Piotr Pogodziński, 284 953

Sprawozdanie

Ochrona Danych - Projekt

Szyfrowanie połączenia SSL

Połączenie klienta z serwerem jest szyfrowane za pomocą protokołu SSL. Został wygenerowany samopodpisany certyfikat. Do wersji produkcyjnej powinno się skorzystać z certyfikatu podpisanego przez odpowiednie organizacje aby uniknąć ostrzeżeń o wyjątkach bezpieczeństwa.

Przechowywanie haseł (hashowanie SHA256 + sól)

Dane użytkowników są przechowywane w bazie danych SQLite w dedykowanej tabeli. Nazwy użytkowników są dostępne w postaci niezaszyfrowanej a hasła są szyfrowane algorytmem SHA256 z dodaną solą.

Hasła są zapisane w postaci: *hash_hasła:sól*
Co pozwala przypisać do każdego hasła inną sól. W celu weryfikacji poprawności hasła, odpowiednia funkcja szyfruje hasło wprowadzone do formularza z użyciem soli porównywanego hasła a następnie są porównywane hashe. Jeśli są zgodnie, to wprowadzone hasło jest poprawne.

Mechanizm sesji

Użytkownik po zalogowaniu otrzymuje ciasteczko potwierdzające zalogowanie. Ciasteczko jest ważne do wyłączenia przeglądarki, bądź do wylogowania.

Mechanizm autoryzacji użytkownika

Po wprowadzeniu danych logowania serwer przeprowadza weryfikację użytkownika za pomocą ww. algorytmu. Następnie odczekuje 0.5s przed podaniem odpowiedzi, w celu wydłużenia ataków na hasło.

Widoczność notatek

Podczas wprowadzania notatki użytkownik może ustawić ją jako publiczną, udostępnić użytkownikowi lub pozostawić tylko dla siebie. Następnie serwer wprowadza notatkę do bazy danych wraz z informacją o tym, czy notatka jest publiczna. Jeśli notatka została udostępniona, to do osobnej tabeli zostaje wprowadzona informacja o użytkowniku upoważnionym do przeglądania notatki.