Lipiec 2021

# Dokumentacja Platformy WEB na potrzeby projektu badawczego „Budowa demonstratora Platformy Cyfrowej Nauki” – etap II

## Wstęp

Etap II projektu webserwisu polegał na implementacji i uruchomieniu prototypu webserwisu, który zawiera m.in. funkcjonalność rejestracji i autoryzacji użytkowników. Dodatkowo webserwis umożliwa przetestowanie podstawowych funkcjonalności zdefiniowanych w wymaganiach i założeniach projektu:

- Integracja ze Sketchfab API Viewer.
- Pobranie danych dotyczących poszczególnych modeli z serwisu Sketchfab.
- Kategoryzacja modeli.
- Definiowanie zasobów „chronionych” modeli (dostępnych po autoryzacji użytkownika).
- Wyszukiwarka AJAX i słowa kluczowe modelu.
- Gromadzenie statystyk wraz z możliwością eksportu danych do PDF.
- Zarządzanie funkcjonalnościami i treściami w Panelu Administracyjnym.

Na potrzeby projektu przeprowadzono rozbudowę i aktualizację rdzenia systemu (1), który ma zostać wykorzystany do implementacji webserwisu. Dodatkowo modernizacji uległa również „część admina” (2) webserwisu

(1) – rdzeń systemu, to pliki systemu, realizujące funkcje poszczególnych warstw. Nie mogą być edytowane/zmieniane. Są aktualizowane za pośrednictwem dedykowanego repozytorium lub w sposób ręczny (gdy środowisko produkcyjne nie pozwala na udział zewnętrznych zasobów). Aktualizacja rdzenia systemu zapewnia bezpieczeństwo systemu, umożliwia rozwój funkcjonalności, a także poprawia komfort i wydajność pracy w „części klienckiej” (więcej w dokumentacji do etapu pierwszego projektu).

(2) – część admina, pliki systemu, połączone z rdzeniem, które nie mogą być zmieniane. Są aktualizowane tylko ręcznie. Aby móc pracować w części admina systemu należy poprawnie przejść proces autoryzacji. Działania realizowane w części admina mają

wpływ zarówno na funkcjonowanie systemu w części klienckiej jak i prezentowanie tam danych z bazy danych (więcej w dokumentacji do etapu pierwszego projektu).

## Poszczególne elementy systemu

### Część kliencka

Użytkownicy

W sekcji „rejestracja", użytkownik może zdefiniować w bazie webserwisu własne konto (które będzie powiązane z jego adresem e-mail). Po udanym procesie rejestracji użytkownik otrzyma na użyty adres e-mail, link ustawienia hasła w webserwisie (brak aktywacji czyli ustawienia własnego hasła, sprawi że użytkownik będzie nieaktywny, a co za tym idzie nie będzie mógł zalogować się do webserwisu). Ostatnią czynnością jaką musi zostać wykonana w celu aktywowania użytkownika jest akceptacja jego konta przez administratora webserwisu.

Ustawienie hasła w webserwisie. W pierwszej kolejności użytkownik musi otworzyć adres webserwisu, a następnie przejść do sekcji „autoryzacja" i „ustaw hasło". Na stronie, która się wyświetli użytkownik musi wprowadzić adres e-mail, który został przypisany do jego konta. Po wypełnieniu pola i kliknięciu przycisku „wyślij", system sprawdzi czy faktycznie taki adres e-mail został wprowadzony do bazy, jeżeli tak, to użytkownik otrzyma na skrzynkę specjalny adres URL (aktywny link). Następnie, ten adres, musi otworzyć w przeglądarce internetowej. Po uruchomieniu strony zostanie wyświetlony przycisk „ustaw hasło". Etap ten zabezpieczony jest w ten sposób, że dla danego użytkownika (adresu e-mail) jest generowany losowy, unikalny i powiązany z kontem specjalny adres URL. Zmiana URL'a w „sposób ręczny" w spowoduję utratę możliwości ustawienia hasła.

Wracając do potwierdzenia tożsamości, użytkownik uruchamiając przycisk „ustaw hasło", otrzyma na adres e-mail już specjalnie wygenerowane hasło (spełniające wymogi „polityki bezpieczeństwa"). Losowe hasło będzie składało się z 9 pól (3 cyfry, 3 litery, 3 znaki specjalne). Ponadto status „potwierdzenia tożsamości" w bazie danych zostanie włączony (jednak użytkownik, aby móc się zalogować będzie musiał poczekać jeszcze na akceptację administratora).

Wygenerowane przez system hasło zapisywane jest w bazie przy pomocy funkcji password_hash(). Funkcja zapewnia ochronę przed odczytem, np. za pomocą np. „tęczowych

tablic", ponieważ generuje losowy ciąg znaków dodawany do każdego hasła, które ma być zaszyfrowane. Postać zaszyfrowana tego samego hasła nigdy nie wygląda tak samo, przez co weryfikacja poprawności może tylko odbywać się za pomocą funkcji password_verify(), (więcej w punkcie „Aspekty bezpieczeństwa w procesie autoryzacji użytkownika")

Powyższy mechanizm zapewni, że z webserwisu będą korzystać tylko faktycznie autoryzowane osoby, a dostępy do kont będą chronione za pomocą haseł o odpowiedniej złożoności.

Po przeprowadzeniu procesu autoryzacji użytkownik będzie mógł zobaczyć na stronie elementy ze statusem „chronione".

Dla potrzymania sesji użytkownika w webserwisie w bazie danych zostaje wygenerowany specjalny token autentyczności sesji (zmiana adresu IP użytkownika, przeglądarki internetowej, itd. – spowoduje natychmiastowe wylogowanie). Dodatkowo po prawidłowym zalogowaniu użytkownika, w bazie danych jest zarejestrowany znacznik czasu sesji.

Operacja „wylogowania" usuwa wyżej wymienione parametry zarówno po stronie serwera jak i po stronie klienta.

Integracja ze Sketchfab API Viewer

Po stronie klienta, integracja ze sketchfab API Viewer zapewnia wyświetlanie obszaru, w którym wyświetlany jest model 3D danego obiektu. Model ten jest w pełni interaktywny, tzn. za pomocą myszy i funkcji „drag&drop" możemy obracać dowolnie obiekt w przestrzeni. Z kolei za pomocą funkcji „scroll" możemy przybliżyć lub oddalić obiekt.

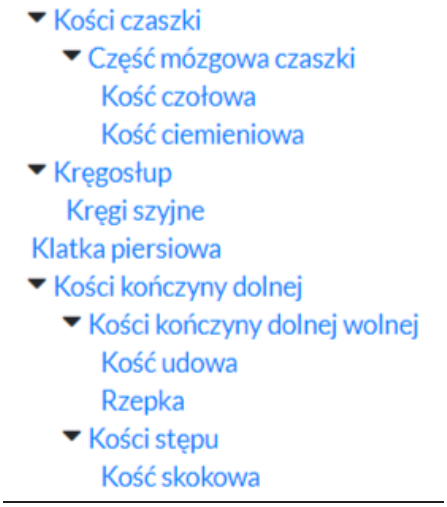

Rys. 1. Obszar wyświetlający model za pośrednictwem Sketchfab API Viewer

Pobranie danych dotyczących poszczególnych modeli z serwisu Sketchfab.

Pobranie danych dotyczących danego modelu z serwisu Sketchfab polega na integracji z API Sketchfab w klasyczny sposób, podczas wykonywania skryptu po stronie serwera (ścieżka URI, REST).

Kategoryzacja modeli.

Za pomocą funkcjonalności kategoryzacji modeli zapewniamy możliwość dostępu do poszczególnych wizualizacji w uporządkowany sposób. Nazwa kategorii wskazuje gdzie w strukturze znajduje się dany model. Drzewo kategorii wraz z przypisanymi modelami tworzy obraz tego, gdzie w hierarchii znajduje się każdy model.




Rys. 2. Przykładowa struktura kategorii

Definiowanie zasobów „chronionych" modeli (dostępnych po autoryzacji użytkownika).

Pliki posiadające status „chronione" zostaną wyświetlone użytkownikowi dopiero po prawidłowo zakończonym procesie autoryzacji.

Wyszukiwarka AJAX i słowa kluczowe modelu.

Użytkownik wpisując słowa kluczowe w pole wyszukiwarki otrzymuje bez odświeżenia strony (kontakt z bazą danych za pośrednictwem technologii AJAX) odpowiedź w postaci nazwy modelu którego dotyczą wpisane przez użytkownika słowa kluczowe. Użytkownik może

skorzystać z podpowiedzi klikając w nią z nich lub po prostu wciskając klawisz ENTER wyświetlić modele pasujące do wprowadzonych słów kluczowych.


Rys. 3. Podpowiedzi AJAX generowane na podstawie słów kluczowych

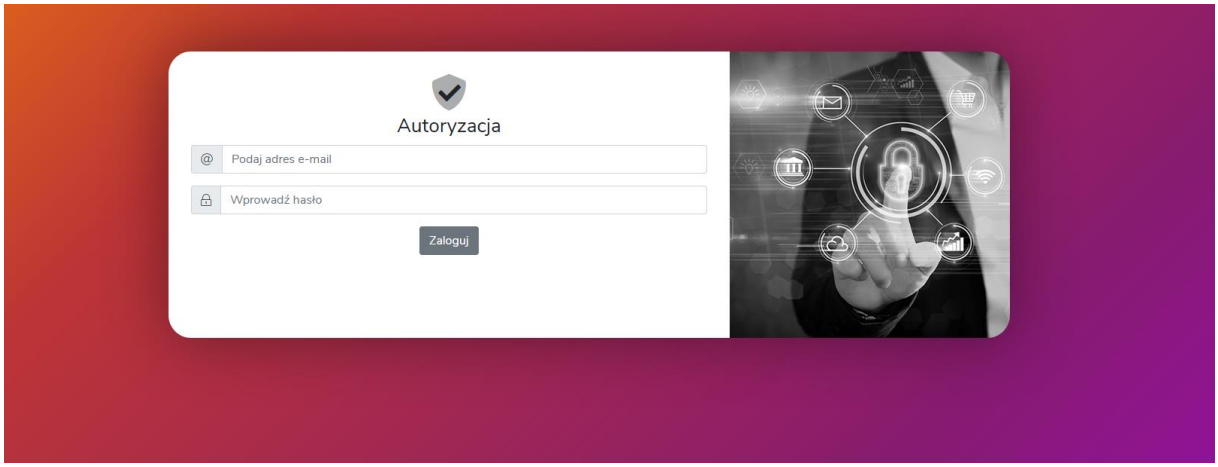
Gromadzenie statystyk wraz z możliwością eksportu danych do PDF.

Do wszelkich zasobów (multimediów) zdefiniowanych w webserwisie są podłączone automatyczne procedury naliczania statystyk pobierania (pliki), wyświetlania (filmy), powiększania (zdjęcia), itp.

**Część admina**

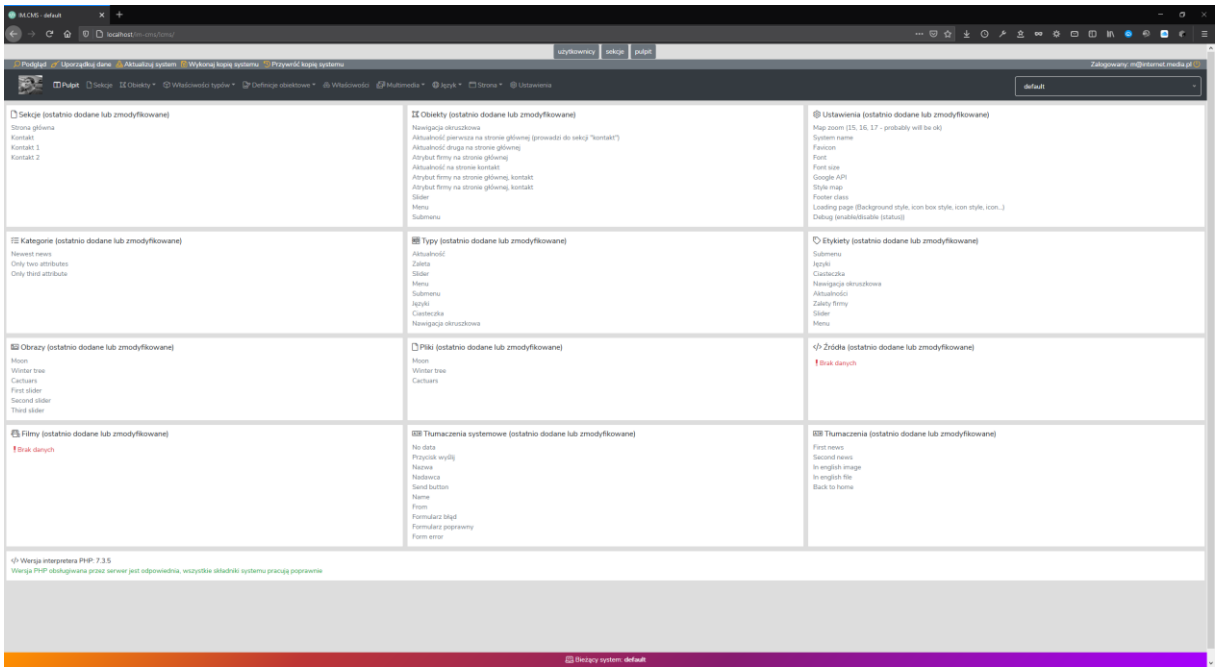
Użytkownicy

Aby zalogować się do zaplecza (CMS) webserwisu należy wpisać w przeglądarce internetowej adres URL zawierający domenę webserwisu http://pcn.cnt.edu.pl i „/[specjalny-ciag-znakow]" (np. **„/&cms"**). Po potwierdzeniu pojawi się okno autoryzacji jak poniżej (rys. 1.).




Rys. 4. Okno autoryzacji administratora

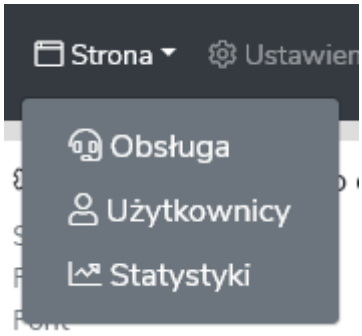
Po wprowadzeniu odpowiednich danych i naciśnięciu przycisku „zaloguj" (klawisz „enter" nie zadziała) ukaże nam się widok „dashboard" CMS webserwisu (rys. 2.).



Rys. 5. Widok „dashboard" administratora webserwisu

Uwaga! Proces autoryzacji wraz z kwestiami technicznymi został omówiony w części „aspekty bezpieczeństwa w procesie autoryzacji użytkownika" niniejszego dokumentu.

Widok po zalogowaniu składa się dużej ilości elementów, w pierwszej kolejności zostanie omówiony sposób zarządzania użytkownikami webserwisu (aktywacja). Aby przejść do listy użytkowników należy w głównym menu wybrać strona => użytkownicy (Rys. 3.).



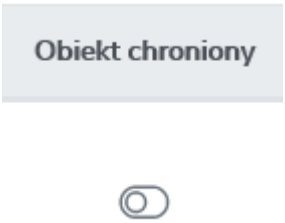

Rys. 6. Główne menu, użytkownicy i statystyki

W oknie pojawia się lista użytkowników zarejestrowanych w systemie. Każdy z użytkowników posiada „status aktywności" (użytkownik nieaktywny nie może się zalogować) i „status potwierdzenia" (użytkownik nie potwierdził tożsamości, czyli nie ustawił hasła dostępu). Każdemu z użytkowników administrator może wysłać wiadomość powitalną. Dodatkowo administrator może dodawać, usuwać, bądź edytować dane użytkowników, a także przypisywać

im prawa do poszczególnych elementów wyświetlanych na stronie (tzw. elementy chronione), w naszym przypadku chronione będą zasoby.

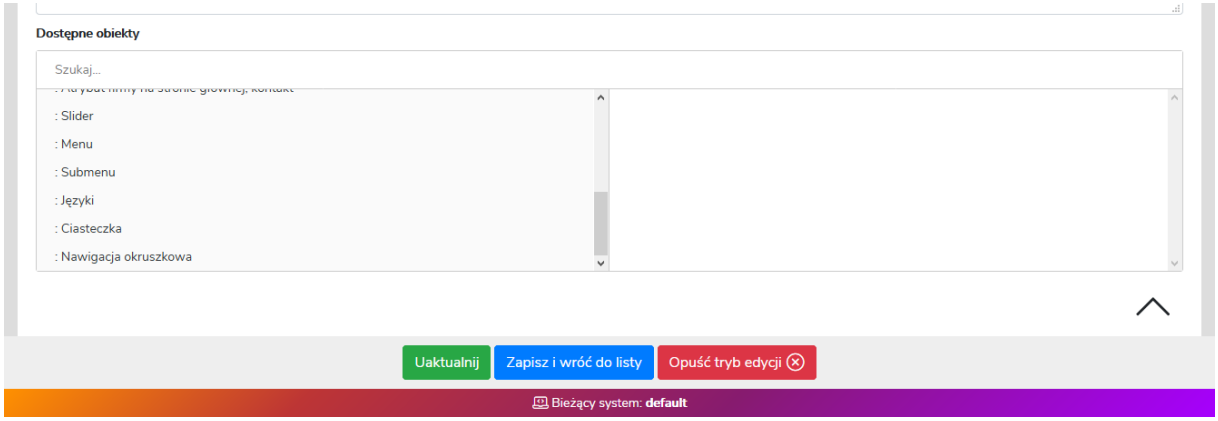
Potwierdzenie tożsamości użytkownika to potwierdzenie za pośrednictwem przypisanego adresu e-mail, swojej tożsamość, czyli rzeczywistego adresu e-mail (więcej w punkcie „część kliencka").

W trybie edycji danego użytkownika znajduje się „sekcja uprawnień" składająca się z dwóch bloków. W lewym bloku znajdują się wszystkie elementy (tzw. obiekty) zdefiniowane/wyświetlane na stronie (definicje elementów/obiektów również tworzy administrator webserwisu). Elementy te, na stronie, są wyświetlane w postaci menu, slidera, tekstu itp. Każdy z tych elementów/obiektów posiada różne właściwości (np. data, zdjęcie, film, formularz, itd.). W naszym przypadku obiektami będą „modele" pobierane z serwisu Sketchfab. Na potrzeby projektu został zdefiniowany nowy element/obiekt wyświetlany na stronie, mianowicie „model". Każdy z modeli będzie mógł mieć status „chroniony" (dostęp dla wybranych użytkowników - autoryzowanych) lub „niechroniony" (wówczas element/obiekt zobaczą wszyscy użytkownicy – z autoryzacją i bez autoryzacji). Obiekt „model" będzie mógł posiadać różne właściwości w postaci zestawu zasobów (np. plików), którym też można nadać status „chroniony".




Rys. 7. Nadanie obiektowi statusu „chroniony"

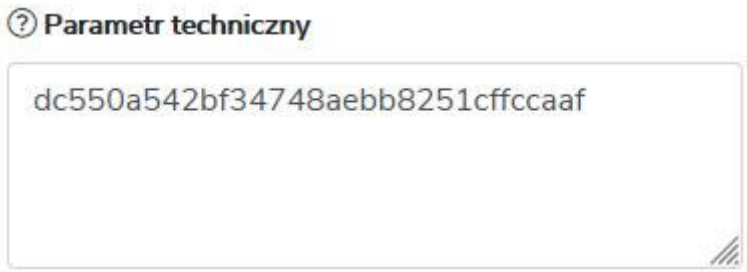
Wracając do sekcji przydzielania praw, podzielonej na dwa bloki, wyżej omówiono blok lewy, natomiast poniżej to czym jest blok prawy. Blok prawy to po prostu elementy/obiekty, które dany użytkownik ma prawo zobaczyć i z którym może pracować (aby ograniczenie działało element/obiekt musi mieć aktywny status „chroniony", a użytkownik oczywiście musi być zautoryzowany).




Rys. 8. Bloki praw w trybie edycji użytkownika

Integracja ze Sketchfab API Viewer

Po stronie admina skonfigurowanie modelu, który ma być pobrany ze Sketchfab ogranicza się jedynie do zdefiniowania w panelu administracyjnym (odpowiednie pole w trybie edycji wybranego modelu) jego UID. Jest to unikalny identyfikator modelu który jest nadawany w serwisie sketchfab każdemu modelowi.




Rys. 9. Pole do wprowadzania UID modelu

Pobranie danych dotyczących poszczególnych modeli z serwisu Sketchfab.

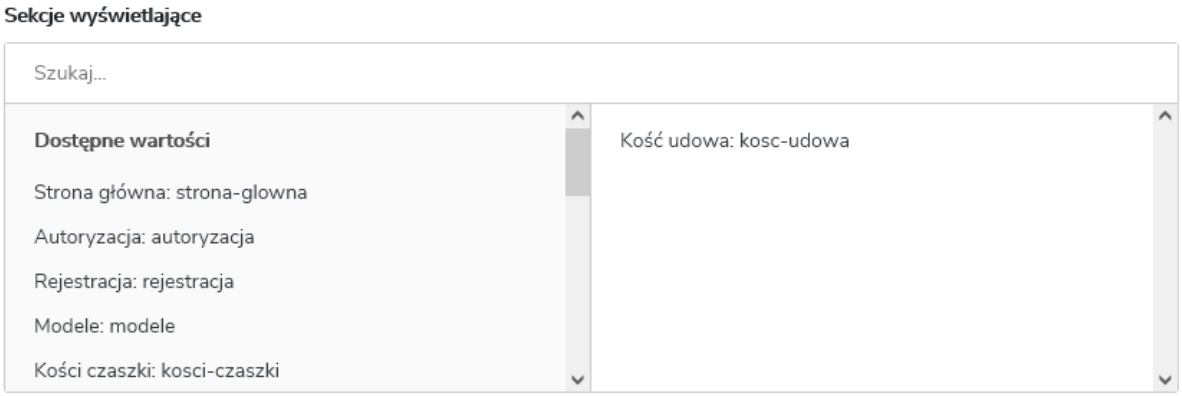
W panelu administracyjnym podając UID modelu w celu integracji ze Sketchfab API Viewer wskazujemy jednocześnie model, którego dane mają zostać pobrane. Tak więc algorytmy webserwisu zapewniają pobieranie danych o modelu już w momencie inicjalizacji jego prezentacji 3D.

Kategoryzacja modeli.

Administrator może sam budować strukturę kategorii przechodząc do *główne menu => sekcje => modele => (ikona „strzałki w prawo" przy danym rekordzie)*.

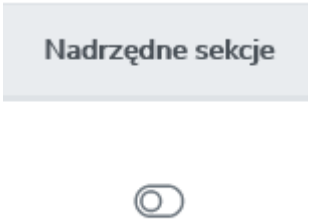

Rys. 10. Przejście do „potomków" danej gałęzi kategorii

Aby przypisać dany model do odpowiedniej gałęzi kategorii, w trybie edycji danego modelu administrator wskazuje w jakich kategoriach (miejsce w strukturze) ma się pojawić.




Rys. 11. Przypisanie modelu do gałęzi kategorii

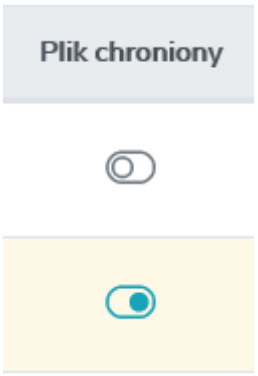
Uwaga, istnieje możliwość „podczepienia" modelu w całej linii kategorii (status „nadrzędne sekcje"), poczynając od „najdalszego potomka" (jego trzeba wskazać w konfiguracji, Rys. 9.) aż do kategorii „root" tego potomka.




Rys. 12. Nadanie obiektowi statusu „nadrzędne sekcje"

Definiowanie zasobów „chronionych" modeli (dostępnych po autoryzacji użytkownika).

W panelu administratora jest możliwość, aby dowolny zasób przełączyć w tryb chroniony (plik, zdjęcie, itd.). Aby to zrobić należy z poziomu listy zasobów (biblioteka zasobów) przełączyć „suwak" w pole „true".




Rys. 13. Włączanie zasobu chronionego (dostępnego po zalogowaniu użytkownika)

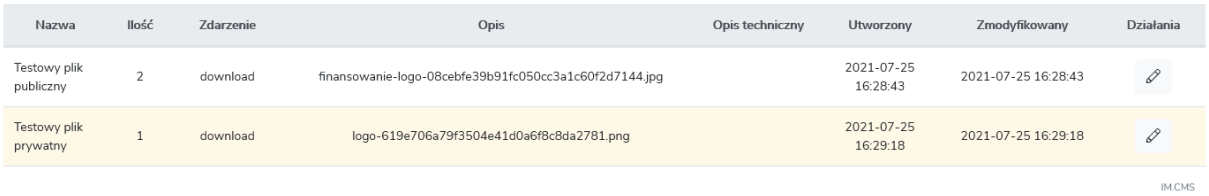
Wyszukiwarka AJAX i słowa kluczowe modelu.

W celu przydzielenia słów kluczowych danemu modelowi należy w trybie jego edycji wprowadzić zbiór w odpowiednie pole.


Rys. 14. Słowa kluczowe przypisane do modelu (w tym przypadku „kość udowa")

Gromadzenie statystyk wraz z możliwością eksportu danych do PDF.

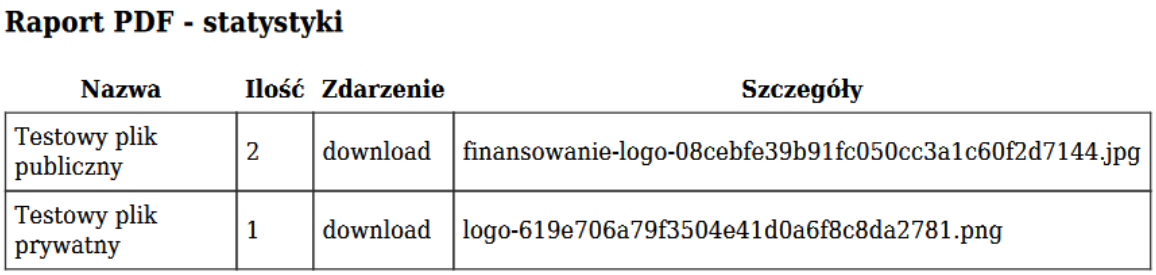
W panelu administracyjnym dostęp do statystyk odbywa się za pośrednictwem *menu głównego => strona => statystyki*. W trybie edycji danej statystyki administrator może dodać swój komentarz. Na wyświetlaną listę statystyk administrator może nałożyć filtr w postaci przedstawienia statystyk dla danego użytkownika (aby statystyka została powiązana z danym użytkownikiem, musi on być zalogowany na swoje konto).



| Nazwa | Ilość | Zdarzenie | Opis | Opis techniczny | Utworzony | Zmodyfikowany | Działania |
|---|---|---|---|---|---|---|---|
| Testowy plik publiczny | 2 | download | finansowanie-logo-08cebfe39b91fc050cc3a1c60f2d7144.jpg | | 2021-07-25 16:28:43 | 2021-07-25 16:28:43 | |
| Testowy plik prywatny | 1 | download | logo-619e706a79f3504e41d0a6f8c8da2781.png | | 2021-07-25 16:29:18 | 2021-07-25 16:29:18 | |

IM.CMS

Rys. 15. Lista statystyk zasobu o zdarzeniu „download"



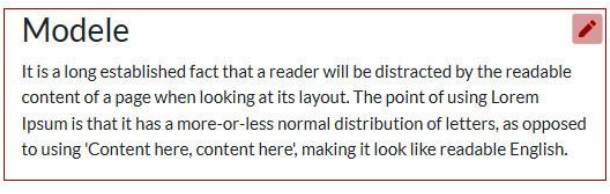
**Raport PDF - statystyki**

| Nazwa | Ilość | Zdarzenie | Szczegóły |
|---|---|---|---|
| Testowy plik publiczny | 2 | download | finansowanie-logo-08cebfe39b91fc050cc3a1c60f2d7144.jpg |
| Testowy plik prywatny | 1 | download | logo-619e706a79f3504e41d0a6f8c8da2781.png |

Rys. 16 Raport w postaci dokumentu PDF

Zarządzanie funkcjonalnościami i treściami w Panelu Administracyjnym.

Panel administracyjny umożliwia zarządzanie wszelkimi treściami w webserwisie. Administrator po pozytywnym przejściu procesu autoryzacji może dodawać, usuwać, zmieniać, włączać lub wyłączać poszczególne elementy na stronie. Dotyczy to zarówno tekstów jak i zdjęć, filmów, plików, źródeł. Dodatkowo w webserwisie edycja poszczególnych zasobów czy tekstów może być dokonywana z poziomu frontu webserwisu (z widoku klienta), za pomocą ikony „edycji" wyświetlonej przy każdym elemencie.




Rys. 17. Edycja z poziomu frontu webserwisu

Wszelkie szczegóły dotyczące pracy z panelem administracyjnym webserwisu zostaną przedstawione w osobnych zasobach lub szkoleniu.

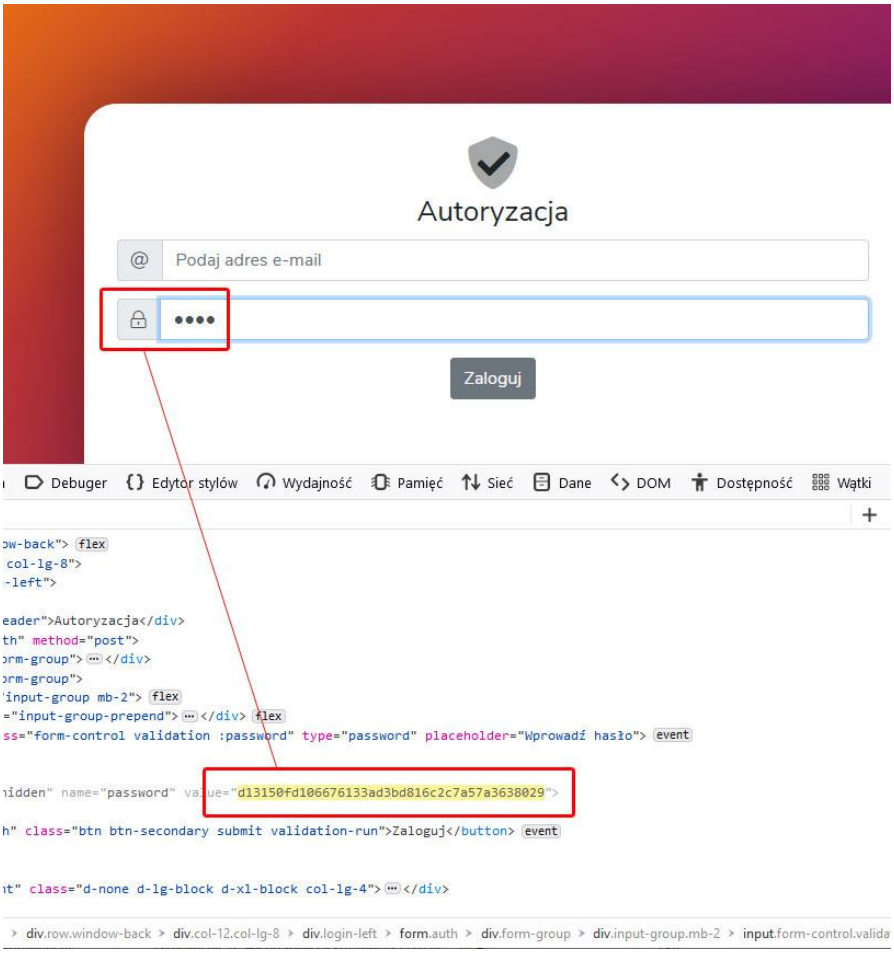
**Proces rozsyłki e-maila**

Do systemu na którym pracuje webserwis została zaimplementowana biblioteka „phpmailer" (pakiet Composer), a sam proces wysyłki odbywa się za pośrednictwem zautoryzowanego konta mailowego (SMTP). Te elementy zapewnią, że przesyłane e-maile będą trafiały do adresatów w sposób należyty i w całości (spam, blokada, filtry).

# Aspekty bezpieczeństwa w procesie autoryzacji użytkownika – funkcja password_hash() i password_verify()

## Proces logowania

Już w formularzu logowania, hasło które wpisuje użytkownik jest hashowane przy pomocy funkcji skrótu SHA1 (nie jest możliwe do odczytania nawet za pomocą narzędzia do podglądu kodu źródłowego). Dodatkowo, za pomocą protokołu SSL przypisanego do domeny webserwisu, odczytanie skrótu np. przy pomocy „tęczowych tablic" (baza skrótów) będzie niemożliwe.




Rys. 18. Hash hasła po stronie klienta przy zdarzeniu keyUp

## Strona serwera

Skrót hasła w postaci SHA1 z formularza jest przesyłany na stronę serwera i tam weryfikacja danych autoryzacji odbywa się przy pomocy funkcji password_verify(). W tym miejscu należy nadmienić, że podczas procesu potwierdzenia tożsamości użytkownika (punkt „poszczególne

elementy systemu", „część kliencka") hasło wygenerowane przez system i wprowadzone do bazy danych zostało zaszyfrowane przy pomocy funkcji password_hash(). Jest to funkcja która zapewnia bardzo wysokie bezpieczeństwo, a także odporność na atak za pośrednictwem „tęczowych tablic". Postać zaszyfrowana tego samego ciągu znaków nigdy nie wygląda tak samo (do ciągu szyfrowanego wprowadzana jest tzw. „sól"), a proces weryfikacji hasła może odbywać się tylko za pomocą funkcji password_verify().

Po tak przeprowadzonej weryfikacji budowana jest strategia potrzymania i weryfikacji sesji, która szerzej została opisana w punkcie „poszczególne elementy systemu", „część kliencka".

Taki sam sposób weryfikacji hasła jest realizowany podczas autoryzacji do panelu zarządzania webserwisu.

Dokumentacja funkcji password_hash():

https://www.php.net/manual/en/function.password-hash.php

Dokumentacja funkcji password_verify():

https://www.php.net/manual/en/function.password-verify.php

Opracowanie: Damian Krawiec

Zielona Góra, 27.07.2021