Bezpieczeństwo komputerowe

Laboratorium - lista nr 5 [C]

Zadanie 1 (100 pkt) Stwórz prototyp strony bankowej (do tego "projektu" będziemy odnosić się na kolejnych listach zadań). Strona ma posiadać następujące elementy (50 pkt):

- ekran zakładania konta (pola: login, email, hasło + weryfikacja hasła)
- ekran logowania (login/hasło),
- możliwość przypominania/resetowania hasła.

Musisz zadbać o bezpieczeństwo, postępuj zgodnie z `https://www.owasp.org/index.php/Input_Validation_Cheat_Sheet`. Dane dotyczące użytkowników przechowuj w SQL-owej bazie danych.

Część właściwa (50 pkt):

- strona z formularzem (możesz w tym celu skopiować formularz do przelewów wykorzystywany w Twoim banku),
- strona z potwierdzeniem danych – wyświetlająca dane wprowadzone w formularzu. Po akceptacji użytkownika, dane są przesyłane na serwer (i zapisywane w bazie danych).
- strona z potwierdzeniem wykonania przelewu – zawierająca dane, które otrzymał serwer.
- strona z historią potwierdzonych przelewów.

Dokonać "przelewu" może jedynie zalogowany użytkownik. Hasło użytkownika ma być przechowywane w sposób bezpieczny. Wykorzystaj wskazówki `https://www.owasp.org/index.php/Password_Storage_Cheat_Sheet`. Pamiętaj o wykorzystaniu Memory-Hard Functions (np. scrypt, ballon hashing, argon2i, catena).

Dane dotyczące przelewów mają być przehowywane w SQL-owej bazie danych.

Zadanie 2 (50 + 50 pkt) (50 pkt) Napisz kod w javascript, który będzie zmieniać działanie wyżej opisanego serwisu w ten sposób, że następuje podmienienie numeru konta na inny. Podmiana ma się dokonać jedynie w warstwie wizualnej tj.:

- serwer ma otrzymać podmieniony numer konta,
- strona ma zawsze wyświetlać wprowadzony numer konta.

Jakie są scenariusze, w których można przeprowadzić taki atak?

(50 pkt) Całość "zamień" w rozszerzenie do przeglądarki (Firefox/Chrome/...), które będzie wykonywać w/w czynności.