Wstęp do bezpieczeństwa komputerowego

Lista P1 (10 IV)

Zadanie 1 (10 pkt) Wykonaj poniższe czynności.

1. Wygeneruj klucze ssh i powiąż je ze swoim kontem github/gitlab.
2. Zapoznaj się z metodami uwierzytelniania dwuskładnikowego, następnie wybierz jedną z metod i włącz 2FA dla swojego konta.
3. Wygeneruj klucze PGP dla konta Github (Gitlab); dodaj podpisany commit.

Zadanie 2 (10 + 10 pkt) (10 pkt) Wykorzystaj istniejący formularz (np. z systemu bankowości, z którego korzystasz), który w pierwszym kroku prosi o podanie danych przelewu, a w drugim wyświetla wprowadzone dane i prosi użytkownika o potwierdzenie.

Napisz kod javascript, który będzie zmieniać działanie formularza w ten sposób, że nastąpi podmienienie wprowadzonego 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?

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

Zadanie 3 (10+10 pkt) Zmodyfikuj działanie "serwisu" bankowego z zadania 2.

- (10) Wygeneruj dla serwera certyfikat TLS dla domeny: www.mojWspanialyBank.com – wykorzystaj w tym celu `https://letsencrypt.org/` (ale może to być inny adres, w szczególności może być konieczność skorzystania z usług typu "dynamic dns").
- (10) Spróbuj wygenerować certyfikat dla adresu prawdziwego banku. Co trzeba zrobić, aby to się udało (i jakie są z tego wnioski)? (podpowiedź: self signed).