Bartłomiej Janik
Nr albumu 308787

Warszawa, 2020 r

Dokumentacja

Aplikacja „Raport”

Przedmiot:
Zaawansowane Aplikacje Internetowe
Studia OKNO
Politechnika Warszawska

Spis treści

1. Opis konfiguracji serwera i uruchomienia witryny

Aplikacja dostępna jest pod adresem:

http://bartjanik.northeurope.cloudapp.azure.com

Login: Ula
Hasło: Ulabiuro

Login: adam

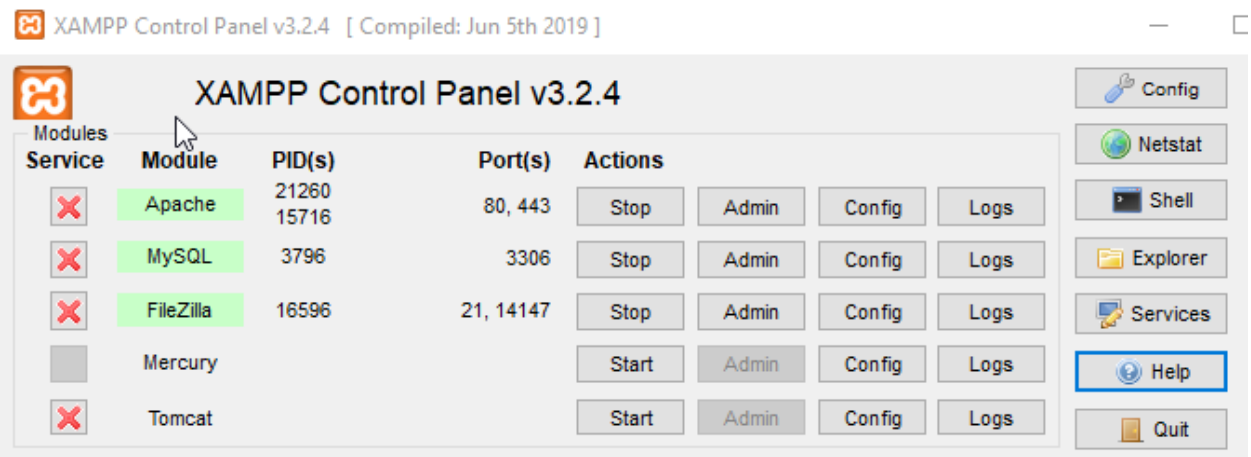
Hasło: adamnewpass

*Jeśli aplikacja jest niedostępna proszę o wiadomość, jest hostowana w Azure i to mogłoby oznaczać, że środki studenckie się skończyły (jest dostępne $100, według planu aplikacja powinna „zużywać" 6 Euro miesięcznie, ale obawiam się jakiś „ukrytych kosztów" co może wyłączyć hosting).

Do uruchomienia aplikacji lokalniem należy zainstalować XAMPP
https://www.apachefriends.org/pl/download.html
Wypakować pliki z paczki .7zip do katalogu C:\xampp\htdocs

I uruchomić serwer Apache i MySQL z panelu XAMPP Control. Nastepnie należy zaimportować plik z bazą danych appdatabase.sql przy użyciu phpMyAdmin http://localhost/phpmyadmin

Do utworzenia aplikacji użyłem środowiska aplikacji XAMPP v3.2.4



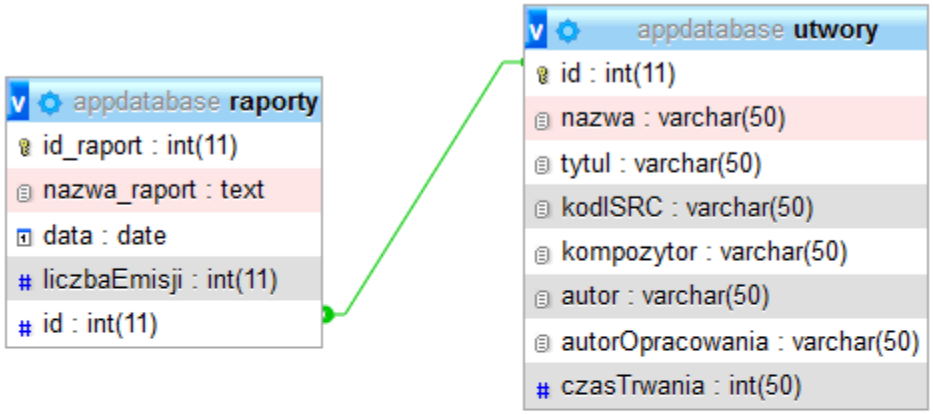
Baza danych mySQL 10.4.14-MariaDB
PHP Version: 7.4.10

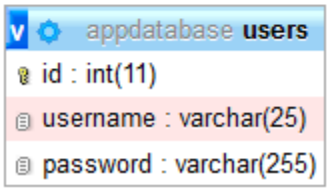
1.1 Opis Bazy danych

Do zarządzania Baza danych, używałem phpMyAdmin i Command line Windows:

```
C:\xampp\mysql\bin>mysql -u root
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 2393
Server version: 10.4.14-MariaDB mariadb.org binary distribution

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> use appdatabase
Database changed
MariaDB [appdatabase]>
```

Baza składa się z 3 tabel:
users – przechowuje dane użytkowników aplikacji
utwory – przehcowuje informacje o utworach
raporty – przechowuje raporty
Skryp bazy danych znajduje się w pliku appdatabase.sql



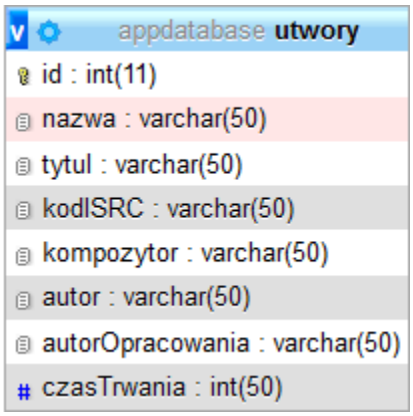


1.2 Tabela users

Służy tylko do logowoania do aplikacji. Nie jest związana relacją z żadną inną tabelą. Hasła są zahashowane dzieki funkcji password_hash.

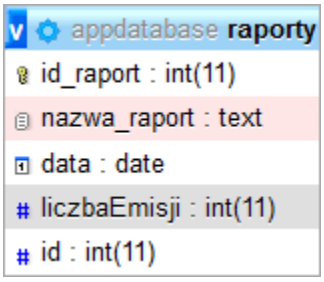
id	username	password
1	adam	$2y$10$7Eoz/riBNUEpoQAyakpTgeU/jrhc5HNSFyzXHu5uoif6hWG3/P.Gm
2	bartek	$2y$10$CMDpE4CapGQZxqFl6Ueg3e1SFovDOlqmr7rEcM4ozURLPiAad.iJK
3	adam1	$2y$10$Ds8xkin958/OkpD/QUTCReMWngl/7l6fSvqT9psCdYcowZ1FYwmj6
4	Julia	$2y$10$X2wyxBQ71uRYEt3fId7.e.WX4WjCYHS.99cCSjOkH6qXlb9WqHnJu
5	Wojtek	$2y$10$sIlIlIQ/XCxqW.e1XYPm2u7LSQB0sM/vFG18Xq3rMaCyMMFkrpSm.
6	Ula	$2y$10$XyGS4vp.9Yu0fhWexgpnAOLD/hjyMf5U3.9QwnKt2WeugCMT7Ukoe
7	John	$2y$10$sSFPQq6kugbDlPNxKnc8.O/7yzI36/KUVH8fTZiMwNlrRd6MTduVK

1.3 Tabela utwory



Pole id jest kluczem głównym tabeli

1.4 Tabela raporty



Pole id_raport jest kluczem głównym, pole id jest kluczem obcym.

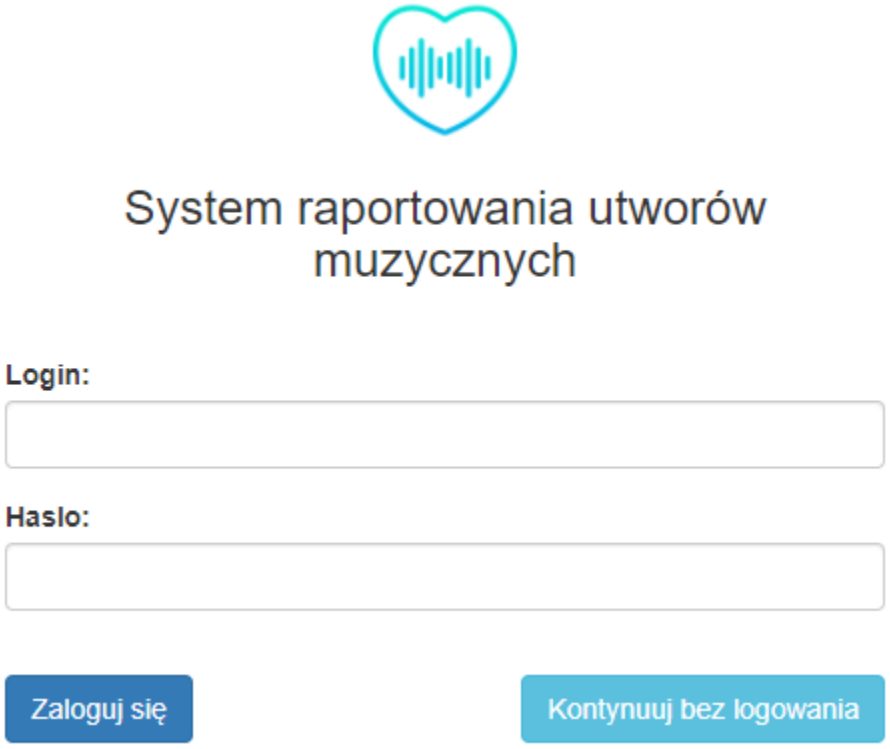
Relacja między tabelami jest okreslona po polu id, z kaskadową regułą usuwania i kasakdową regułą modyfikacji rekordów. Dzięki temu, gdy usunie się lub edytuje dane w tabeli utwory (np. zmiana nazwy) to zostanie również zmodyfikowana tabela raporty, dzięki czemu Raport będzie zawierał zawsze aktualne dane.

```
ALTER TABLE `raporty`
  ADD CONSTRAINT `raporty_ibfk_1` FOREIGN KEY (`id`) REFERENCES `utwory` (`id`) ON DELETE CASCADE ON UPDATE CASCADE;
COMMIT;
```

2. Opis kodu aplikacji

2.1 Strona logowania do aplikacji

Index.php – stonra główna aplikacji. Jest to również storna logowania.



Sprawdzenie czy użytkownik jest zalogowany:

```php
<?php
    //Sprawdzamy czy user jest zalogowany, jak nie to na strone logowania
    session_start();
        if(isset($_SESSION['zalogowany']) && ($_SESSION['zalogowany']==true))
    {
        header('Location: welcome.php');
        exit();
    } //jesli istnieje zmienna zalogowany i jest na true to kieruj do welcome.php

?>
```

Przykładowe dane logowania:
Login: **Ula**
Haslo: **Ulabiuro**

Po wpisaniu Login/Haslo, wykona sie plik **zaloguj.php** i przekieruje do strony Startowej zalogowanego użytkownika **welcome.php**

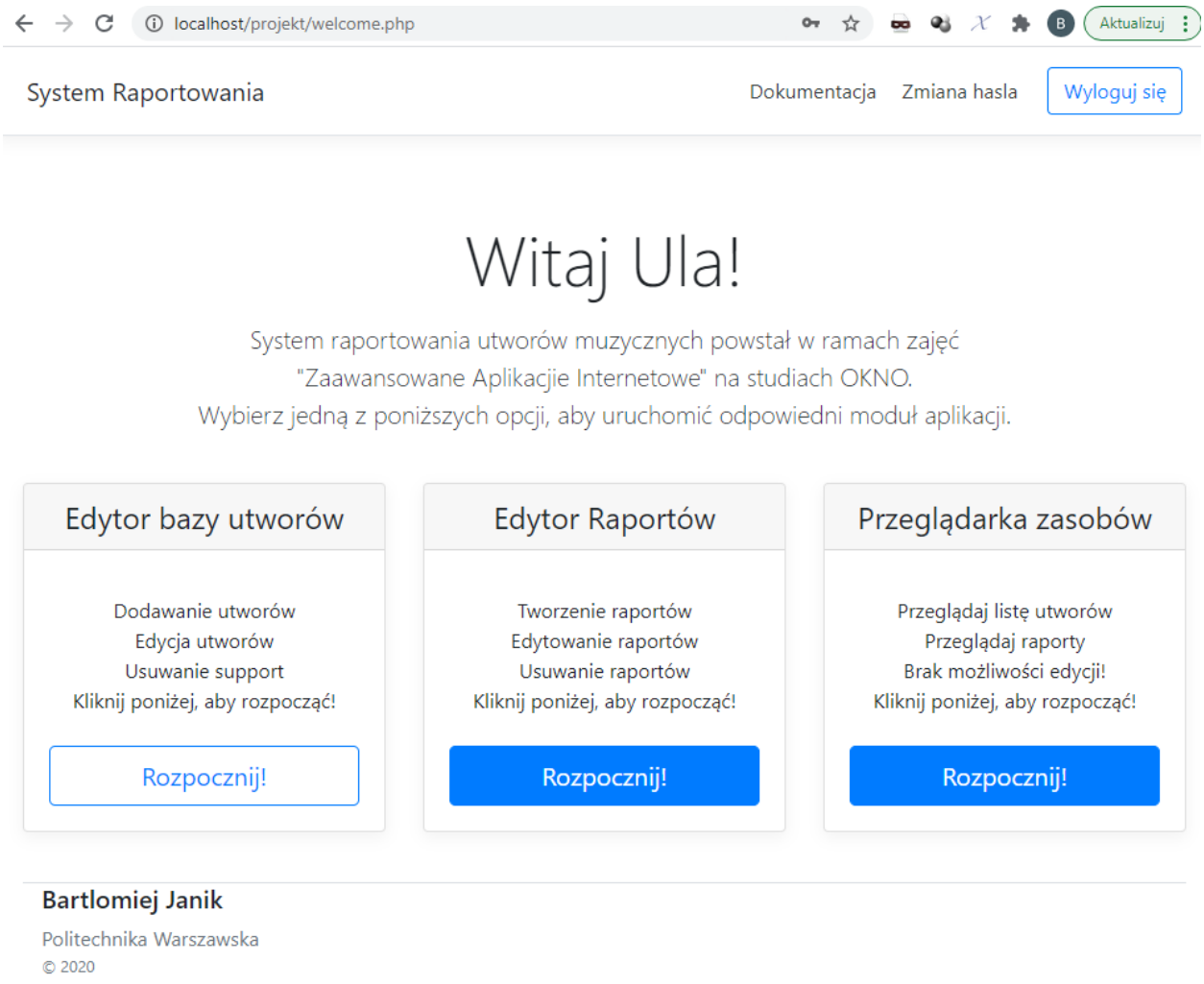
Ochrona przed SQL injection jest zpaeniona dzięki funkcji htmlentities w pliku **zaloguj.php**

```
$login = htmlentities($login, ENT_QUOTES, "UTF-8");
$haslo = htmlentities($haslo, ENT_QUOTES, "UTF-8");
```

Przy ataku SQL injection, atakujący wpisuje w pole formularza login i hasło np. jak niżej:
Login: „aaa”
Hasło: ‘ OR 1=1 --
[apostrof, spacja, OR, spacja, 1=1, spacja, dwa myślniki, spacja]
Z formualrza html do bazy wykona się zapytanie jak niżej:

```
SELECT * from users WHERE
user='aaa' AND password='' OR 1=1 -- '
```

Zaznaczony na żółto warunek da zawsze wartośc False, a na zielono zawsze true (ostatni apostrof będzie pominięty dzięki – znakowi komentarza). W mojej aplikacji dzięki przepuszczeniu pól formularza login i haslo przez funkcje htmlentities, co blokuje atak.



2.2 Zmiana hasła

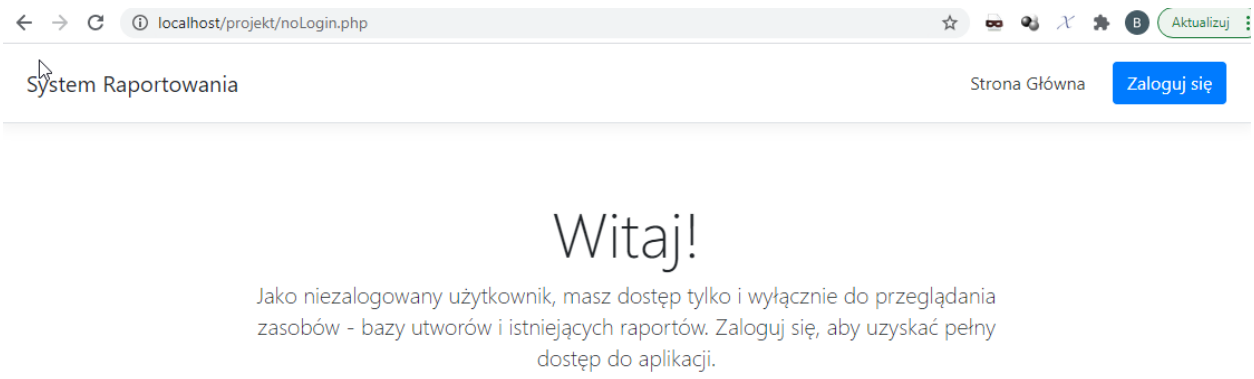
reset-password.php – służy do resetowania i nadania nowego hasła przez zalogowanego użytkownika

```php
// Procesowanie formularza, gdy uzytkownik kliknie Zatwierdź
if($_SERVER["REQUEST_METHOD"] == "POST"){

    // Walidacja nowego hasła
    if(empty(trim($_POST["new_password"]))){
        $new_password_err = "Wpisz nowe haslo!";
    } elseif(strlen(trim($_POST["new_password"])) < 6){
        $new_password_err = "Haslo musi miec minimum 6 znaków!";
    } else{
        $new_password = trim($_POST["new_password"]);
    }

    // Walidacja pola potwierdzenia hasła
    if(empty(trim($_POST["confirm_password"]))){
        $confirm_password_err = "Potwierdź hasło!";
    } else{
        $confirm_password = trim($_POST["confirm_password"]);
        if(empty($new_password_err) && ($new_password != $confirm_password)){
            $confirm_password_err = "Wpisane hasła nie są takie same!";
        }
    }

    // Sprawdzam czy są błędy zanim Update sie wykona
    if(empty($new_password_err) && empty($confirm_password_err)){
        // Update statement
        $sql = "UPDATE users SET password = ? WHERE id = ?";

        if($stmt = mysqli_prepare($link, $sql)){
            // Dopisanie zmiennych do prepared statement jako parametry
            mysqli_stmt_bind_param($stmt, "si", $param_password, $param_id);

            // Przypisanie parametrów, w tym hash z wpisanego hasła
            $param_password = password_hash($new_password, PASSWORD_DEFAULT);
            $param_id = $_SESSION["id"];

            // Wykonanie prepared statement
            if(mysqli_stmt_execute($stmt)){
                // Jesli hasło zmienione to destroy session i przekiruj na index.php
                session_destroy();
                header("location: index.php");
                exit();
            } else{
                echo "Cos poszlo nie tak.";
            }

            // zamykam statement
            mysqli_stmt_close($stmt);
        }
    }
```

3. Moduły aplikacji

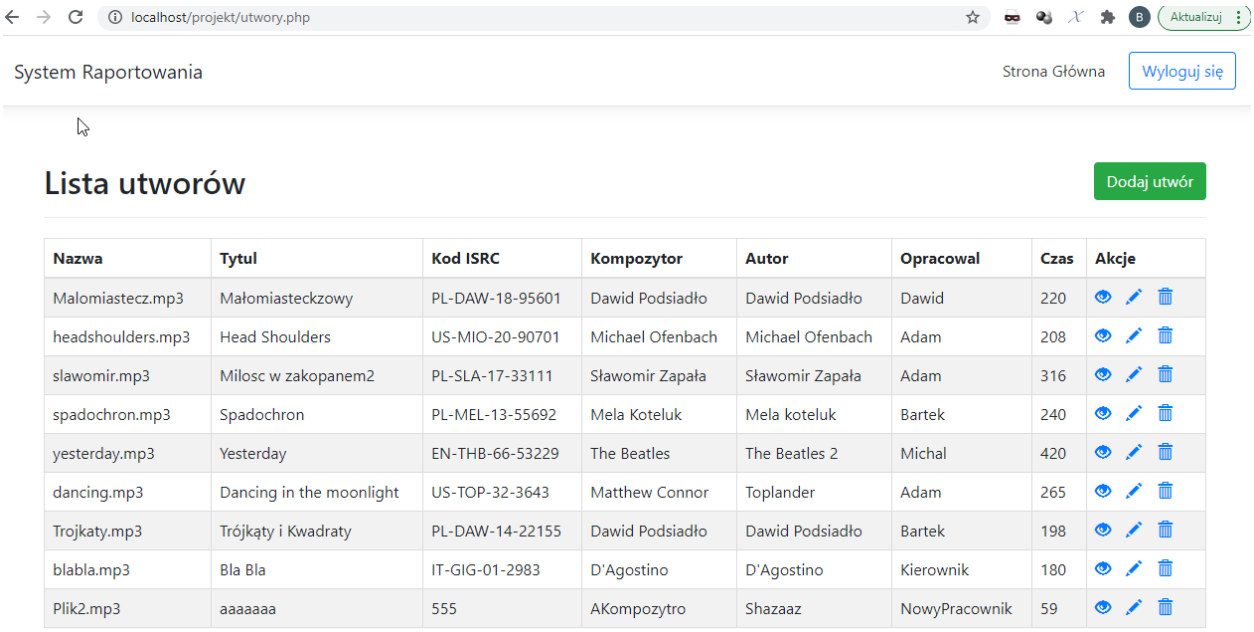
Aplikacja składa się z 3 modułów:
Edytor bazy utworów -> **utwory.php**
Edytor Raportów **-> raporty.php**
Przeglądarka zasobów -> **viewer.php**

Natomiast, po kliknięciu „Kontynuuj bez logowania” przekeiruje do **noLogin.php** – strony startowej dla niezalogowanego użytkonika



3.1 Edytor bazy utworów

utwory.php – Moduł do podglądania, edycji, dodawania i usuwania utworów z tabeli utwory.



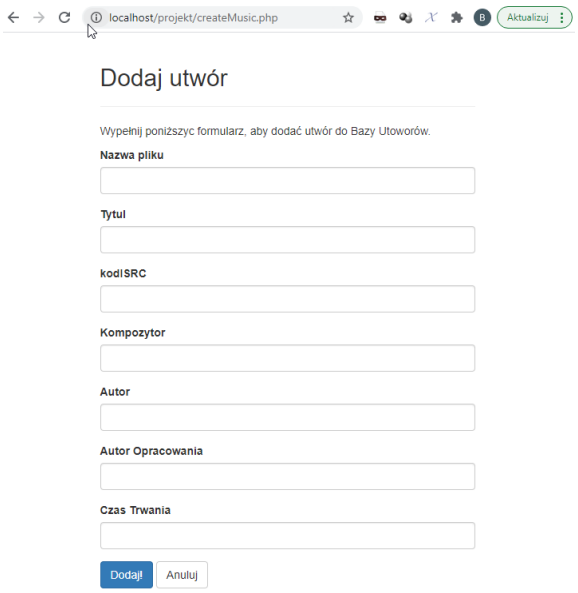
Nazwa	Tytul	Kod ISRC	Kompozytor	Autor	Opracowal	Czas	Akcje
Malomiastecz.mp3	Małomiasteckzowy	PL-DAW-18-95601	Dawid Podsiadło	Dawid Podsiadło	Dawid	220	
headshoulders.mp3	Head Shoulders	US-MIO-20-90701	Michael Ofenbach	Michael Ofenbach	Adam	208	
slawomir.mp3	Milosc w zakopanem2	PL-SLA-17-33111	Sławomir Zapała	Sławomir Zapała	Adam	316	
spadochron.mp3	Spadochron	PL-MEL-13-55692	Mela Koteluk	Mela koteluk	Bartek	240	
yesterday.mp3	Yesterday	EN-THB-66-53229	The Beatles	The Beatles 2	Michal	420	
dancing.mp3	Dancing in the moonlight	US-TOP-32-3643	Matthew Connor	Toplander	Adam	265	
Trojkaty.mp3	Trójkąty i Kwadraty	PL-DAW-14-22155	Dawid Podsiadło	Dawid Podsiadło	Bartek	198	
blabla.mp3	Bla Bla	IT-GIG-01-2983	D'Agostino	D'Agostino	Kierownik	180	
Plik2.mp3	aaaaaaa	555	AKompozytro	Shazaaz	NowyPracownik	59	

```php
<?php
// Dołączam plik z połączeniem bazy danych
require_once "connect.php";
$link = mysqli_connect($host, $db_user, $db_password, $db_name);

// Wykonanie zapytania do bazy
$sql = "SELECT * FROM utwory"; //wybieram wszystkie z tbaeli utowry i wrzucam do tabeli html poniżej
if($result = mysqli_query($link, $sql)){
    if(mysqli_num_rows($result) > 0){
        echo "<table class='table table-bordered table-striped'>";
            echo "<thead>";
                echo "<tr>";
                    //echo "<th>#</th>";
                    echo "<th>Nazwa</th>";
                    echo "<th>Tytul</th>";
                    echo "<th>Kod ISRC</th>";
                    echo "<th>Kompozytor</th>";
                    echo "<th>Autor</th>";
                    echo "<th>Opracowal</th>";
                    echo "<th>Czas</th>";
                    echo "<th>Akcje</th>";
                echo "</tr>";
            echo "</thead>";
            echo "<tbody>";
            while($row = mysqli_fetch_array($result)){
                echo "<tr>";
                    //echo "<td>" . $row['id'] . "</td>";
                    echo "<td>" . $row['nazwa'] . "</td>";
                    echo "<td>" . $row['tytul'] . "</td>";
                    echo "<td>" . $row['kodISRC'] . "</td>";
                    echo "<td>" . $row['kompozytor'] . "</td>";
                    echo "<td>" . $row['autor'] . "</td>";
                    echo "<td>" . $row['autorOpracowania'] . "</td>";
                    echo "<td>" . $row['czasTrwania'] . "</td>";
                    echo "<td>";
```

Przyciski akcji: w zalezności od użytego przkeirują do plików read.php update.php delete.php dodając do url, id wybranego utworu. (ikony z bootstrap, dołączony na początku pliku)

```php
echo "<td>";
    echo "<a href='read.php?id=". $row['id'] ."' title='Podgląd' data-toggle='tooltip'><span class='glyphicon glyphicon-eye-open'></span></a>";
    echo "<a href='update.php?id=". $row['id'] ."' title='Edycja' data-toggle='tooltip'><span class='glyphicon glyphicon-pencil'></span></a>";
    echo "<a href='delete.php?id=". $row['id'] ."' title='Usuń!' data-toggle='tooltip'><span class='glyphicon glyphicon-trash'></span></a>";
echo "</td>";
```

Po kliknięciu „Dodaj utwór” przekieruje createMusic.php, gdzie użytkownik wpisuje informacje o utworze i po kliknięciu Dodaj! Wykonuje się Insert do bazy danych. Anuluj – wróci do utowry.php



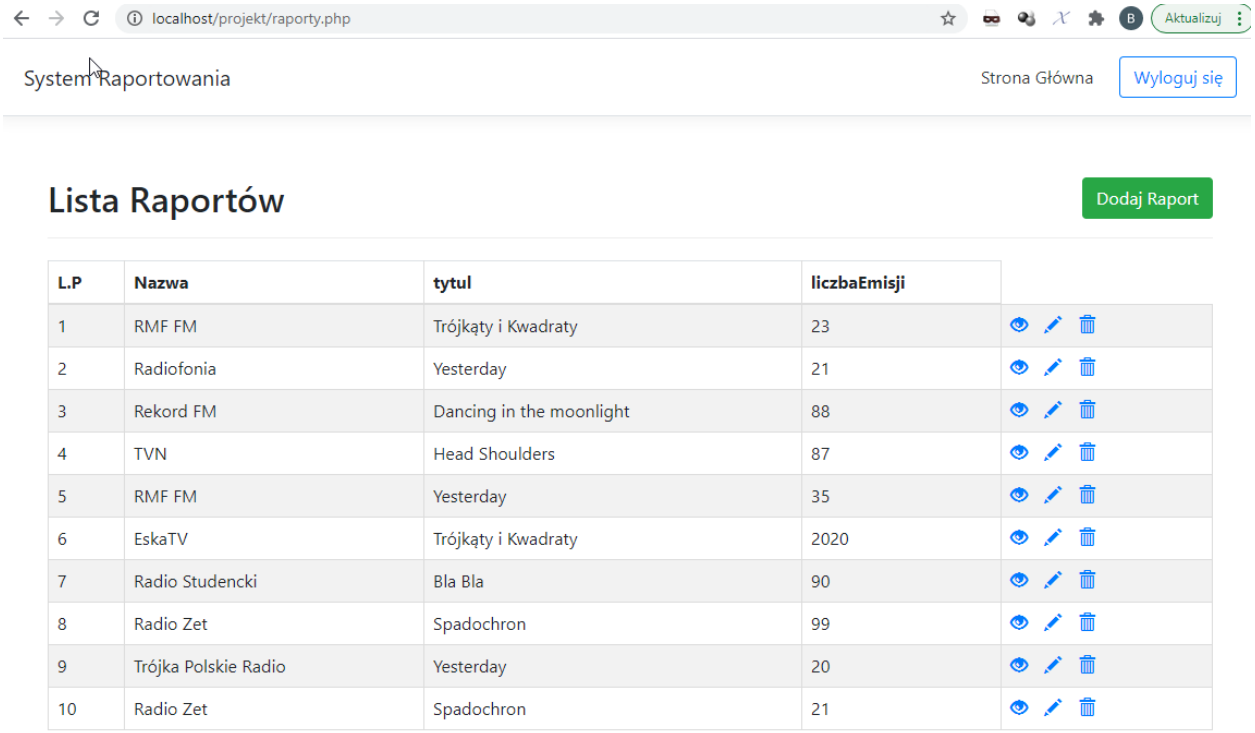
createMusic.php

Po kliknięciu dodaj wykona się poniższy Insert do bazy danych

```php
$sql = "INSERT INTO utwory (nazwa, tytul, kodISRC, kompozytor, autor, autorOpracowania, czasTrwania) VALUES (?, ?, ?, ?, ?, ?, ?)";

if($stmt = mysqli_prepare($link, $sql)){
    // Dołączenie zmiennych jako parametrów do prepared statements
    mysqli_stmt_bind_param($stmt, "sssssss", $param_name, $param_tytul, $param_kodISRC, $param_kompozytor, $param_autor, $param_autorOpracowania, $param_czasTrwania);

    // Przypisanie parametrów
    $param_name = $nazwa;
    $param_tytul = $tytul;
    $param_kodISRC = $kodISRC;
    $param_kompozytor = $kompozytor;
    $param_autor = $autor;
    $param_autorOpracowania = $autorOpracowania;
    $param_czasTrwania = $czasTrwania;

    // Wykonanie prepared statement
    if(mysqli_stmt_execute($stmt)){
        // Records created successfully. Redirect to landing page
        header("location: utwory.php");
        exit();
    } else{
        echo "Cos poszlo nie tak!";
    }
}
```

3.2 Edytor Raportów

raporty.php - Przedstawia istniejące Raporty oraz po kliknięciu Dodaj! (createRaport.php) Umożliwia dodanie nowego raportu



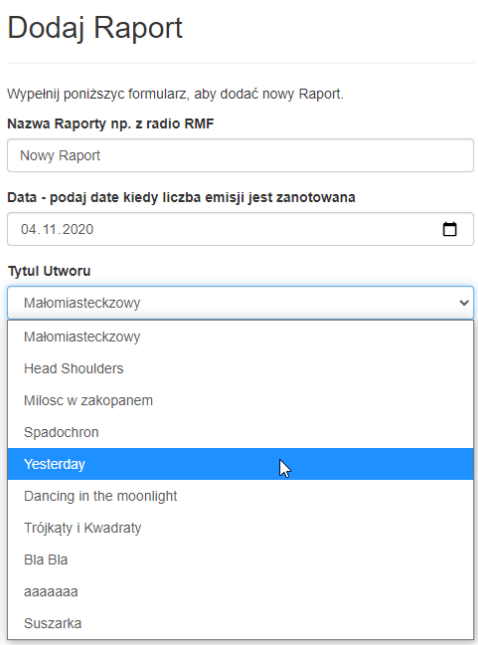
L.P	Nazwa	tytul	liczbaEmisji
1	RMF FM	Trójkąty i Kwadraty	23
2	Radiofonia	Yesterday	21
3	Rekord FM	Dancing in the moonlight	88
4	TVN	Head Shoulders	87
5	RMF FM	Yesterday	35
6	EskaTV	Trójkąty i Kwadraty	2020
7	Radio Studencki	Bla Bla	90
8	Radio Zet	Spadochron	99
9	Trójka Polskie Radio	Yesterday	20
10	Radio Zet	Spadochron	21

Plik **raporty.php**

Tutaj, aby wyświetlić dany raport, trzeb użyć złączenia Left Join tabel raporty i utwory używając pola id z tabeli utwory. Select będzie wyglądał jak poniżej

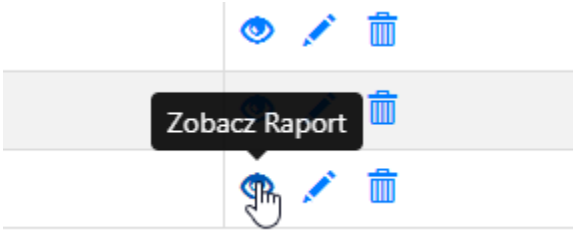
```php
<?php
// Dołacznie pliku config
require_once "connect.php";
$link = mysqli_connect($host, $db_user, $db_password, $db_name);

// Attempt select query execution
$sql = "SELECT * FROM (raporty LEFT JOIN utwory USING(id))";
if($result = mysqli_query($link, $sql)){
    if(mysqli_num_rows($result) > 0){
        echo "<table class='table table-bordered table-striped'>";
            echo "<thead>";
                echo "<tr>";
                    echo "<th>L.P</th>";
                    echo "<th>Nazwa</th>";
                    //echo "<th>id</th>";
                    echo "<th>tytul</th>";
                    echo "<th>liczbaEmisji</th>";
                echo "</tr>";
            echo "</thead>";
            echo "<tbody>";
            while($row = mysqli_fetch_array($result)){
                echo "<tr>";
                    echo "<td>" . $row['id_raport'] . "</td>";
                    echo "<td>" . $row['nazwa_raport'] . "</td>";
                    //echo "<td>" . $row['id'] . "</td>";
                    echo "<td>" . $row['tytul'] . "</td>";
                    echo "<td>" . $row['liczbaEmisji'] . "</td>";
                    echo "<td>";
```

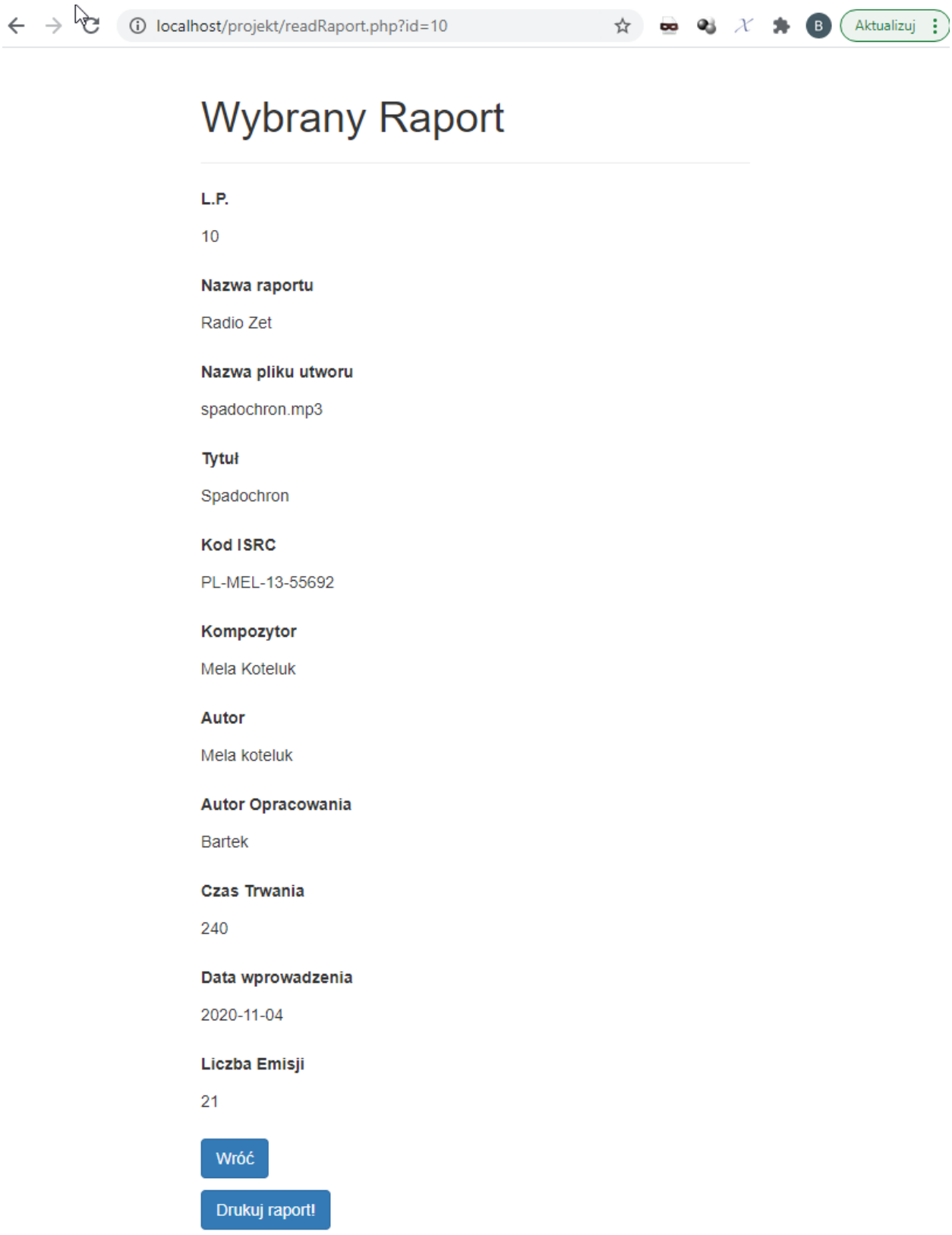
Po Kliknięciu Dodaj raport, przekieruje do createRaport.php, ktora to storna umożliwia utworzenie raportu, wybierając utwór z listy rozwijanej, z istnijących utworów w tabeli „utwory”.



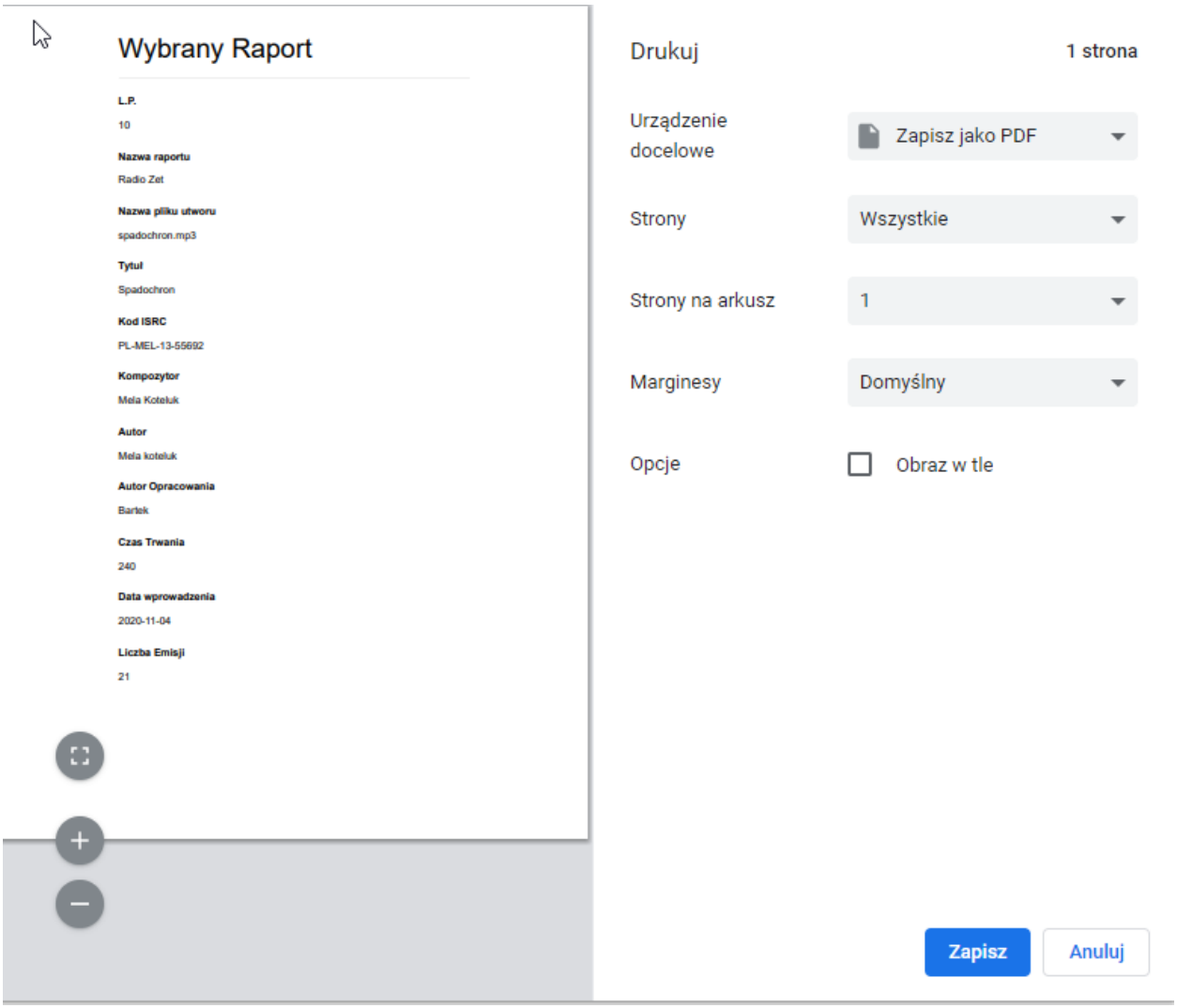

```
<div class="form-group">
    <label>Tytul Utworu</label>
    <select id ="id" name="id"  class="form-control"  >
    <?php
    $sql1 = "SELECT id, tytul FROM utwory";
    if($result1 = mysqli_query($link, $sql1)){
        while($row1 = mysqli_fetch_array($result1)){
            echo '<option value= "'.$row1["id"] .'" >'.$row1["tytul"].'</option>';
            }
    }
            ?>
    </select>
    </div>
```

Po kliknięciu w ikonę „Zobacz Raport” przekiruje do widoku raportu (readRaprot.php) gdzie można będzie wydrukować raport.





Po klinięciu „Drukuj raport” wyświetli się podgląd wydruku, bez Przycisków Wróć i Drukuj Raport:




```
<p><a href="raporty.php" class="btn btn-primary" id="back-btn">Wróć</a></p>
<button onclick="window.print();" class="btn btn-primary" id="print-btn">Drukuj raport!</button>
```

Odpowiada, za to print.css, który ukrywa Buttony:

print.css

```
/*Plik obsluguje wygląd wydruku, usuwa buttony z wydruku */
@page
{
  size:A4;
  margin: 0;
}
#print-btn
{
  display: none;
  visibility: none;
}
#back-btn
{
  display: none;
  visibility: none;
}
```

3.3 Przeglądarka zasobów

Moduł ten pozwala na przeglądanie zasobów: Utworów i Raportów, ale nie pozwala na ich edycje lub usunięcie. Jeydna dozwolna akcja do Wyświetl.

Jest to taka sama strona, do której ma dostęp użytkownik niezalogowany.

4 Wykorzystane technologie

MySQL 10.4.14-MariaDB
PHP Version: 7.4.10
HTML, CSS, Bootstrap