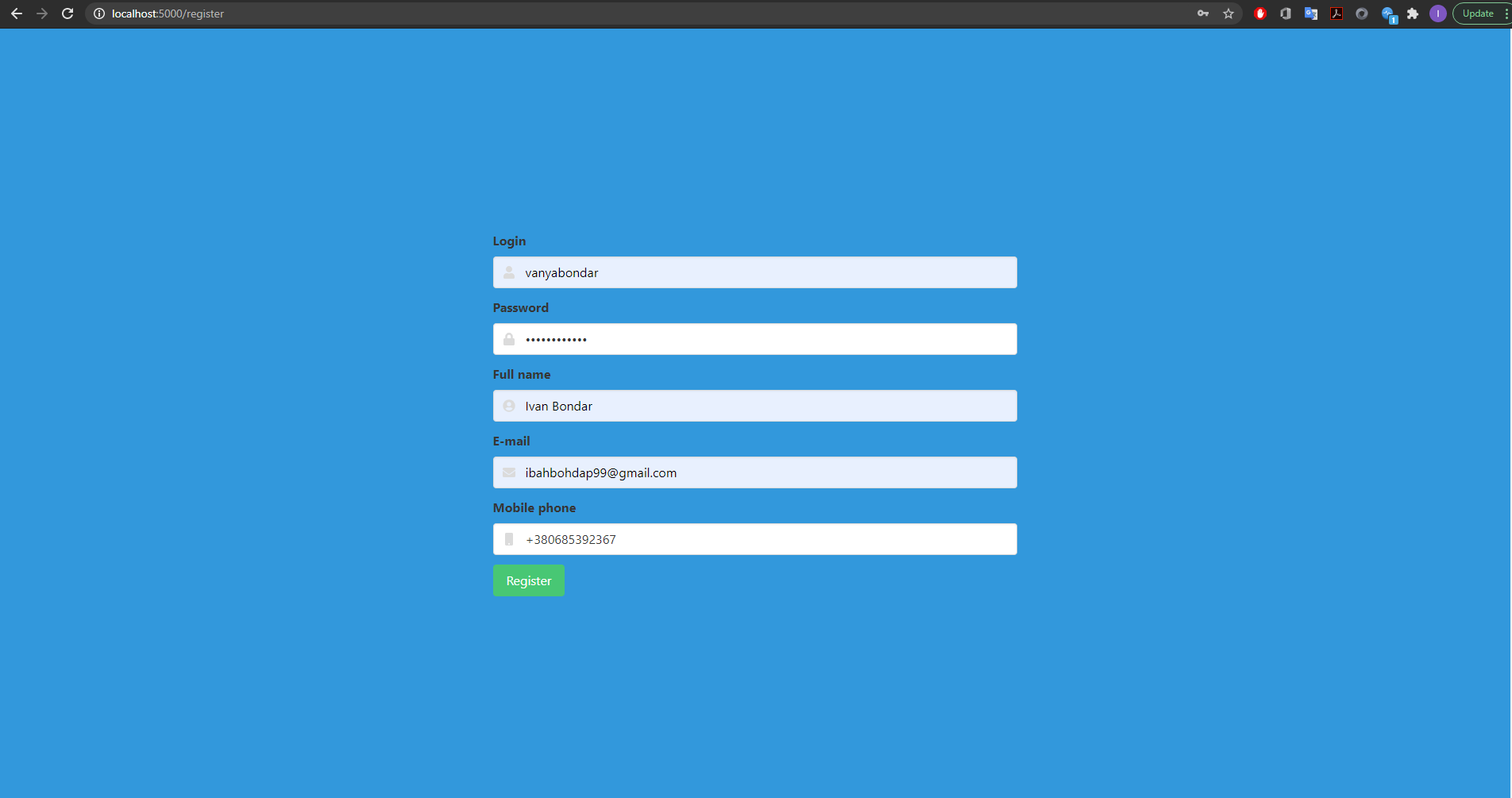
Для виконання лабораторної роботи було розроблено клієнт-серверну програму з можливістю реєстрації та аутентифікації. Для створення веб-додатку було використано фреймворк Flask.

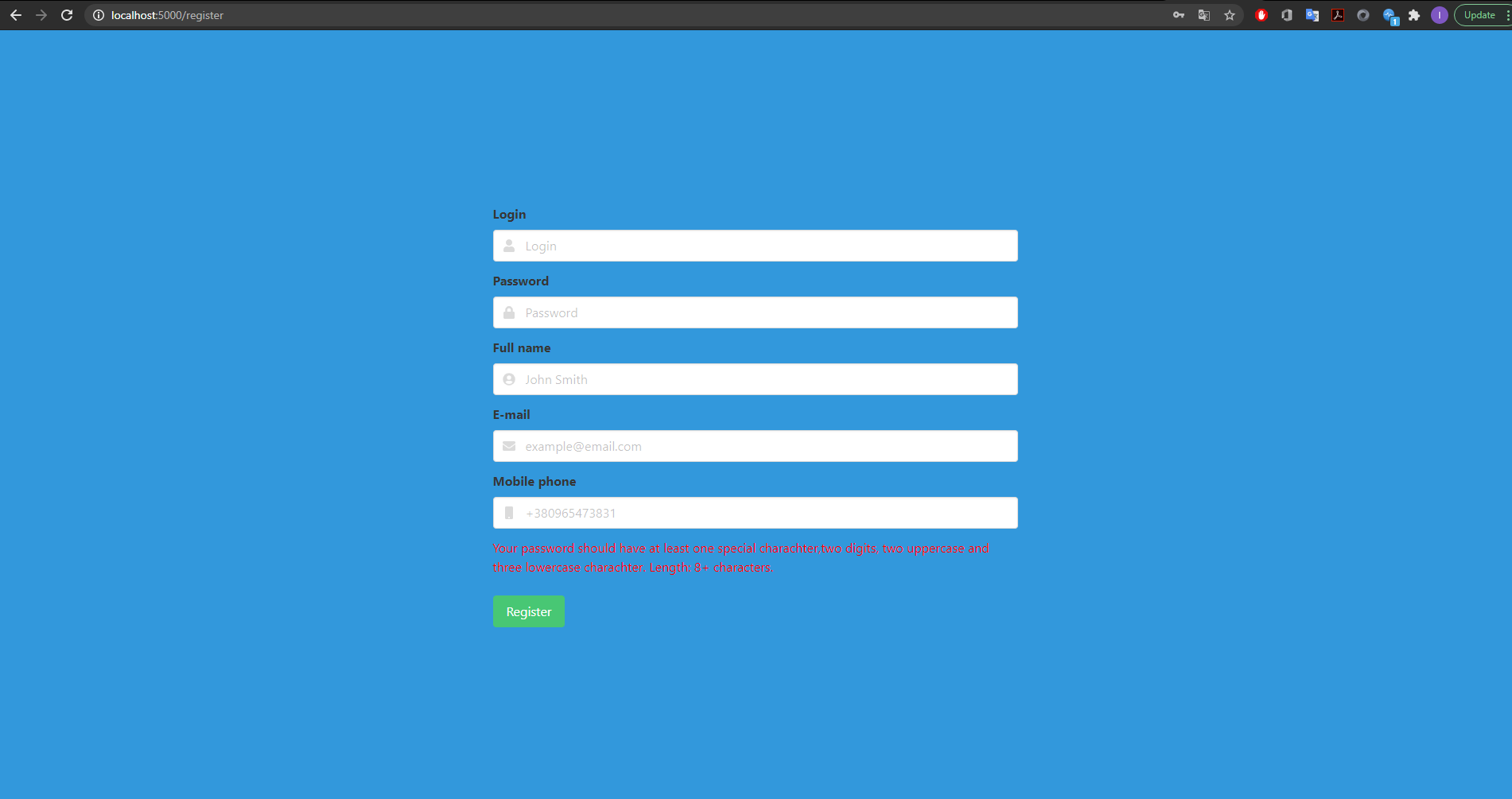


При спробі реєстрації пароль перевіряється на надійність, він має відповідати наступним вимогам:

* Містити не менше 8 символів
* Містити не менше 2 букв у верхньому регістрі
* Містити не менше 2 цифр
* Містити не менше 3 цифр в нижньому регістрі
* Містити хоча б один спеціальний символ

Також пароль не має верхнього обмеження по довжині.

Якщо заданий користувачем пароль не відповідає вимогам, користувач отримує повідомлення про невідповідність його паролю умовам.



Якщо дані введені користувачем відповідають вимогам, ми зберігаємо дані про користувача в базі даних. Замість пароля зберігається його хеш, який знаходиться за допомогою bcrypt.

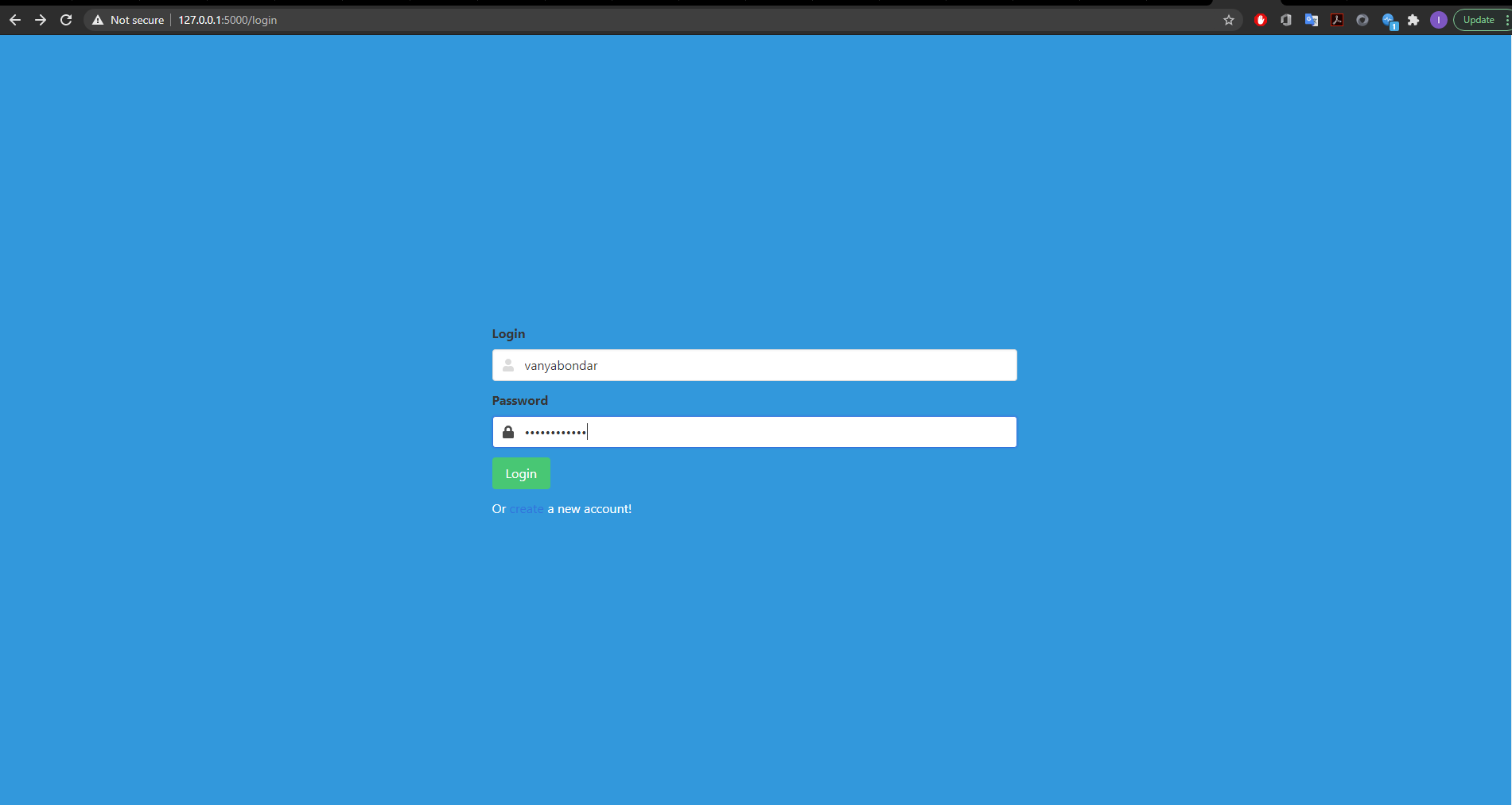
Функція bcrypt була обрана тому, що вона є адаптивною, і час її роботи можна налаштовувати(сповільнювати), щоб ускладнити атаку перебором.

Для хешування також використовується сіль, що генерується для кожного пароля за допомогою методу bcrypt.gensalt().

Так як, bcrypt опрацьовує рядки тільки до 72 символів, то для того, щоб користувач міг обирати пароль будь-якої довжини, спочатку паролі хешуються за допомогою sha256.

Окрім логіна, імені, пошти, номеру телефону та хеша пароля в базі даних також містяться поля version та compromised.

При аутентифікації користувач вводить логін та пароль.



За допомогою методу bcrypt.checkpw порівнюється переданий користувачем та хеш збережений в базі даних для відповідного логіна. Якщо метод повертає позитивну відповідь тоді користувачеві повертається сторінка з його профілем.

