Konspekt projektu

Sklep Motoryzacyjny aut Amerykańskich

**Przygotowują:**

Klaudia Winiarska – 241425  
Rafał Szymanek – 241436

Github: https://github.com/rafalszymanek/AmericanCarsDealership

Spis treści

[Projekt realizowany w ramach zajęć: 3](#_Toc23191003)

[Używane technologie 3](#_Toc23191004)

[Backend 3](#_Toc23191005)

[Frontend 3](#_Toc23191006)

[Baza danych 3](#_Toc23191007)

[Ogólny opis projektu 3](#_Toc23191008)

[Funkcjonalności: 3](#_Toc23191009)

[Opis do projektu Zarządzania infrastrukturą teleinformatyczną 4](#_Toc23191010)

[Zaimplementowane podatności 4](#_Toc23191011)

[Dodatkowe implementacje: 4](#_Toc23191012)

[Opis do projektu Bazy danych 5](#_Toc23191013)

[Przechowywane dane: 5](#_Toc23191014)

[Przykładowy podział bazy danych: 5](#_Toc23191015)

# Projekt realizowany w ramach zajęć:

* Projekt - Zarządzania infrastrukturą teleinformatyczną
* Projekt - Bazy danych

# Używane technologie

Backend  
PHP – Laravel ver. 5

## Frontend

HTML+CSS+JavaScript (Agular ver. 7\*)

\*W planie w ostatniej fazie projektu

## Baza danych

MySQL 8.0

# Ogólny opis projektu

Aplikacja będzie przedstawiała sklep motoryzacyjny specjalizujący się w sprzedaży samochodów amerykańskich. Zostanie ona również zainstalowana na fizycznym serwerze, który będzie wystawiony do Internetu w ramach prezentacji.

## Funkcjonalności:

* Przeglądanie samochodów (modeli)
* Wybór samochodu
* Dostosowywanie samochodów do własnych preferencji (?)
* Wyszukiwanie konkretnego modelu
* Składanie zamówień
* Komunikacja z sprzedawca klient (za pomocą komentarzy)
* Zakładanie konta
* Logowanie do aplikacji
* Podgląd realizacji zamówienia po stronie klienta
* Przegląd historii zamówień (i klient i pracownik)
* Podgląd realizacji zamówienia po stronie dealera
* Zmiany statusu zamówienia (pracownik)
* Finalizalizacja zamówienia
* Wywołanie przypadku płatności

# Opis do projektu Zarządzania infrastrukturą teleinformatyczną

**Temat:** 20 – Implementacja serwisu webowego podatnego na ataki OWASP Top Ten

W ramach projektu z kursu „Zarządzanie infrastrukturą teleinformatyczną” planujemy zaimplementować wybrane podatności z rankingu OWASP Top Ten.

## Zaimplementowane podatności

1. **Security misconfigurations** – pozostawienie podstawowych danych do logowania. Brak haszowania haseł.
2. **Sensitive data exposure** – Implementacja podatności Path Traversal, dzięki której atakujący będzie mógł zdobyć dane do logowania.
3. **XSS** – B formularza, który będzie zostawiał komentarz na stronie.
4. **Broken Authentication** – Brak implementacji systemu captcha oraz zliczania ilości prób logowania. System będzie podatny na atak Brute Force.
5. **SQL Injection** – Implementacja w formularzu logowania do serwisu. Atakujący będzie mógł wyciągnąć m.in. hasła z serwisu.

## Dodatkowe implementacje:

Podatności zostaną zaimplementowane w aplikacji webowej, jednakże zostaną również przygotowane gotowe „łatki” poprawiające bezpieczeństwo aplikacji. Dzięki temu nauczymy się nie tylko w jaki sposób mogą powstać dane zagrożenia, a także nauczymy się je naprawiać.

# Opis do projektu Bazy danych

**Temat:** Sklep Internetowy

W ramach projektu „Bazy danych” będzie tworzona strona Internetowa (sklep) opartej   
o relacyjną bazy danych w systemie MySQL.

## Przechowywane dane:

* Modele samochodów
* Użytkownicy
  + Klienci
  + Pracownicy
  + Administratorzy
* Zamówienia

## Przykładowy podział bazy danych:

