

Zajęcia 11

Wykorzystanie bazy danych MySQL w PHP cz. 1

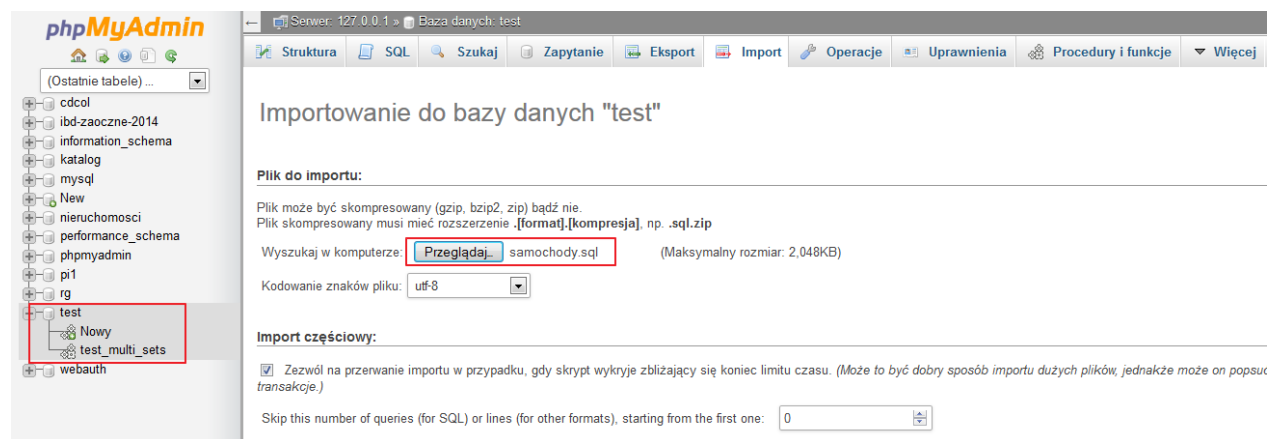
Cel zajęć

Na zajęciach zaprezentowana zostanie mini aplikacja służąca do zarządzania danymi zapisanymi w tabeli *samochody* w bazie danych MySQL.

Dostęp do aplikacji będzie możliwy po zalogowaniu się. Dane użytkowników przechowywane będą w tabeli *uzytkownicy* w bazie danych.

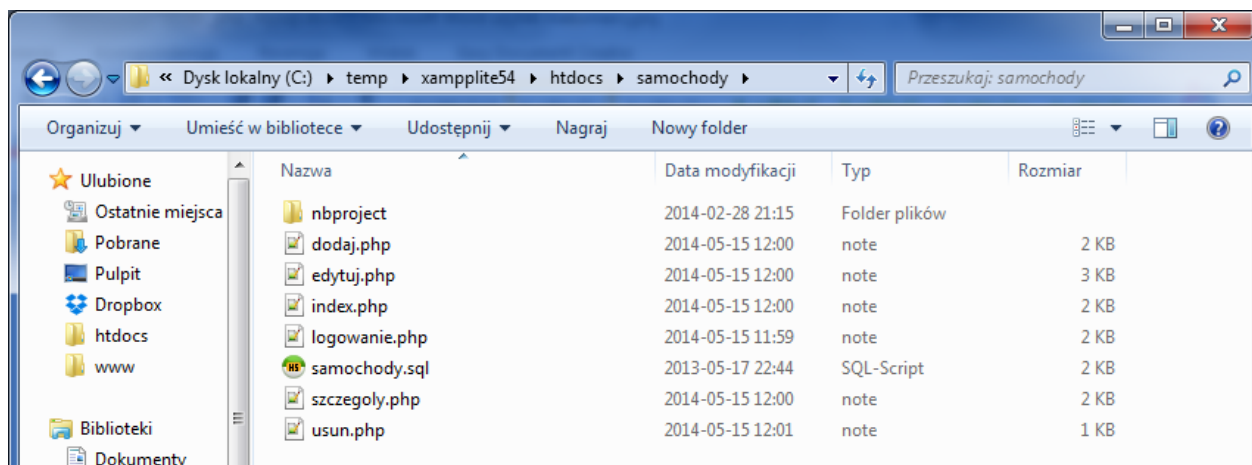
Import struktury bazy danych

Do poprawnego działania aplikacji wymaga dwóch tabel w bazie danych (*samochody* i *uzytkownicy*). Kod tworzący te tabele oraz wstawiający do nich przykładowe dane został umieszczony w skrypcie **samochody.sql**, który należy zaimportować przy pomocy narzędzia **phpMyAdmin** do bazy danych **test**.



Kod aplikacji

Pliki zawierające kod aplikacji zostały udostępnione w UBI i należy je rozpakować do katalogu *htdocs* w folderze *xampp*



Logowanie do systemu

Po otwarciu w przeglądarce aplikacji (<http://localhost/samochody>) użytkownik zostanie przekierowany do ekranu logowania:



Kod obsługujący logowanie sprawdza (po wciśnięciu przycisku *Zaloguj*), czy w tabeli użytkownicy znajduje się rekord zawierający podany login i hasło. Jeśli uda się go znaleźć, do sesji wstawiana jest informacja o zalogowaniu, a następnie użytkownik jest przekierowany do strony *index.php*, która wyświetla listę samochodów.

Do połączenia się z bazą danych wykorzystywana jest biblioteka PDO, której konstruktor jako parametr przyjmuje string definiujący sterownik bazy danych, adres serwera, nazwę bazy danych, login i hasło użytkownika.

Po utworzeniu połączenia do bazy danych zostaje przygotowany obiekt Statement z treścią zapytania SQL i oznaczonymi parametrami login i hasło.

Ostatnim krokiem jest wywołanie zapytania z parametrami pobranymi z formularza wypełnionego przez użytkownika oraz pobranie tablicy asocjacyjnej z danymi.

Kod wygląda następująco:

```
<?php

session_start();

if (isset($_POST['zaloguj'])) {
    $pdo = new PDO('mysql:host=localhost;dbname=test', 'root', '');

    $stmt = $pdo->prepare("SELECT * FROM uzytkownicy WHERE login = :login AND haslo = :haslo");
    $stmt->execute(['login' => $_POST['login'], 'haslo' => $_POST['haslo']]);
    $wynik = $stmt->fetch();

    if ($wynik) {
        $_SESSION['zalogowany'] = 'tak';
        $_SESSION['id'] = $wynik['id'];
        header("Location: index.php");
    } else {
        $komunikat = "Wprowadzono zły login lub hasło.";
    }
}

?>

<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <meta http-equiv="X-UA-Compatible" content="ie=edge">
    <title>Logowanie</title>
</head>
<body>
    <?php if (!empty($komunikat)): ?>
        <p style="font-weight: bold; color: red;"><?=$komunikat ?></p>
    <?php endif; ?>

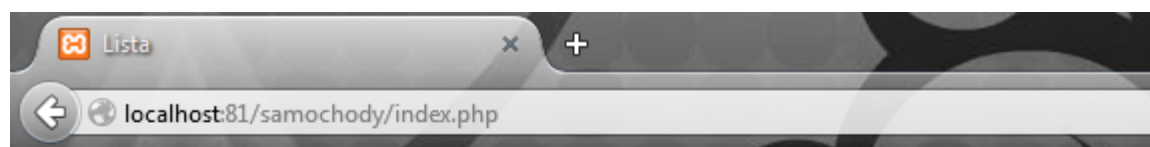
    <form method="post" action="">
        <table>
```

```
<tr>
  <td>Login</td>
  <td><input type="text" name="login" /></td>
</tr>
<tr>
  <td>Hasło</td>
  <td><input type="password" name="haslo" /></td>
</tr>
<tr>
  <td colspan="2"><input type="submit" name="zaloguj" value="Zaloguj" /></td>
</tr>
</table>
</form>
</body>
</html>
```

W zaimportowanej bazie danych znajduje się jeden użytkownik o loginie **test** oraz hasło **test**. Można użyć tych danych do zalogowania się do systemu.

Lista samochodów

Plik *index.php* odpowiada za wyświetlenie listy samochodów. Dane pobierane są z bazy danych przy pomocy zapytania SQL *SELECT*, a następnie przetwarzane w pętli (buforowane w tablicy *\$dane*). Po tej operacji tworzona jest pętla *foreach*, której zadaniem jest wyświetlenie danych samochodów w tabeli HTML.



[\[Dodaj samochod \]](#)

Marka	Model	Rok	Operacje
Fiat	Punto	1995	szczegóły edytuj usuń
Mazda	626	1997	szczegóły edytuj usuń
Skoda	Fabia	2000	szczegóły edytuj usuń
Volkswagen	Passat	2002	szczegóły edytuj usuń

Kod podstrony:

```
<?php

session_start();

if (empty($_SESSION['zalogowany'])) {
    header("Location: logowanie.php");
    exit();
}

$dane = [];
$pdo = new PDO('mysql:host=localhost;dbname=test', 'root', '');
foreach ($pdo->query('SELECT * FROM samochody ORDER BY marka, model') as $wiersz) {
    $dane[] = $wiersz;
}
?>

<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <meta http-equiv="X-UA-Compatible" content="ie=edge">
    <title>Lista</title>
</head>
<body>
    <?php if(isset($_GET['komunikat'])): ?>
        <p style='color:red; font-weight:bold;'>
            <?php if($_GET['komunikat'] == 1): ?>
                Samochod zostal dodany.
            <?php elseif($_GET['komunikat'] == 2): ?>
                Samochod zostal usuniety.
            <?php endif; ?>
        </p>
    <?php endif; ?>

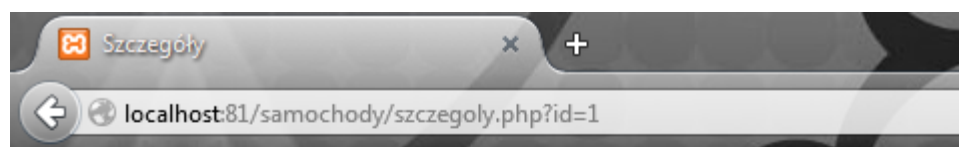
    <p>
        <a href="dodaj.php">[ Dodaj samochod ]</a>
    </p>
</body>
</html>
```

```
</p>
<table>
  <tr>
    <th>Marka</th>
    <th>Model</th>
    <th>Rok</th>
    <th>Operacje</th>
  </tr>

  <?php foreach($dane as $d): ?>
    <tr>
      <td><?=$d['marka'] ?></td>
      <td><?=$d['model'] ?></td>
      <td><?=$d['rok'] ?></td>
      <td>
        <a href="szczegoly.php?id=<?=$d['id'] ?>">szczegóły</a>
        <a href="edytuj.php?id=<?=$d['id'] ?>">edytuj</a>
        <a href="usun.php?id=<?=$d['id'] ?>">usuń</a>
      </td>
    </tr>
  <?php endforeach; ?>
</table>
</body>
</html>
```

Szczegóły samochodu

W ramach podstrony *szczegoly.php* wyświetlane są dane pojedynczego rekordu. Kluczem do wykonania tej operacji jest pobranie jednego rekordu z bazy danych (o ID podanych w linku – parametr `$_GET['id']`).



Marka	Fiat
Model	Punto
Rok	1995
Pojemność	1.2
Typ silnika	benzyna
Liczba poduszek	0
ABS	nie
ESP	nie

[\[Powrót do listy \]](#)

Kod podstrony:

```
<?php

session_start();

if (empty($_SESSION['zalogowany'])) {
    header("Location: logowanie.php");
    exit();
}

if (isset($_GET['id'])) {
    $pdo = new PDO('mysql:host=localhost;dbname=test', 'root', '');

    $stmt = $pdo->prepare("SELECT * FROM samochody WHERE id = :id");
    $stmt->execute(['id' => $_GET['id']]);
    $wiersz = $stmt->fetch();

    if (!$wiersz) {
        die("Nie znaleziono podanego samochodu!");
    }
} else {
    die("Nie podano parametru!");
}
?>

<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <meta http-equiv="X-UA-Compatible" content="ie=edge">
    <title>Szczegóły</title>
</head>
<body>
    <table>
        <tr>
            <td>Marka</td>
            <td><?=$wiersz['marka'] ?></td>
```

```
</tr>
<tr>
  <td>Model</td>
  <td><?=$wiersz['model'] ?></td>
</tr>
<tr>
  <td>Rok</td>
  <td><?=$wiersz['rok'] ?></td>
</tr>
<tr>
  <td>Pojemność</td>
  <td><?=$wiersz['pojemnosc'] ?></td>
</tr>
<tr>
  <td>Typ silnika</td>
  <td><?=$wiersz['typ_silnika'] ?></td>
</tr>
<tr>
  <td>Liczba poduszek</td>
  <td><?=$wiersz['liczba_poduszek'] ?></td>
</tr>
<tr>
  <td>ABS</td>
  <td><?=$wiersz['abs'] ?></td>
</tr>
<tr>
  <td>ESP</td>
  <td><?=$wiersz['esp'] ?></td>
</tr>
</table>

<p>
  <a href="index.php">[ Powrót do listy ]</a>
</p>
</body>
</html>
```

Zadania

1. Proszę o dodanie do formularza logowania automatycznego blokowania konta po nieudanych 3 próbach logowania (metoda dowolna).
2. Proszę o zahaszowanie hasła użytkownika w bazie danych przy pomocy algorytmu bcrypt.
 - a. Do haszowania służy funkcja `password_hash()`
<https://www.php.net/manual/en/function.password-hash.php>
 - b. Do weryfikacji poprawności wprowadzonego hasła należy wykorzystać funkcję `password_verify()`
<https://www.php.net/manual/en/function.password-verify.php>