

ZADANIE PRAKTYCZNE 1 — KWALIFIKACJA INF.03

Aplikacja internetowa „Wypożyczalnia Samochodów”

Baza danych MySQL, skrypty PHP, dokumenty HTML i styl CSS

Wykonaj aplikację internetową do ewidencji samochodów wypożyczalni. Aplikacja wykorzystuje gotową bazę danych MySQL wypożyczalnia_samochodow, składa się z czterech podstron połączonych wspólnym menu i jednego arkusza stylów. Wygląd podstron przedstawiono na Rysunkach 1–4.

Pliki do przygotowania

zapytania.sql, formularz.php, pokaz.php, szukaj.php, wynik.php, styl.css, a w punkcie 4 (jeśli wykonałeś skrypty metodą niebezpieczną): formularz2.php, pokaz2.php, szukaj2.php, wynik2.php. Wszystkie pliki zapisz w jednym folderze w katalogu serwera WWW (np.htdocs).

1. Operacje na bazie danych

Uruchom serwer Apache i MySQL. W narzędziu phpMyAdmin zaimportuj plik 1_wypożyczalnia_samochodow.sql (zakładka Import). Skrypt sam utworzy bazę wypożyczalnia_samochodow z tabelami: Miasta, Klient, Samochod, Wypożyczenia i wypełni je danymi. Struktura bazy:

Tabela	Pola (PK – klucz główny, → klucz obcy)
Klient	ID_klient (PK), imie (varchar(50)), nazwisko (varchar(50)), telefon (varchar(20)), e_mail (varchar(100)), ID_miasta → Miasta.ID_miasta
Miasta	ID_miasta (PK), nazwa (varchar(50))
Samochod	ID_samochodu (PK), marka (varchar(50)), rok_produkcji (int), kraj_produkcji (varchar(50))
Wypożyczenia	ID_wypożyczenia (PK), ID_samochodu → Samochod.ID_samochodu, ID_klienta → Klient.ID_klient, data_wypożyczenia (date), miejsce_start (varchar(50)), miejsce_stop (varchar(50)), data_oddania (date)

Zaprojektuj zapytania SQL, które zostaną wykorzystane w skryptach PHP. Wszystkie zapytania zapisz w pliku zapytania.sql (w zapytaniach, które korzystają z danych od użytkownika, użyj przykładowych wartości):

Zapytanie 1: wstawia do tabeli Samochod nowy rekord z danymi przesłanymi z formularza (marka, rok produkcji, kraj produkcji). Pole ID_samochodu jest nadawane automatycznie.

Zapytanie 2: wybiera wszystkie pola wszystkich rekordów tabeli Samochod.

Zapytanie 3: oblicza najmniejszą, największą i średnią wartość kolumny rok_produkcji.

Zapytanie 4: wybiera kraje produkcji oraz liczbę samochodów z każdego kraju (grupowanie według kraju produkcji).

Zapytanie 5: wybiera markę samochodu oraz datę wypożyczenia, miejsce startu i miejsce zakończenia wszystkich wypożyczeń samochodów, których marka zawiera podany przez użytkownika fragment tekstu. Zapytanie łączy tabele Samochod i Wypożyczenia relacją; wyniki są posortowane rosnąco według daty wypożyczenia.

2. Witryna internetowa

Skrypty z tego punktu możesz wykonać najprostszą metodą — tak jak w zadaniu o przychodni (zmienne wklejone bezpośrednio do treści zapytania SQL, wynik wypisany przez echo). Zabezpieczenie aplikacji wykonasz w punkcie 4.

2.1. Elementy wspólne wszystkich podstron

Wszystkie podstrony mają jednakowy układ bloków: blok nagłówka, pod nim blok boczny (menu, po lewej) i blok główny (po prawej), a na dole stopka. Blok boczny występuje w kodzie HTML przed blokiem głównym.

- Język dokumentu: polski, kodowanie UTF-8, tytuł strony (widoczny na karcie przeglądarki) zależny od podstrony, np. „Wypożyczalnia Samochodów – Dodaj samochód”.
- Arkusz stylów `styl.css` jest dołączony do każdej podstrony.
- Blok nagłówka (`<header>`): nagłówek pierwszego stopnia o treści „Wypożyczalnia Samochodów”.
- Blok boczny (`<aside>`): element `<nav>` z listą punktowaną zawierającą trzy odnośniki: „Dodaj samochód”, „Pokaż samochody”, „Szukaj wypożyczeń”, prowadzące kolejno do plików `formularz.php`, `pokaz.php`, `szukaj.php`.
- Blok główny (`<main>`): treść właściwa dla danej podstrony (opisana niżej).
- Stopka (`<footer>`): akapit o treści „© 2026 Wypożyczalnia Samochodów.”, a po nim numer zdającego.

2.2. Podstrona „Dodaj samochód” (`formularz.php`)

Rysunek 1. Podstrona „Dodaj samochód” po poprawnym dodaniu rekordu

W bloku głównym umieść nagłówek drugiego stopnia „Formularz dodawania samochodu”, a pod nim formularz wysyłany metodą POST do tego samego pliku. Formularz zawiera:

- pole tekstowe: Marka,
- pole numeryczne: Rok produkcji (wartość minimalna 1990),
- listę rozwijaną Kraj produkcji z opcjami: „-- wybierz --” (pusta wartość), „Japonia”, „Niemcy”, „Czechy”, „Francja”, „Korea Południowa”, „Włochy”,
- przyciski „Dodaj” (wysyła formularz) i „Reset” (czyści formularz).

Wszystkie pola są wymagane. Każde pole jest opisane etykietą.

Skrypt po naciśnięciu przycisku „Dodaj”:

1. łączy się z bazą danych,
2. odbiera dane z formularza,

3. sprawdza rok produkcji: jeżeli jest większy niż bieżący rok, rekord nie jest zapisywany, a nad formularzem wyświetla się komunikat „Rok produkcji nie może być z przyszłości”,
4. w przeciwnym wypadku wysyła Zapytanie 1 i nad formularzem wyświetla komunikat „Dodano samochód: <marka> (rok <rok produkcji>)”; gdy zapis się nie powiedzie – „Nie udało się wstawić danych.”,
5. zamyka połączenie z bazą danych.

2.3. Podstrona „Pokaż samochody” (pokaz.php)

Dodaj samochód
Pokaż samochody
Szukaj wypożyczeń

Lista samochodów

ID	Marka	Rok produkcji	Kraj produkcji
1	Toyota	2020	Japonia
2	Toyota	2019	Japonia
3	Volkswagen	2021	Niemcy
4	Volkswagen	2018	Niemcy
5	Skoda	2020	Czechy
6	Skoda	2017	Czechy
7	Ford	2019	Niemcy
8	BMW	2022	Niemcy
9	Audi	2021	Niemcy
10	Opel	2018	Niemcy
11	Renault	2019	Francja
12	Peugeot	2020	Francja
13	Kia	2021	Korea Południowa
14	Hyundai	2019	Korea Południowa
15	Mazda	2022	Japonia
16	Honda	2021	Japonia
17	Nissan	2020	Japonia

Najstarszy rocznik: 2017
Najnowszy rocznik: 2022
Średni rok produkcji: 2020

Liczba samochodów z każdego kraju:

- Czechy: 2 szt.
- Francja: 2 szt.
- Japonia: 5 szt.
- Korea Południowa: 2 szt.
- Niemcy: 6 szt.

© 2026 Wypożyczalnia Samochodów. Numer zdającego: 0000000000

Rysunek 2. Podstrona „Pokaż samochody”

W bloku głównym umieść nagłówek drugiego stopnia „Lista samochodów”. Skrypt:

1. wysyła Zapytanie 2 i wyświetla wszystkie rekordy w tabeli z nagłówkami kolumn: ID, Marka, Rok produkcji, Kraj produkcji; tabela ma obramowanie,
2. pod tabelą, na podstawie Zapytania 3, wyświetla w osobnych akapitach najstarszy rocznik, najnowszy rocznik i średni rok produkcji (zaokrąglony do liczby całkowitej), w formacie „Najstarszy rocznik: <wartość>”, „Najnowszy rocznik: <wartość>”, „Średni rok produkcji: <wartość>”,
3. pod nimi wyświetla nagłówek trzeciego stopnia „Liczba samochodów z każdego kraju:”, a pod nim, na podstawie Zapytania 4, listę punktowaną w formacie „<kraj produkcji>: <liczba> szt.”,
4. gdy tabela nie zawiera rekordów, zamiast tabeli i statystyk wyświetla akapit „Brak rekordów do wyświetlenia.”,

5. zamyka połączenie z bazą danych.

2.4. Podstrona „Szukaj wypożyczeń” (szukaj.php)

Rysunek 3. Podstrona „Szukaj wypożyczeń”

W bloku głównym umieścić nagłówek drugiego stopnia „Wyszukaj wypożyczenia samochodu”, a pod nim formularz wysyłany metodą GET do pliku wynik.php. Formularz zawiera wymagane pole tekstowe o nazwie marka z etykietą „Podaj markę:” oraz przycisk „Szukaj”. Użytkownik może wpisać pełną nazwę lub jej fragment.

2.5. Podstrona wyników wyszukiwania (wynik.php)

Rysunek 4. Wyniki wyszukiwania dla frazy „toy”

Skrypt odbiera wpisaną frazę, wysyła Zapytanie 5 i wyświetla w bloku głównym:

- nagłówek drugiego stopnia „Wypożyczenia samochodów marki: "<frazą>"",
- akapit „Liczba wypożyczeń: <liczba>",
- listę punktowaną znalezionych rekordów w formacie „<marka> — <data wypożyczenia>: <miejsce startu> → <miejsce zakończenia>”; gdy nic nie znaleziono – akapit „Brak wypożyczeń dla podanej marki.”,
- odnośnik „Wróć do wyszukiwania” prowadzący do pliku szukaj.php.

3. Styl CSS witryny internetowej

Plik styl.css powinien zawierać formatowanie:

- Dla wszystkich elementów strony (selektor uniwersalny): marginesy zewnętrzne i wewnętrzne równe 0, szerokość i wysokość elementu obejmują jego marginesy wewnętrzne i obramowanie.

- Dla całej strony: krój czcionki Arial, w drugiej kolejności Helvetica, w ostateczności dowolny krój bezszeryfowy.
- Dla bloku nagłówka: kolor tła #1565C0, kolor czcionki biały, marginesy wewnętrzne 20 px.
- Dla bloku bocznego: pływający, przyległy do lewej strony okna, szerokość 200 px, kolor tła #F2F2F2.
- Dla bloku głównego: margines zewnętrzny lewy 200 px, marginesy wewnętrzne 20 px, kolor tła biały.
- Dla stopki: nie dopuszcza elementów pływających z żadnej strony, kolor tła #333333, kolor czcionki biały, tekst wyśrodkowany, marginesy wewnętrzne 10 px.
- Dla listy w menu bloku bocznego: brak punktów.
- Dla elementów listy menu: marginesy wewnętrzne 10 px.
- Dla odnośników w menu: bez podkreślenia (brak dekoracji tekstu), kolor czcionki #333333.
- Dla tabeli: obramowanie komórek połączone w pojedynczą linię, margines zewnętrzny górny 15 px.
- Dla komórek tabeli i komórek nagłówka tabeli: marginesy wewnętrzne górny i dolny 6 px, lewy i prawy 10 px.
- Dla komórek nagłówka tabeli: kolor tła #BBDEFB.
- Dla etykiet formularza: wyświetlane jako elementy liniowo-blokowe, szerokość 130 px, margines zewnętrzny górny 8 px.
- Właściwości elementów, których nie wymieniono w treści, powinny mieć wartości domyślne.

4. Wersja bezpieczna — pliki z końcówką 2

Jeżeli skrypty z punktu 2 wykonałeś metodą niebezpieczną (zmienne z formularza wklejone bezpośrednio do treści zapytania SQL, dane wypisywane na stronie bez zabezpieczenia), utwórz kopie tych plików i nadaj im nazwy z końcówką 2:

Plik metodą niebezpieczną	Kopia rozwiązana metodą bezpieczną
formularz.php	formularz2.php
pokaz.php	pokaz2.php
szukaj.php	szukaj2.php
wynik.php	wynik2.php

Pliki z końcówką 2 rozwiąż metodą bezpieczną. Ich wygląd i działanie mają być takie same jak w punkcie 2, a dodatkowo:

- odnośniki w menu plików z końcówką 2 prowadzą do plików formularz2.php, pokaz2.php i szukaj2.php; formularz w szukaj2.php jest wysyłany do wynik2.php, a odnośnik „Wróć do wyszukiwania” prowadzi do szukaj2.php; pliki styl.css i zapytania.sql pozostają wspólne,
- po połączeniu z bazą ustaw kodowanie znaków na utf8mb4 (funkcja `mysqli_set_charset()`),
- Zapytanie 1 (dane z formularza) i Zapytanie 5 (frazę wyszukiwania) wykonaj jako **zapytania przygotowane**: w treści zapytania w miejscu danych wstaw znaki `?`, a dane przekaz funkcjami `mysqli_prepare()`, `mysqli_stmt_bind_param()`, `mysqli_stmt_execute()` (wynik zapytania `SELECT` pobierz funkcją `mysqli_stmt_get_result()`; znaki `%` dla operatora `LIKE` dołącz do zmiennej, a nie do treści zapytania,
- wszystkie dane pochodzące od użytkownika lub z bazy, wypisywane na stronie (komunikat, fraza, zawartość tabeli i list), przepuść przez funkcję `htmlspecialchars()`.

Sprawdź różnicę. Wykonaj te same próby w obu wersjach aplikacji i porównaj wyniki:

- w wyszukiwarce wpisz ' OR '1'='1 — ile rekordów pokazuje wynik.php, a ile wynik2.php?
- w wyszukiwarce wpisz XSS — jak wygląda nagłówek z frazą w obu wersjach?
- w formularzu w polu „Marka” wpisz tekst z apostrofem, np. D'Arcy — w której wersji rekord zostanie zapisany?

```
-- =====
```

```
-- Baza danych: wypożyczalnia_samochodow
```

```
-- =====
```

```
DROP DATABASE IF EXISTS wypożyczalnia_samochodow;
```

```
CREATE DATABASE wypożyczalnia_samochodow CHARACTER SET utf8mb4;
```

```
USE wypożyczalnia_samochodow;
```

```
CREATE TABLE Miasta (
```

```
    ID_miasta INT PRIMARY KEY AUTO_INCREMENT,
```

```
    nazwa VARCHAR(50) NOT NULL
```

```
);
```

```
CREATE TABLE Klient (
```

```
    ID_klient INT PRIMARY KEY AUTO_INCREMENT,
```

```
    imie VARCHAR(50) NOT NULL,
```

```
    nazwisko VARCHAR(50) NOT NULL,
```

```
    telefon VARCHAR(20),
```

```
    e_mail VARCHAR(100),
```

```
    ID_miasta INT,
```

```
    FOREIGN KEY (ID_miasta) REFERENCES Miasta(ID_miasta)
```

```
);
```

```
CREATE TABLE Samochod (
```

```
    ID_samochodu INT PRIMARY KEY AUTO_INCREMENT,
```

```
    marka VARCHAR(50) NOT NULL,
```

```
    rok_produkcji INT NOT NULL,
```

```
    kraj_produkcji VARCHAR(50) NOT NULL
```

```
);
```

```
CREATE TABLE Wypozyczenia (
```

```
    ID_wypozyczenia INT PRIMARY KEY AUTO_INCREMENT,
```

```
    ID_samochodu INT NOT NULL,
```

```
ID_klienta INT NOT NULL,  
data_wypożyczenia DATE NOT NULL,  
miejsce_start VARCHAR(50),  
miejsce_stop VARCHAR(50),  
data_oddania DATE,  
FOREIGN KEY (ID_samochodu) REFERENCES Samochod(ID_samochodu),  
FOREIGN KEY (ID_klienta) REFERENCES Klient(ID_klient)  
);
```

```
INSERT INTO Miasta (nazwa) VALUES
```

```
('Warszawa'),  
('Kraków'),  
('Katowice'),  
('Kielce'),  
('Wrocław'),  
('Poznań'),  
('Gdańsk'),  
('Łódź'),  
('Szczecin'),  
('Koszalin');
```

```
INSERT INTO Klient (imie, nazwisko, telefon, e_mail, ID_miasta) VALUES
```

```
('Anna','Kowalski','685822412','anna.kowalski@example.com',2),  
('Piotr','Nowak','603356886','piotr.nowak@example.com',5),  
('Katarzyna','Wiśniewski','632868828','katarzyna.wiśniewski@example.com',4),  
('Marek','Wójcik','618728463','marek.wojcik@example.com',2),  
('Ewa','Kowalczyk','690825067','ewa.kowalczyk@example.com',9),  
('Tomasz','Kamiński','611668732','tomasz.kamiński@example.com',10),  
('Magdalena','Lewandowski','656629388','magdalena.lewandowski@example.com',1),  
('Krzysztof','Zieliński','603999315','krzysztof.zieliński@example.com',2),  
('Agnieszka','Szymański','629345092','agnieszka.szymański@example.com',4),  
('Michał','Woźniak','667827638','michał.woźniak@example.com',10),  
('Joanna','Dąbrowski','603561597','joanna.dąbrowski@example.com',9),  
('Paweł','Kozłowski','626687537','paweł.kozłowski@example.com',9),  
('Monika','Jankowski','656306997','monika.jankowski@example.com',4),
```

```
('Grzegorz','Mazur','660291817','grzegorz.mazur@example.com',10),
('Natalia','Kwiatkowski','637338124','natalia.kwiatkowski@example.com',1),
('Andrzej','Krawczyk','621429110','andrzej.krawczyk@example.com',7),
('Aleksandra','Piotrowski','645667651','aleksandra.piotrowski@example.com',5),
('Rafał','Grabowski','620868105','rafał.grabowski@example.com',4),
('Karolina','Nowicki','645176955','karolina.nowicki@example.com',2),
('Dariusz','Pawłowski','612448136','dariusz.pawłowski@example.com',7);
```

```
INSERT INTO Samochod (marka, rok_produkcji, kraj_produkcji) VALUES
```

```
('Toyota',2020,'Japonia'),
('Toyota',2019,'Japonia'),
('Volkswagen',2021,'Niemcy'),
('Volkswagen',2018,'Niemcy'),
('Skoda',2020,'Czechy'),
('Skoda',2017,'Czechy'),
('Ford',2019,'Niemcy'),
('BMW',2022,'Niemcy'),
('Audi',2021,'Niemcy'),
('Opel',2018,'Niemcy'),
('Renault',2019,'Francja'),
('Peugeot',2020,'Francja'),
('Kia',2021,'Korea Południowa'),
('Hyundai',2019,'Korea Południowa'),
('Mazda',2022,'Japonia'),
('Honda',2021,'Japonia'),
('Nissan',2020,'Japonia');
```

```
INSERT INTO Wypozyczenia (ID_samochodu, ID_klienta, data_wypozyczenia, miejsce_start, miejsce_stop,
data_oddania) VALUES
```

```
(1,1,'2024-01-05','Warszawa','Kraków','2024-01-08'),
(2,1,'2024-02-10','Kraków','Warszawa','2024-02-12'),
(3,1,'2024-03-01','Warszawa','Wrocław','2024-03-05'),
(1,1,'2024-04-15','Poznań','Warszawa','2024-04-18'),
(5,1,'2024-05-20','Gdańsk','Gdańsk','2024-05-22'),
(2,2,'2024-01-10','Katowice','Katowice','2024-01-12'),
```

(4,2,'2024-02-14','Wrocław','Poznań','2024-02-16'),
(2,2,'2024-03-20','Kraków','Kielce','2024-03-23'),
(6,2,'2024-06-01','Łódź','Warszawa','2024-06-03'),
(7,3,'2024-01-18','Warszawa','Szczecin','2024-01-20'),
(1,3,'2024-02-25','Kraków','Warszawa','2024-02-27'),
(3,3,'2024-04-02','Poznań','Wrocław','2024-04-05'),
(8,3,'2024-05-10','Warszawa','Warszawa','2024-05-11'),
(1,4,'2024-01-22','Warszawa','Kraków','2024-01-24'),
(2,5,'2024-02-02','Kraków','Katowice','2024-02-04'),
(3,6,'2024-02-18','Kielce','Warszawa','2024-02-20'),
(4,7,'2024-03-05','Wrocław','Poznań','2024-03-07'),
(5,8,'2024-03-15','Poznań','Gdańsk','2024-03-18'),
(6,9,'2024-03-28','Gdańsk','Łódź','2024-03-30'),
(7,10,'2024-04-08','Łódź','Szczecin','2024-04-10'),
(8,11,'2024-04-20','Szczecin','Koszalin','2024-04-22'),
(9,12,'2024-05-02','Koszalin','Warszawa','2024-05-04'),
(10,13,'2024-05-14','Warszawa','Wrocław','2024-05-16'),
(11,14,'2024-05-28','Kraków','Kielce','2024-05-30'),
(12,15,'2024-06-08','Katowice','Kraków','2024-06-10'),
(13,16,'2024-06-18','Poznań','Warszawa','2024-06-20'),
(14,17,'2024-07-01','Gdańsk','Gdańsk','2024-07-03'),
(1,18,'2024-07-12','Wrocław','Wrocław','2024-07-14'),
(2,19,'2024-07-25','Łódź','Warszawa','2024-07-27'),
(3,20,'2024-08-05','Szczecin','Poznań','2024-08-07');