# Kryptografia i bezpieczeństwo

## Laboratorium - lista nr 4, 20 XI 2016

**Z tej listy można uzyskać 10 punktów.**

**Zadanie 1 (10 pkt)** Stwórz prototyp strony do wykonywania przelewów zawierający następujące elementy:

- ekran logowania (login/hasło).
- strona z formularzem (możesz w tym celu wykorzystać 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`

Następnie 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?

Całość "zamień" w rozszerzenie do przeglądarki, które będzie wykonywać w/w czynności.

**Zadanie 2 (10 pkt)** Zmodyfikuj kod klienta systemu Helios w taki sposób (możesz stworzyć odpowiednie rozszerzenie do przeglądarki), aby klient: postępował zgodnie z protokołem do momentu "kliknięcia" przycisku CAST. Po kliknięciu na ten przycisk ma zostać wygenerowany nowy głos, na innego kandydata niż wybrany przez głosującego.

Zaprezentuj działanie zmodyfikowanego klienta w praktyce `https://vote.heliosvoting.org/`.