Perceptus IT Security Academy
Zadanie praktyczne

1. Opis zagadnień poruszanych w zadaniu

- Frameworki,
- REST API | GraphQL | RMI & RPC,
- HSM,
- PKI,
- TDE,
- Szyfrowanie symetryczne, asymetryczne,
- Bazy danych SQL i NoSQL,
- Jira, Scrum, Agile, zarządzanie projektem,
- Testy automatyczne,
- Testy penetracyjne,
- Praca w zespole,
- Organizacja czasu,
- Prezentacja efektów.

2. Cel główny
Implementacja aplikacji webowej służącej do bezpiecznego przechowywania plików tzw. *Secure vault* z użyciem możliwości oferowanych przez HSM.

3. Cele szczegółowe
Frontend:
- panel logowania, składający się z:
    - formularza logowania, składającego się z:
        - pola login,
        - pola hasło,
        - przycisku **Zaloguj się**,
    - przycisku pomocy technicznej przekierowującego do panelu pomocy technicznej,
    - przycisku **Zapomniałeś hasła?**, umożliwiającego reset hasła,
    - formularz logowania musi być odporny na ataki typu brute-force,
- panel pomocy technicznej, składający się z:
    - formularza zgłoszeń, składającego się z:
        - pola imię,
        - pola nazwisko,
        - pola adres e-mail,
        - pola opis zgłoszenia,
        - przycisku wyślij zgłoszenie,
    - formularz musi być dostępny przed zalogowaniem (np. w przypadku gdy ktoś ma problem z dostępem do swojego konta),
    - formularz musi implementować mechanizmy antyspamowe,

- panel aktywacji konta:
    - widoczny po wejściu w link aktywacyjny wysłany po zaproszeniu przez administratora,
    - składa się z:
        - pola hasło,
        - pola powtórz hasło,
        - przycisku **Nadaj hasło**,
- panel resetowania hasła:
    - dostępny po naciśnięciu przycisku **Zapomniałeś hasła?**,
    - składa się z:
        - pola adres e-mail,
        - przycisku **Zresetuj hasło,**
    - po naciśnięciu przycisku resetowania hasła wysyła mail z linkiem resetującym na podany adres,
    - po wejściu w link w wiadomości e-mail przekierowuje do ekranu nadania nowego hasła,
- panel nadania nowego hasła:
    - dostępny po wejściu w link w wiadomości e-mail dot. resetowania hasła,
    - składa się z:
        - pola hasło,
        - pola powtórz hasło,
        - przycisku **Nadaj hasło**,
- panel administratora:
    - po zalogowaniu widoczny jest dashboard z:
        - przydatnymi wykresami, np. statystykami o zajętym miejscu, ilości użytkowników itp,
        - zakładkami,
        - przyciskiem do wylogowania,
        - przyciskiem przejścia do widoku ustawień,
    - zakładki:
        - zarządzanie użytkownikami:
            - prezentacja użytkowników i informacji o nich:
                - imienia,
                - nazwiska,
                - danych kontaktowych - adresu e-mail,
                - ilości zajętych danych vs. przydzielonych,
            - możliwość zapraszania nowych użytkowników,
            - możliwość edycji istniejących użytkowników,
            - możliwość przydzielania miejsca na dysku użytkownikom (np. w mb),
        - zarządzanie dyskiem:
            - zakładka do zarządzania ogólnymi ustawieniami:
                - dozwolone rozszerzenia na dysku,
                - maksymalny czas sesji użytkownika,
        - zarządzanie zgłoszeniami:
            - przeglądanie zgłoszeń,
            - dodawanie notatek o zgłoszeniu,
            - możliwość zamknięcia zgłoszenia,
    - możliwość wylogowania.

- panel użytkownika:
    - po zalogowaniu widoczna jest zakładka “moje pliki”,
    - na ekranie panelu muszą być widoczne następujące zakładki:
        - ulubione:
            - możliwość dodania plików do ulubionych, które pojawiają się na tej liście,
        - moje pliki:
            - lista plików wysłanych na dysk,
        - udostępnione:
            - lista plików udostępnionych przez innych użytkowników,
        - kosz:
            - lista plików usuniętych na ekranie moich plików,
            - zostają tutaj do momentu ręcznego lub automatycznego usunięcia,
            - czas automatycznego usunięcia definiowany w ustawieniach,
        - ustawienia:
            - 2fa,
            - zmiana hasła,
            - zmiana czasu, po którym usuwane są pliki,
    - widok zajętego miejsca,
    - lista plików w formacie: nazwa pliku, typ, właściciel, rozmiar, data wysłania,
    - każdy plik można pobrać, usunąć, skopiować, udostępnić (publicznie w formie linku, w obrębie organizacji - konkretnej osobie),
    - możliwość tworzenia i usuwania folderów,
    - możliwość pobierania i udostępniania folderów w całości jako zip,
    - możliwość wylogowania,

Backend:

- uwierzytelnianie i autoryzacja użytkowników,
- bezpieczne przechowywanie danych
- szyfrowanie danych z wykorzystaniem kluczy kryptograficznych (przechowywanych z wykorzystaniem HSM)
- wysyłanie maili
- 2fa z wykorzystaniem minimum kodu OTP na email i QR do TOTP (np. google authenticator)

4. Założenia

- Zespoły 2-6 osobowe
- Technologie: dowolne (zalecana Spring + React.js)
- Jeżeli zespół wpadnie na pomysł dodania czegoś od siebie musi to skonsultować i uzasadnić,
- Każdy zespół musi przynajmniej raz zaprezentować postęp prac na wzór wystąpienia weekly,
- Wyłącznie rozwiązania niekomercyjne (użycie bibliotek/szablonów jedynie z licencjami MIT, OpenSource i podobnych),
- Zapewnienie responsywności dla urządzeń mobilnych typu smartfon/tablet,
- Co zajęcia zespół powinien przesłać raport z przeprowadzonych prac - wraz z opisem i zrzutami ekranu - szablon raportu według uznania (do 5 stron).

Przewodnik-prawny-licencje.pdf