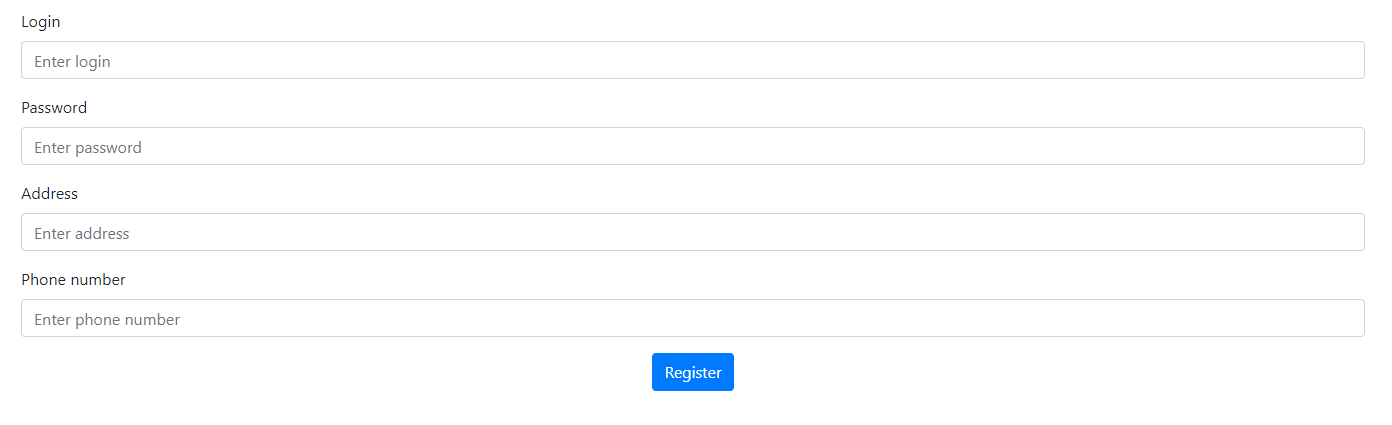
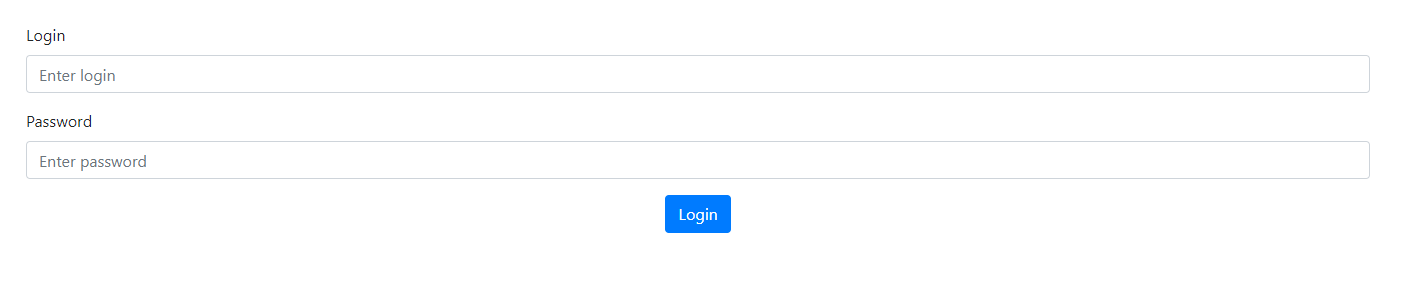
**ЗВІТ 5-6 ЛР**

На цих лабораторних ми розробили NodeJS + Express аплікуху, яка має 2 сторінки: реєстрація + логін та два відповідних ендпоінта (реєстрація + логін):

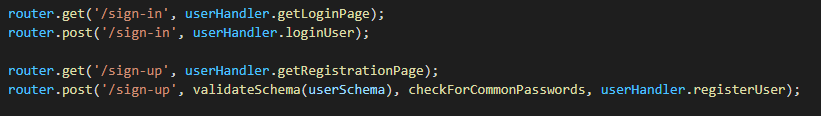


Реєстрація



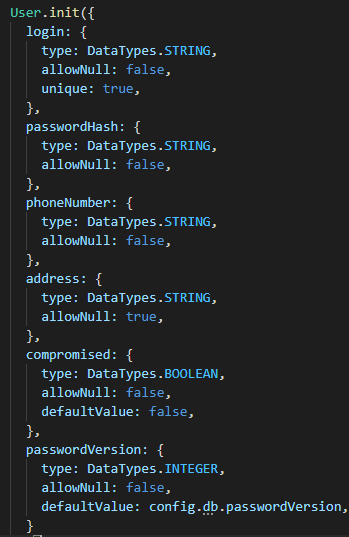
Логін

Просто банально зроблено 2 форми на двох сторінках з відповідними полями.

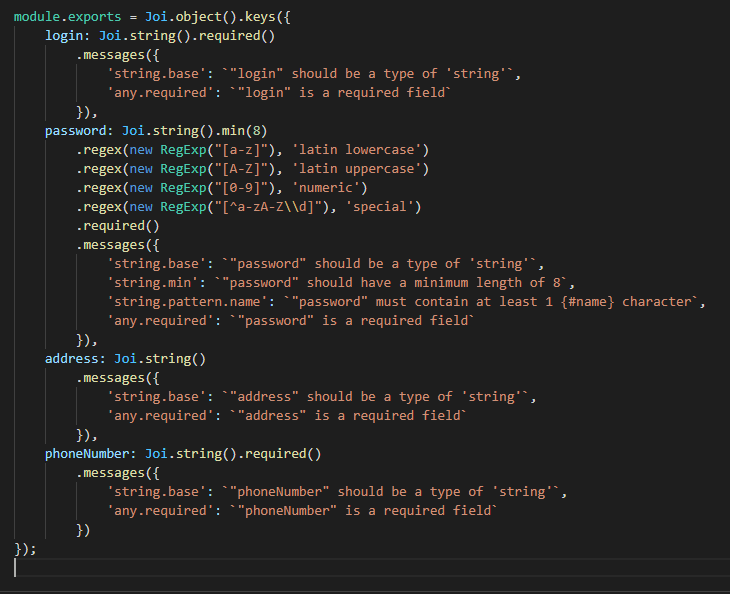


Роути

Також були добавлені поля для версії паролів та булеве поле compromised:



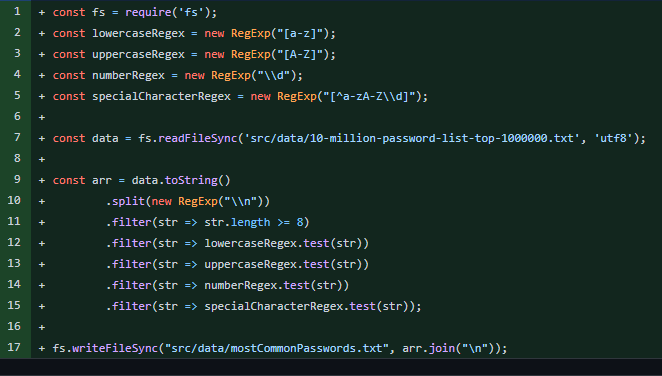
Добавлена валідація на сторінку реєстрації:



Валідація

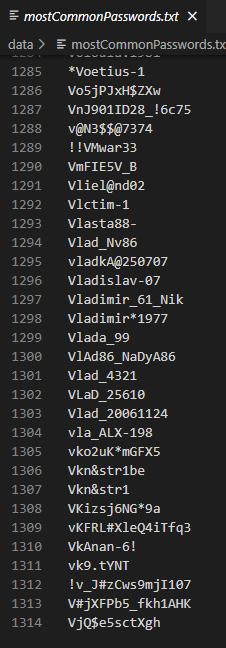
Валідація на пароль: 1 ловеркейс символ, 1 апперкейс символ, 1 цифра та один спец символ. Також мінімальна довжина 8 символів.

Також використовується ще одна перевірка для пароля: було взято 1,000,000 найпопулярніших паролів, відфільтровано по нашим вимогам до паролів:



Створення файлу найпопулярніших паролів

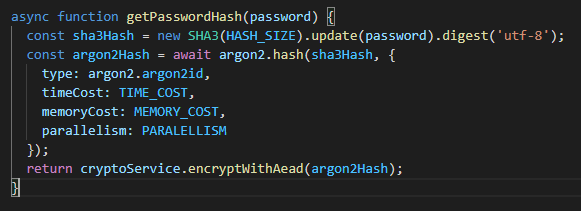
Вийшов файл з 1314 паролями:

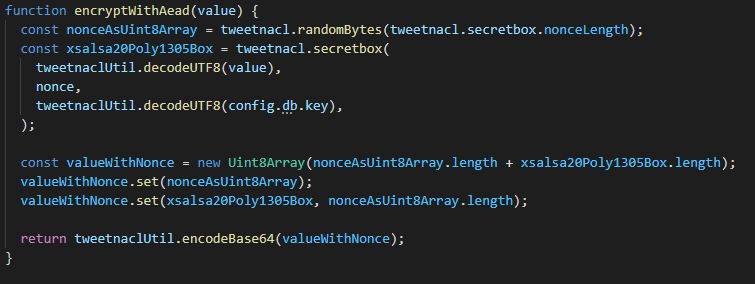


І добавлена перевірка, якщо введений пароль еквівалентний паролю з цього файла, то викидається помилка про те, що цей пароль не є надійним.



Для зберігання паролів була вибрана наступна схема: SHA3(512) -> argon2id -> XSalsa20-Poly1305.





Для аргон2 вибрані наступні опції (мінімальні по OWASP cheatsheets):



Також вразливі поля (address, phone) були зашифровані тією ж самою AEAD (XSalsa20-Poly1305). Ключ як і всі інші конфіги (дані про БД) були збережені на локальному файлі.