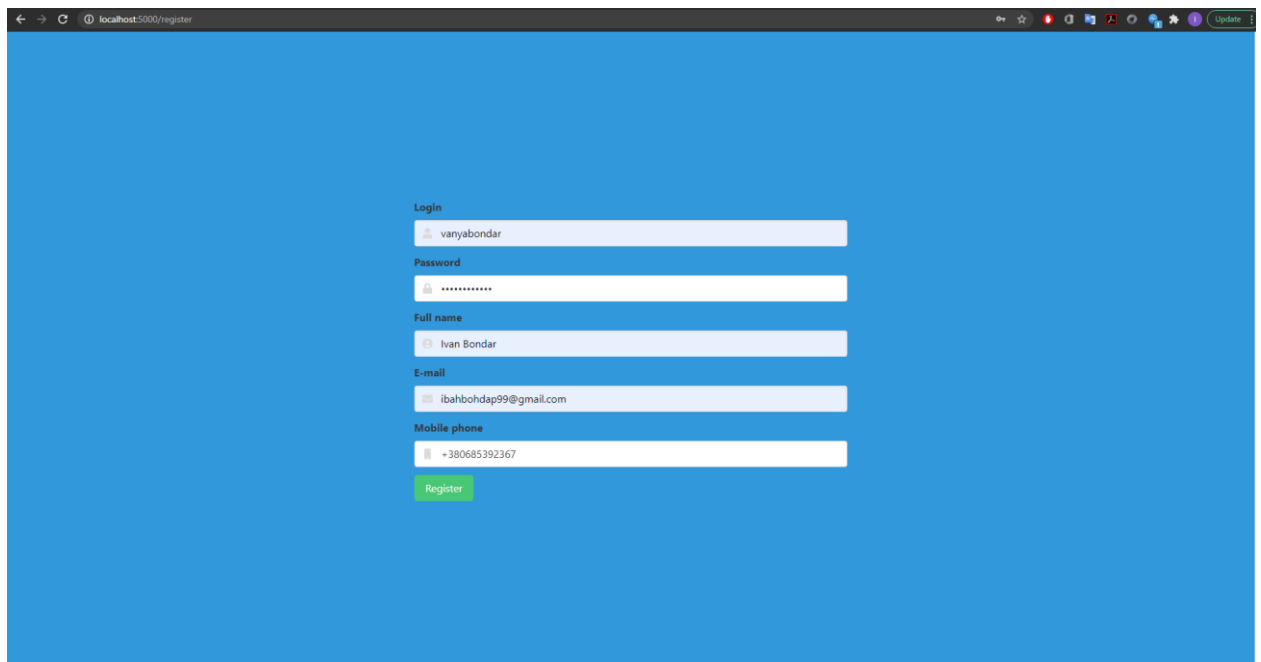


Для виконання лабораторної роботи було розроблено клієнт-серверну програму з можливістю реєстрації та аутентифікації. Для створення веб-додатку було використано фреймворк Flask.



localhost:5000/register

Login

vanyabondar

Password

Full name

Ivan Bondar

E-mail

ibahbohdap99@gmail.com

Mobile phone

+380685392367

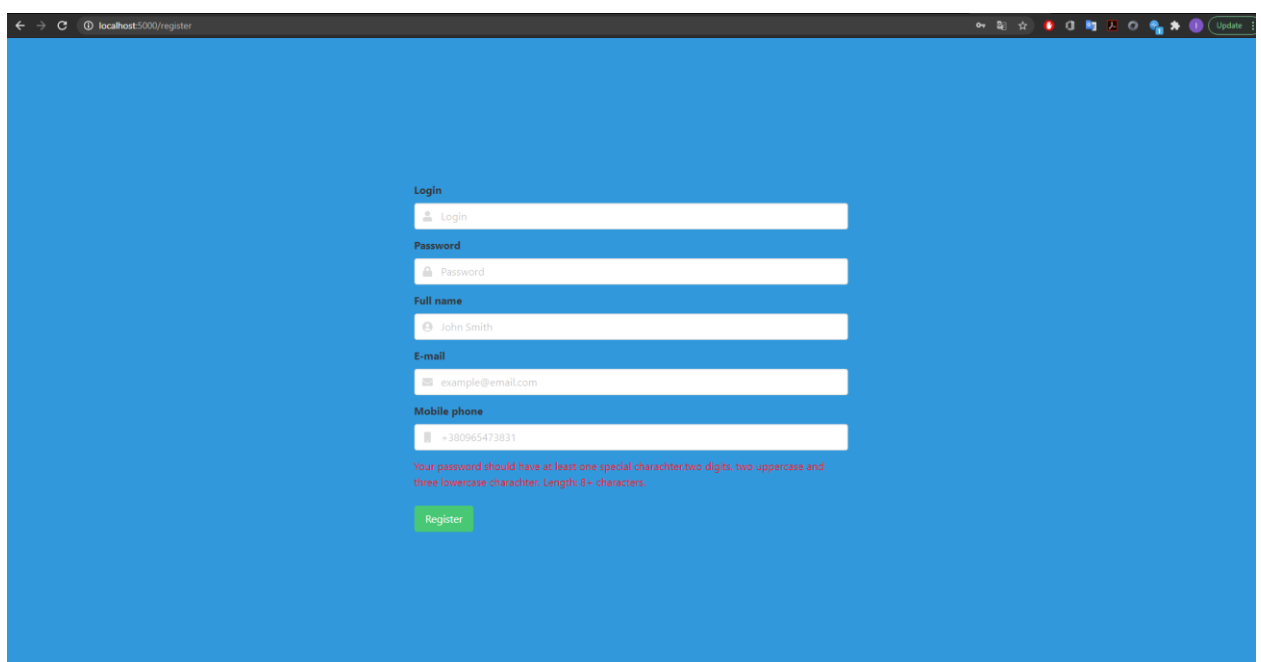
Register

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.



localhost:5000/register

Login

Login

Password

Password

Full name

John Smith

E-mail

example@email.com

Mobile phone

+380965473831

Your password should have at least one special character, two digits, two uppercase and three lowercase character. Length: 8+ characters.

Register

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

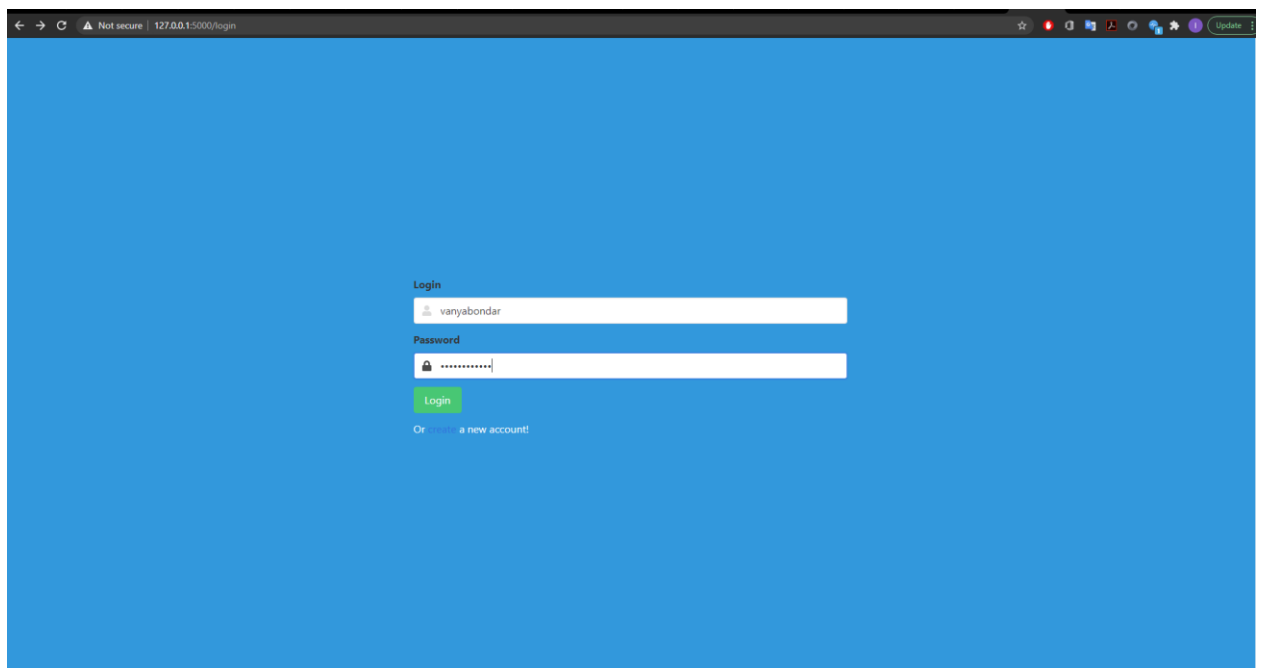
Функція bcrypt була обрана тому, що вона є адаптивною, і час її роботи можна налаштовувати(сповільнювати), щоб ускладнити атаку перебором.

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.

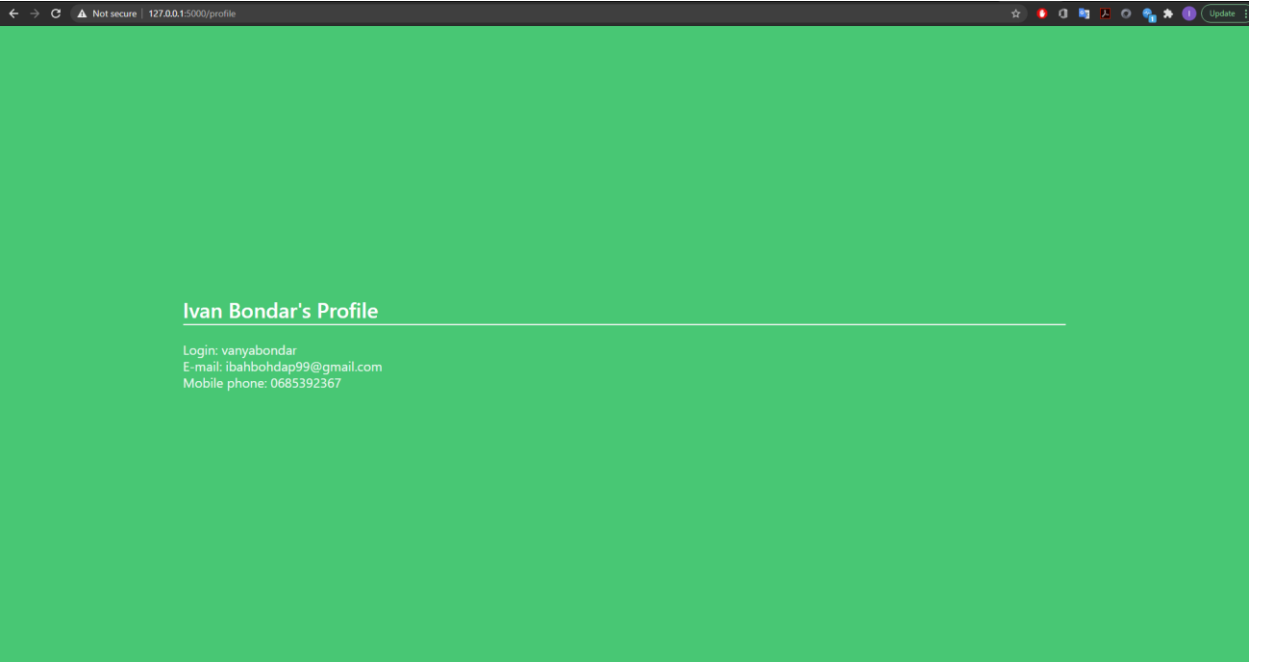
Окрім логіна, імені, пошти, номеру телефону та хеша пароля в базі даних також містяться поля version та compromised.

При аутентифікації користувач вводить логін та пароль.



The screenshot shows a web browser window with a blue background. In the center, there is a login form. The form has two input fields: the first is labeled 'Login' and contains the text 'vanyebondar'; the second is labeled 'Password' and contains masked characters (dots). Below the password field is a green button labeled 'Login'. At the bottom of the form, there is a link that says 'Or login with a new account!'.

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.



Ivan Bondar's Profile

Login: vanyabondar
E-mail: ibahbohdap99@gmail.com
Mobile phone: 0685392367