Для виконання завдання було обрано мову JavaScript і середовище виконня Node.js

Використані наступні бібліотеки і фреймворки

Express – web фреймворк

Jsonwebtoken – широко викоростовувана бібліотека для автентифікації і авторизаці

Mongoose – модуль для роботи з базою данних Mongoose

Cookie-parser – парсинг і відправка кукі

Joi – валідація вхідних запитів

Bcrypt, crypto - шифрування

Про технології

Jsonwebtoken або jwt- це стандартизований формат контейнера для безпечного кодування інформації, пов’язаної з користувачами та клієнтами (тоді як вміст файлів cookie та підписання / шифрування не стандартизовані)

Є два приватних ключі

Одним шифрується телефон користувача

Іншим підписується jwt-token

Завдання 1

Реєстрація

Встановлене обмеження на пароль мінімум 8 символів

Пароль шифрується за допомогою бібліотеки bcrypt і зберігається в базі данних

Логін

Після успішного входу користувачеві видається тимчасовий токен обмежений часом на 10 хвилин

Він записується в http-only cookie і не вразливий до інєкцій чи крадіжки

Профіль

Доступ до цієї сторінки є лише у авторизованих користувачів

Завдання 2

Сторінка Profile

Приватна сторінка доступ до якої можуть отримати лише авторизовані користувачі

Якщо користувач авторизований він може додати або змінити свій номер телефону

Також йому видно нікнейми і телефони інших користувачів

Телефони зберігаються в базі даних в зашифрованому вигляді тому в разі її крадіжки зловмисник не зможе отримати їх без ключа шифрування

таким способом також можна шифрувати інші дані

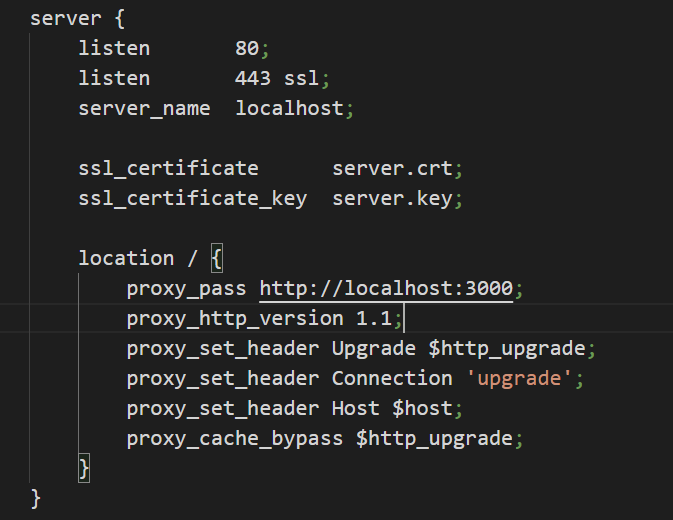
Телефони шифрується алгоритмом aes-256-cb з використанням приватного ключа

Завдання 3

Було вибрано nginx як reverse-proxy для додатка

Він прослуховує запити та перенаправляє їх на порт додатку

Конфігуровано наступним чином



Згенеровані самопідписані SSL сертифікати за допомогою утиліти OpenSSL

Наступною командою

**openssl req -x509 -newkey rsa:4096 -keyout key.pem -out cert.pem -days 365**

та було отримано два файли

