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
Używane technologie	
Backend	
Frontend	
Baza danych	3
Ogólny opis projektu	3
Funkcjonalności:	3
Opis do projektu Zarządzania infrastrukturą teleinformatyczną	4
Zaimplementowane podatności	4
Dodatkowe implementacje:	4
Opis do projektu Bazy danych	5
Przechowywane dane:	5
Przykładowy podział bazy danych:	5

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)
- Dostosowywanie samochodów do własnych preferencji (?)
- Wyszukiwanie konkretnego modelu
- Składanie zamówień
- Komunikacja z sprzedawca klient (za pomocą komentarzy)
- Logowanie do aplikacji
- Podgląd realizacji zamówienia po stronie klienta
- Podgląd realizacji zamówienia po stronie dealera
- Zmiany statusu zamówienia

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** Pozostawienie niezabezpieczonego 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

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

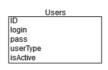
Przechowywane dane:

- Modele samochodów
- Użytkownicy
 - o Klienci
 - Pracownicy
 - Administratorzy
- Zamówienia

Przykładowy podział bazy danych:







Retailers

userID
userLogin
userPass
Name
Surname
OrderID

Clients
UserID
UserLogin
UserPass
ID
Name
Surname
Street
House No.
Post
City