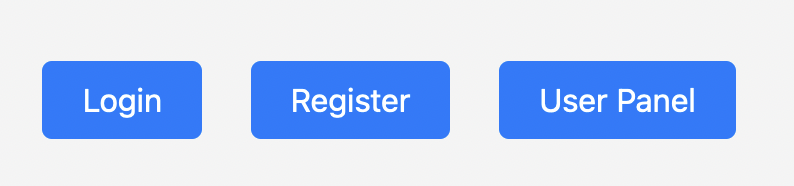
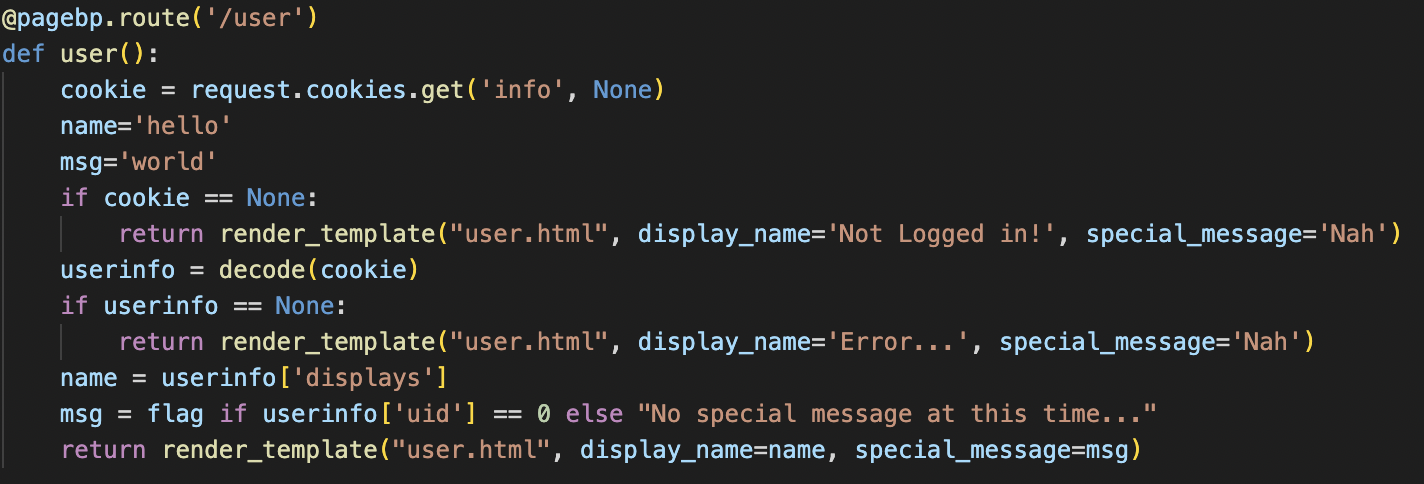
**Web Enumeration**

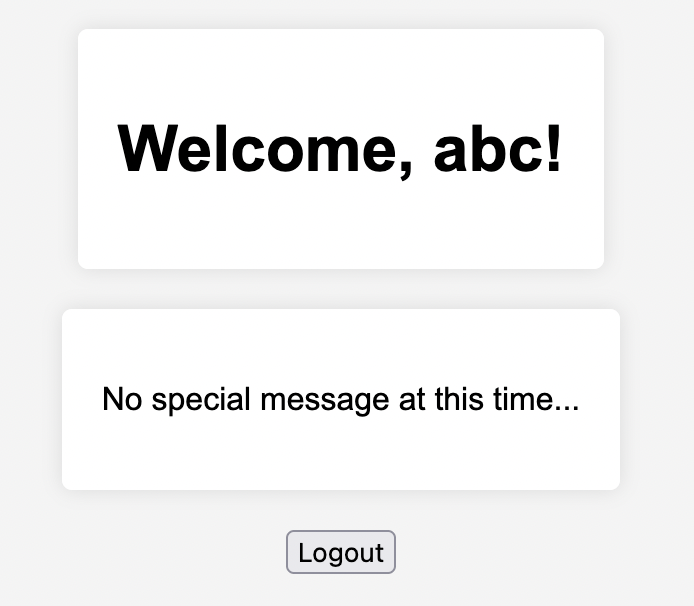
Trang web cho bạn đăng ký, đăng nhập, đặt uid =1



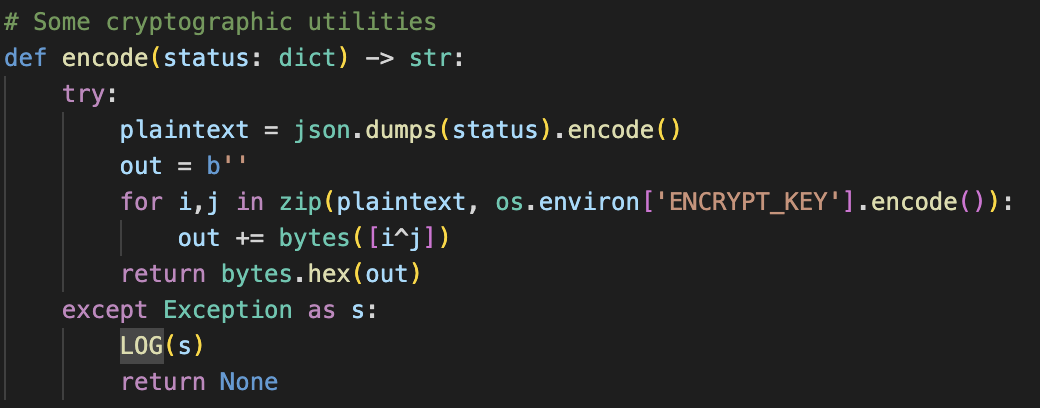
Để lấy được flag, bạn phải làm cho uid bằng 0



Nếu uid bằng 1 thì nó sẽ hiện thông báo sau:



Để làm được điều này, mình phải thay đổi cookie info



Làm sao để biết ENCRYPT\_KEY?

Ứng dụng dùng thuật toán khá đơn giản để mã hóa và giải mã: phép toán xor. Nếu bạn biết được thuật toán, plaintext và ciphertext thì dễ suy ra encrypt key. Nó gọi là Known Plaintext Attack.

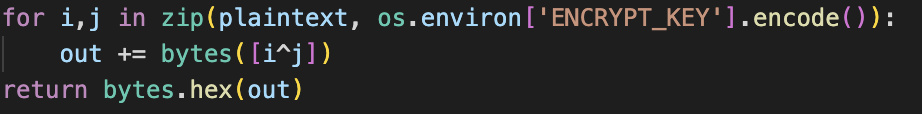
Ví dụ:

dict: {'username': 'abc', 'displays': 'abc', 'uid': 1}

plaintext: b'{"username": "abc", "displays": "abc", "uid": 1}'

ENCRYPT\_KEY.encode(): b'…'

Ciphertext: 2f05,<'5(){rat$!+cbgg =;9?612vcow5\*\*lgiu<%(nag8



Trong vòng lặp trên, i là “{“ (decimal là 123), j là “I” (decimal là 73), 123^73=50 (là số 2)

Số 1 nằm ở byte thứ 47 (plaintext) tương ứng với chữ g (ciphertext). Để thay đổi uid là 0, ciphertext phải dịch về 1 byte (chữ f)

**Flag: flag{fake\_flag}**