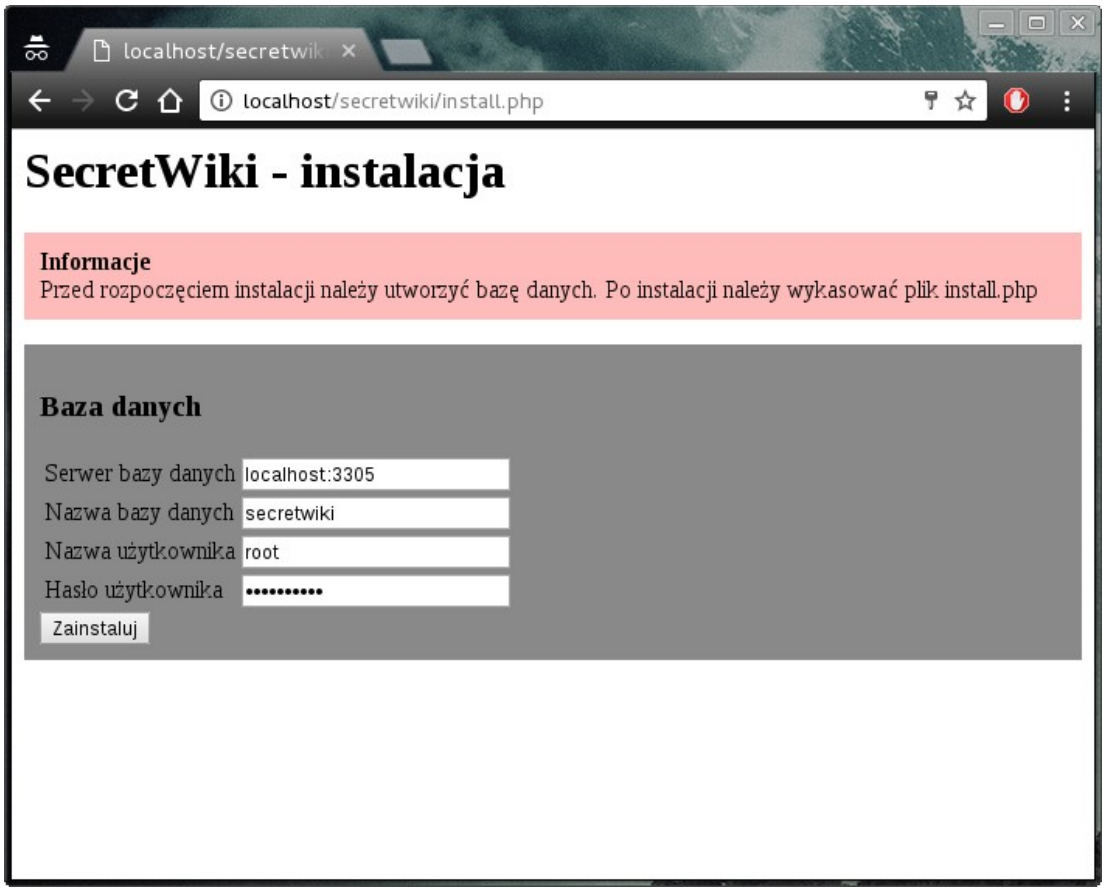
SecretWiki jest aplikacją napisaną w języku PHP w oparciu o framework Smarty i współpracującą z bazą danych MySQL.
Zadaniem aplikacji jest przechowywanie danych w zaszyfrowanej formie i organizowanie ich w formie stron które mogą być linkowane wzajemnie. Możliwe jest również dodanie multimediów (grafik, aplikacji itp.) oraz ich osadzenie na poszczególnych stronach.

Pobranie z repozytorium

Aplikację można pobrać ze strony http://noweenergie.org/index.php?0/Article/38

Instalacja

Pobrane z repozytorium archiwum ZIP należy umieścić w docelowym folderze na serwerze i rozpakować archiwum.
Należy utworzyć w bazę danych oraz użytkownika (np. za pośrednictwem phpMyAdmin).
Następnie otworzyć za pomocą przeglądarki internetowej plik install.php znajdujący się na serwerze.

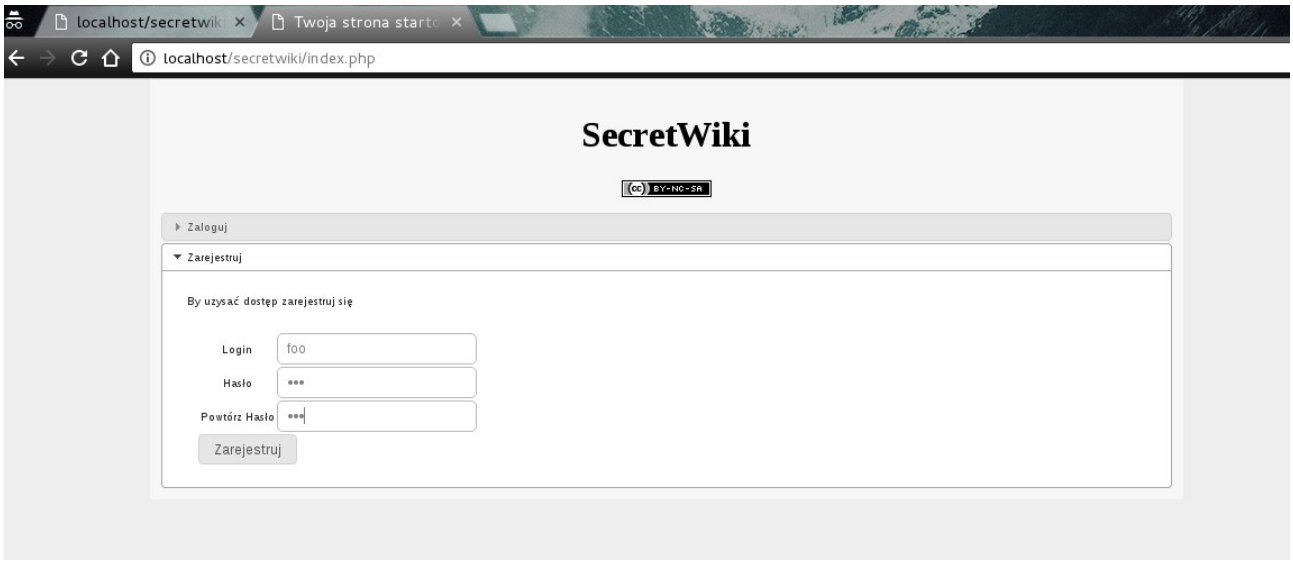


Okno instalacyjne

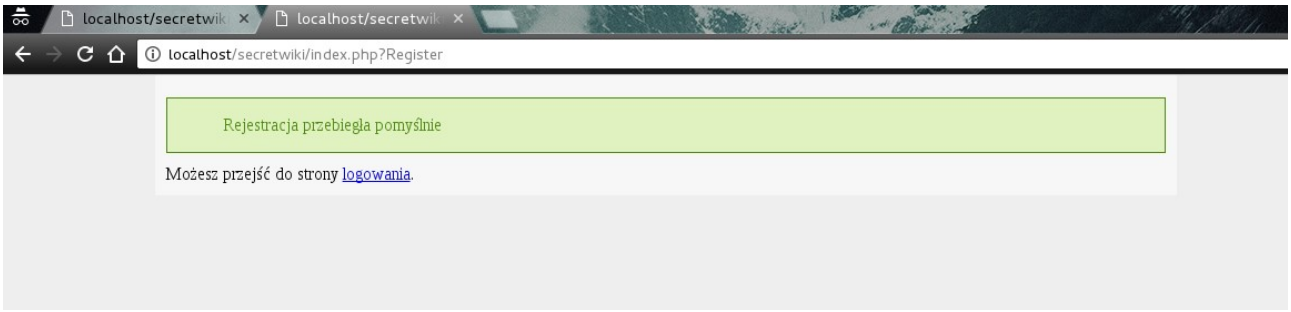
Należy wypełnić formularz i kliknąć przycisk „Zainstaluj”. Efektem działania instalatora będzie:
- wygenerowanie pliku konfiguracyjnego (config/config.php),
- instalacja w bazie danych tabel zdefiniowanych w pliku config/database.sql.

Rejestracja użytkownika

Po zainstalowaniu aplikacji jest ona gotowa do rejestracji użytkowników. W trakcie tego procesu następuje weryfikacja, czy login nie jest używany przez innego użytkownika oraz tworzona jest główna strona startowa.



Rejestracja użytkownika.



Podsumowanie poprawnie przeprowadzonej rejestracji.

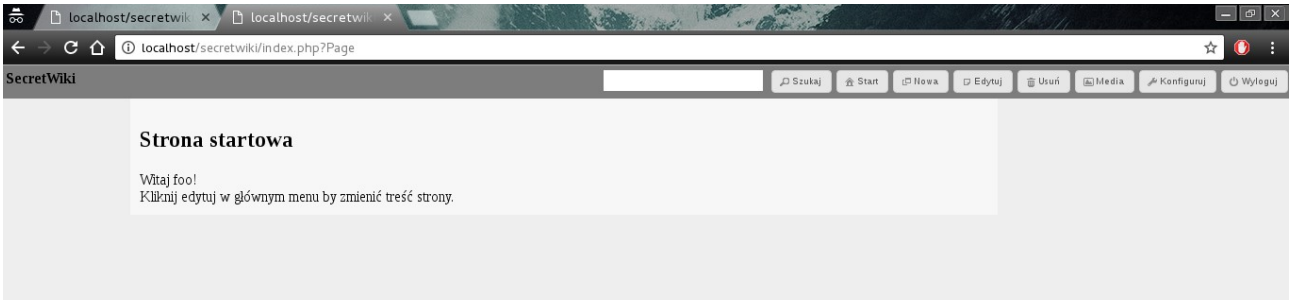
Logowanie

Zarejestrowany użytkownik loguje się na zakładce „logowanie”.

Logowanie użytkownika.

Strona startowa

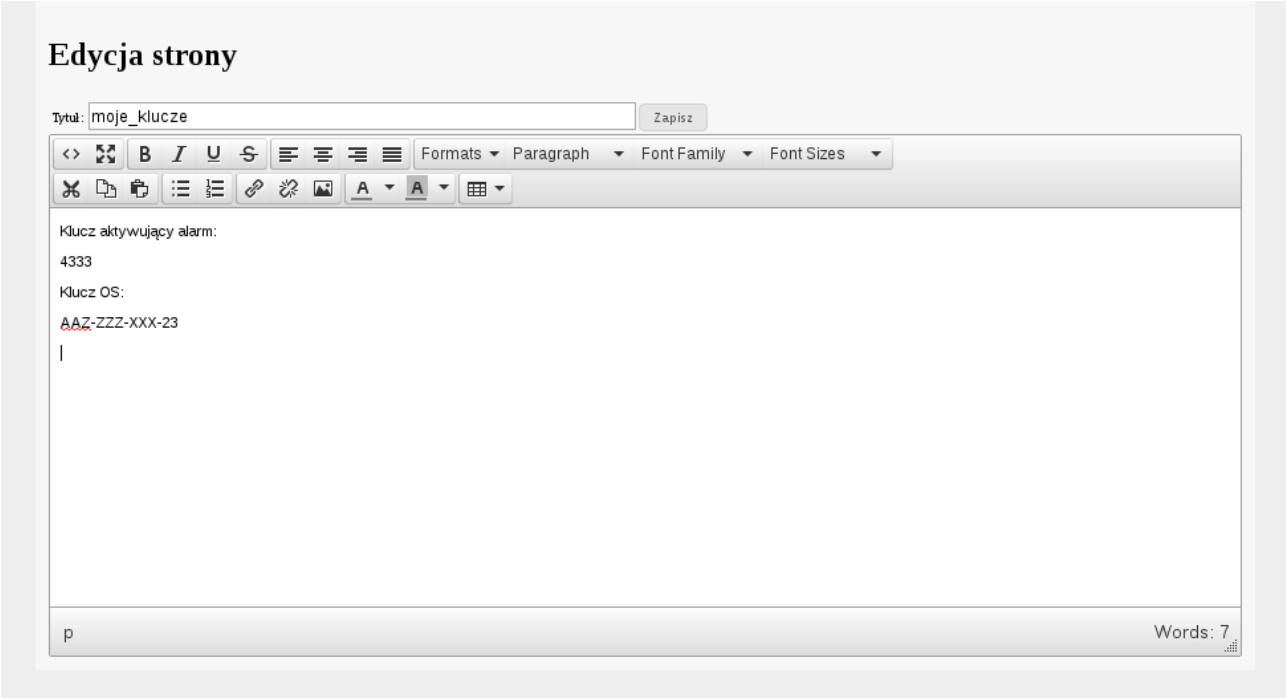
Po zalogowaniu wyświetlana jest strona główna. Użytkownik może na niej zamieścić własne treści, odnośniki do swoich podstron itp.



Strona startowa.

Zakładanie strony

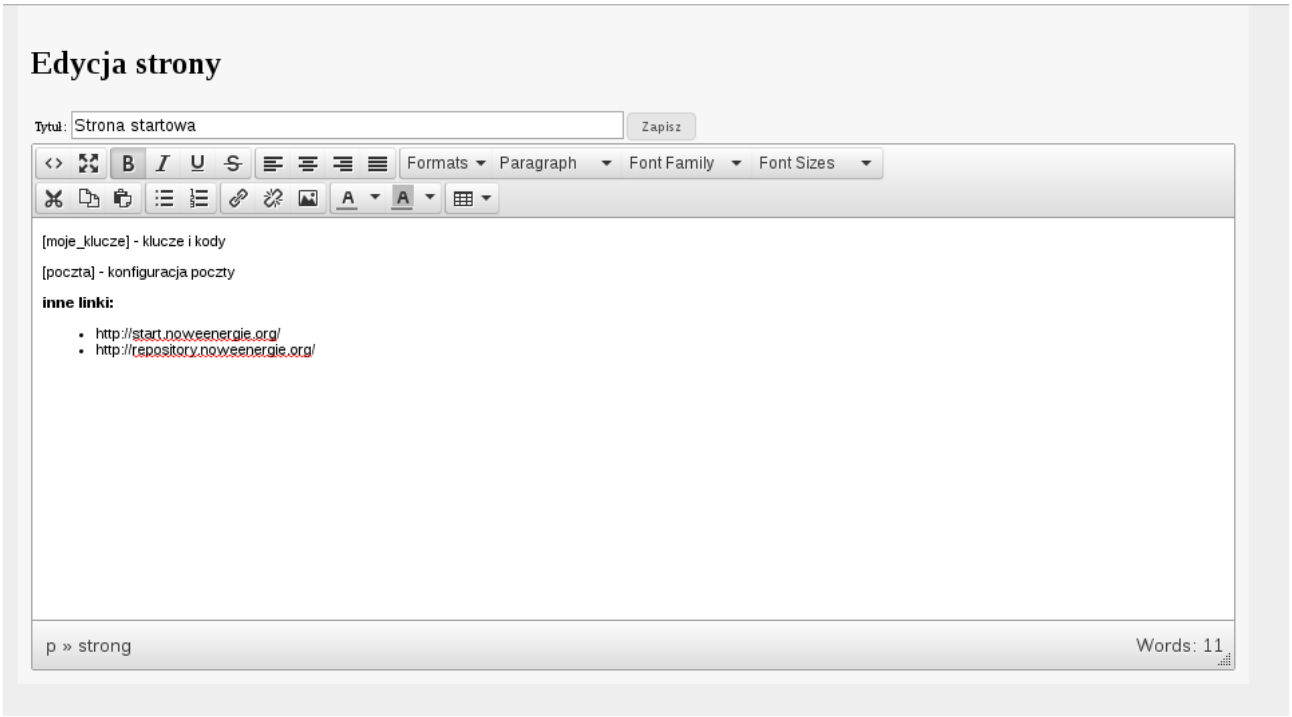
By utworzyć podstronę, należy z głównego menu kliknąć przycisk „Nowa”. Tytuł strony nie może zawierać spacji oraz znaków diakrytycznych, gdyż tytuł strony będzie użyty do stworzenia adresu URL np. strona o tytule „moje_klucze” będzie dostępna pod adresem http://localhost/secretwiki/index.php?Page/moje_klucze



Nowa strona.

Edycja strony

Aktualnie wyświetlona strona może zostać edytowana po kliknięciu przycisku „Edytuj” z głównego menu.



Edycja strony.

Tworzenie odnośników do podstron może zostać zautomatyzowane. Po wprowadzeniu tytułu strony w nawiasach kwadratowych aplikacja automatycznie będzie wyświetlać hiperłącze do danej strony.

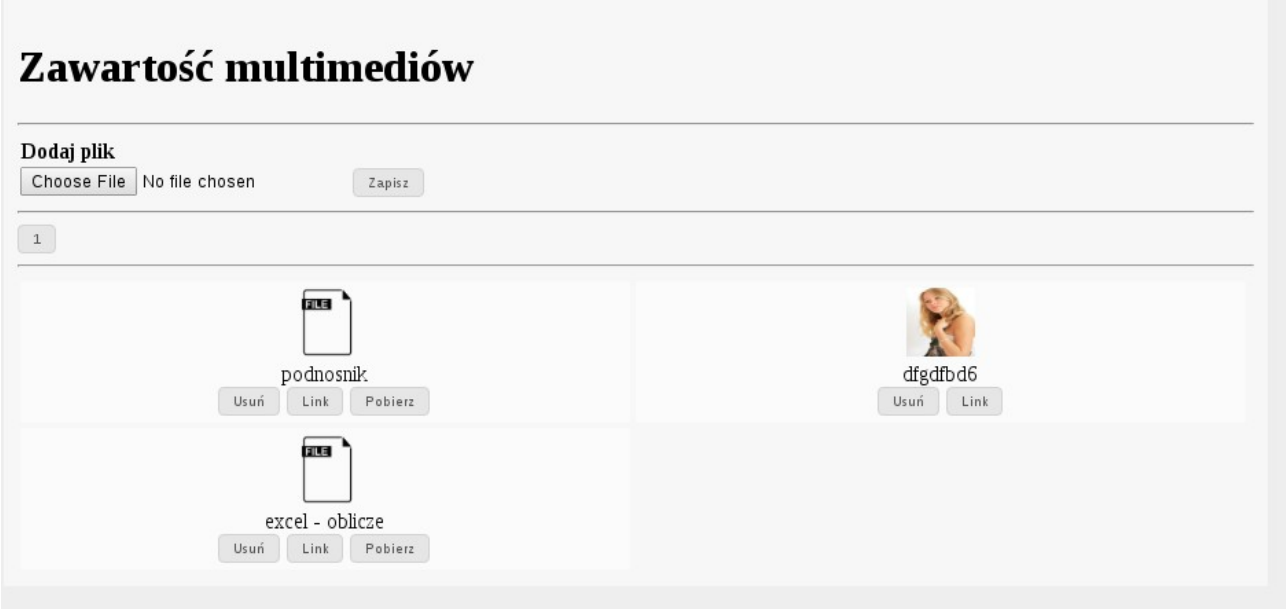
Przykładowo: [moje_klucze]
spowoduje wstawienie hiperłącza:
moje_klucze
W treści strony w trakcie trybu podglądu.

Usuwanie strony

Wyświetlona strona może zostać wykasowana po kliknięciu przycisku „Usuń” z głównego menu. Nie jest możliwe wykasowanie strony startowej a jedynie jej modyfikacja.

Media

Po kliknięciu przycisku „Media” z głównego menu następuje uruchomienie modułu zarządzającego plikami. W obszarze „Dodaj plik” po wybraniu z komputera użytkownika pliku i kliknięciu „Zapisz” następuje wysłanie pliku do aplikacji. Pliki graficzne mogą zostać podejrzane po ich kliknięciu, natomiast pliki tekstowe, aplikacje itp. mogą zostać pobrane po kliknięciu przycisku „Pobierz”. Przycisk „Link” otwiera okno z adresem URL pliku, który może zostać osadzony na dowolnej stronie w aplikacji.



Zawartość multimediów.

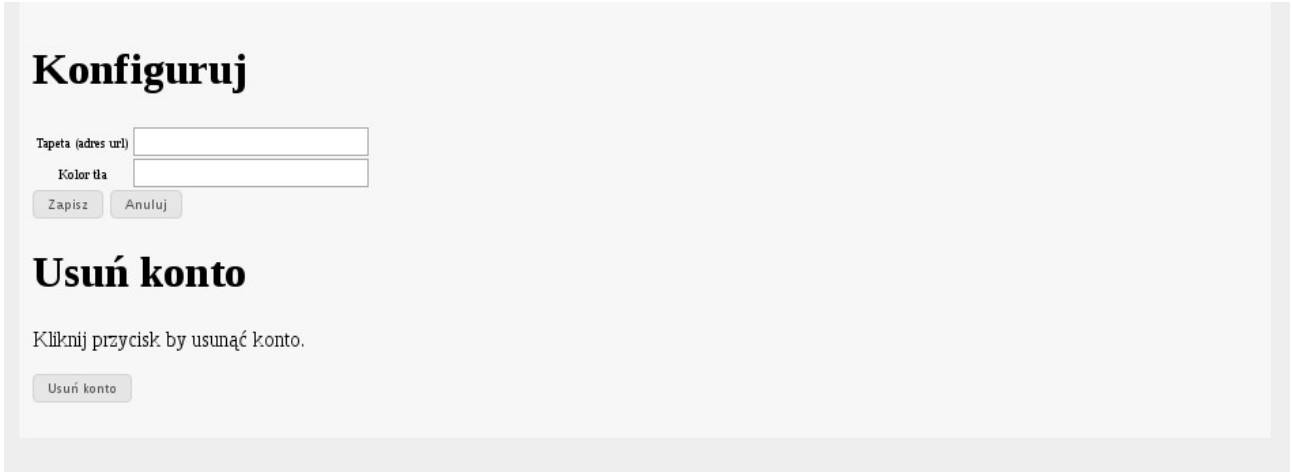
Wyszukiwanie

Wyszukiwanie treści na utworzonych stronach następuje po wpisaniu szukanej frazy w polu obok głównego menu i kliknięciu przycisku „Szukaj”.

Wyniki wyszukiwania.

Konfiguracja

Personalizacja aplikacji oraz usunięcie konta wraz z wszelkimi danymi odbywa się po kliknięciu przycisku „Konfiguruj” z głównego menu.



Personalizacja aplikacji.

Algorytm szyfrujący

Zarówno pliki użytkownika jak i utworzone strony są zapisane w bazie danych w formie zaszyfrowanej.

W trakcie rejestracji użytkownika tworzony jest losowy ciąg CKEY, który wraz loginem i hasłem zapisany zostaje w bazie danych.

$ckey = md5(uniqid(rand(), true));

CKEY bierze udział w algorytmie szyfrującym i deszyfrującym. Przekazywany jest wraz z hasłem i ciągiem do zaszyfrowania do metody DataCrypt.

DataCrypt($plaintext, $password, $ckey)

Algorytm szyfrujący następnie buduje ciąg będący hasłem które składa się z hasła użytkownika i CKEY:

$k = md5($password . '' . $ckey);

następnie tworzony jest klucz:

$key = pack('H', $k);*

$key_size = strlen($key);

By w kolejnym etapie przejść do szyfrowania za pomocą RIJNDAEL128.

$iv_size = mcrypt_get_iv_size(MCRYPT_RIJNDAEL_128, MCRYPT_MODE_CBC);

$iv = mcrypt_create_iv($iv_size, MCRYPT_RAND);

$ciphertext = mcrypt_encrypt(MCRYPT_RIJNDAEL_128, $key, $plaintext, MCRYPT_MODE_CBC, $iv);

$ciphertext = $iv . $ciphertext;

Zaszyfrowane dane są następnie kodowane transportowo do BASE64 co ułatwia ich zapis w bazie danych w formie tekstowej.

return base64_encode($ciphertext);

SSL

W celu zabezpieczenia przesyłanych danych należy zapewnić połączenie SSL z serwerem.