Ochrona Danych - Projekt

Sprawozdanie

Janusz Sawicki 284933

23 stycznia 2019

1 Funkcjonalność aplikacji

Aplikacja składa się jedynie z modułu logowania, nie posiada rozbudowanej funkcjonalności po etapie uwierzytelnienia.

1.1 Rejestrowanie nowego użytkownika

Po wejściu na główną stronę klikamy opcję "Zarejestruj się".

W formularzu podajemy nazwę użytkownika, adres email oraz hasło (dwukrotnie). W czasie podawania hasła wyświetlana jest jego siła.

Po kliknięciu przycisku "Zarejestruj się" na podany adres email zostanie wysłana wiadomość zawierająca link aktywujący konto. Do czasu aktywowania konta zalogowanie nie bedzie możliwe.

1.2 Logowanie na konto

Na stronie głównej, w formularzu, podajemy nazwę użytkownika oraz hasło. Następnie wybieramy przycisk "Zaloguj się".

1.3 Zmiana hasła użytkownika

Po zalogowaniu się na konto klikamy przycisk "Zmień hasło"

W formularzu podajemy aktualne hasło oraz hasło jakie chcemy ustawić (dwukrotnie). Zatwierdzamy zmiany przyciskiem "Zatwierdź".

1.4 Odzyskiwanie hasła

W razie problemów z zalogowaniem na konto wybieramy opcję "Zapomniałem hasła"

Następnie w formularzu podajemy adres email powiązany z kontem na jakie chcemy się zalogować.

Po kliknięciu przycisku "Zatwierdź" na podany adres email zostanie wysłana wiadomość zawierająca link umożliwiający zmianę hasła.

Po otwarciu linku ukaże się nam fommularz w którym możemy podać nowe hasło (dwukrotnie).

Po zatwierdzeniu zmian hasło zostanie zmienione i będziemy mogli zalogować się używając nowego hasła.

2 Użyte zabezpieczenia

2.1 Walidacja danych wejściowych

W celu ułatwienia użytkownikowi wypełniania pól formularzy wszystkie dane wejściowe są walidowane po stronie widoku.

Po stronie serwerowej danymi walidowanymy są nazwa użytkownika oraz adres email (w każdym miejscu, gdzie istnieje możliwość ich podania). Dane te są walidowane metodą białej listy przy pomocy odpowiednich wyrażeń regularnych.

2.2 Ochrona przed SQL Injection

W przypadku tej aplikacji metodami ochrony sa wspomniana walidacja danych wejściowych oraz użycie mapowania obiektowo-relacyjnego w taki sposób, aby w żadnym miejscu w aplikacji nie były używane standardowe zapytania SQL.

2.3 Ochrona przed Cross-Site Scripting

W przypadku tej aplikacji jedynymi danymi kontrolowanymi przez użytkownika zwracanymi później na stronie HTML jest nazwa użytkownika. Metodami ochrony są więc walidacja danych wejściowych oraz dodatkowo kodowanie znaków specjalnych podczas ich zwracanie w treści strony.

Ponadto, dzięku użyciu flask session, ciasteczkom nadawana jest flaga HttpOnly, dzięki czemu nie jest możliwe wyświetlenie/przesłanie zawartości ciasteczek za pomocą wstrzykniętego kodu JavaScript.

2.4 Hashowanie haseł zapisywanyh w bazie

Przed zapisaniem w bazie, hasło jest hashowane za pomocą algorytmu SHA512 z użyciem PBKDF2 oraz HMAC oraz z użyciem soli.

2.5 Ochrona przed atakami czasowymi

W każdym fragmencie aplikacji, w którym hasło jest hashowane i zapisywane w bazie lub hashowane i porównywane z hasłem znajdującym się w bazie, dodana jest funkcja powodująca opóźnienie trwające losową liczbę milisekund (z przedziału [0,1000]).