# CRY301x\_02-A\_VN – ASSIGNMENT 3

## Cách thức triển khai và chạy ứng dụng

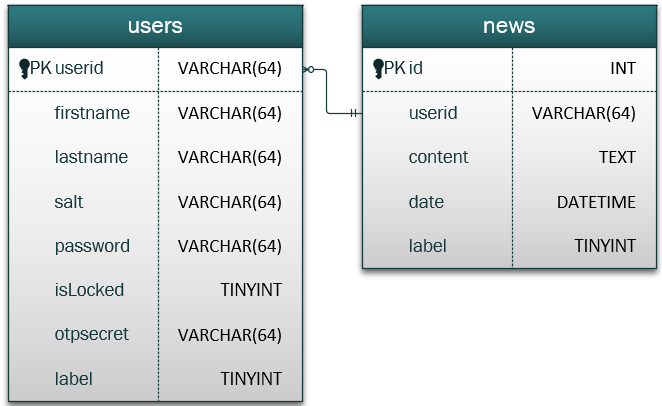
### Công cụ phát triển và Cấu trúc thư mục

* Cài đặt môi trường phát triển cho ngôn ngữ Java trên Windows 11, xem [Cài đặt môi trường Java | How Kteam](https://howkteam.vn/course/lap-trinh-java-co-ban-den-huong-doi-tuong/cai-dat-moi-truong-java-3834)
* Đăng ký JetBrains Student Pack bằng tài khoản education, cài đặt và sử dụng IDE Intelliji cho việc phát triển ứng dụng, xem <https://www.jetbrains.com/academy/student-pack/>
* Tạo JakartaEE project với Intelliji và cài đặt cấu trúc project như sau:
  + Common: Chứa các constants, utilities, etc.
  + Crypto: encryption utilities and OTP.
  + DAO: Chứa các DAO.
  + Enums: Chứa enum
  + Module chính của project có tên com.cry301x.asm3.mfaauth chứa các Servlet
  + Models: chứa models.
  + Wepapp: Chứa các JSP, HTML, CSS và resource files khác.
* Trên trình duyệt, cài đặt extension Authenticator để generate OTP cho ứng dụng, xem và tải tại <https://chromewebstore.google.com/detail/authenticator/bhghoamapcdpbohphigoooaddinpkbai>

### 1.2. Database

Dựa trên database được thiết kế như trong bài học, chạy lệnh SQL dưới đây trong MySQL để khởi tạo database.

|  |
| --- |
| CREATE DATABASE mfa\_sys;  USE mfa\_sys;  CREATE TABLE users (  userid VARCHAR(64) PRIMARY KEY,  firstname VARCHAR(64),  lastname VARCHAR(64),  salt VARCHAR(64) NOT NULL,  password VARCHAR(64) NOT NULL,  isLocked TINYINT,  faillogin TINYINT NOT NULL,  otpsecret VARCHAR(64) NOT NULL,  label TINYINT NOT NULL,  CONSTRAINT chk\_label CHECK (label IN (1, 2, 3, 4))  );  CREATE TABLE news (  id INT PRIMARY KEY AUTO\_INCREMENT,  userid VARCHAR(64),  content TEXT,  date DATETIME NOT NULL,  label TINYINT NOT NULL,  CONSTRAINT chk\_label\_news CHECK (label IN (1, 2, 3, 4)),  FOREIGN KEY (userid) REFERENCES users(userid)  ); |



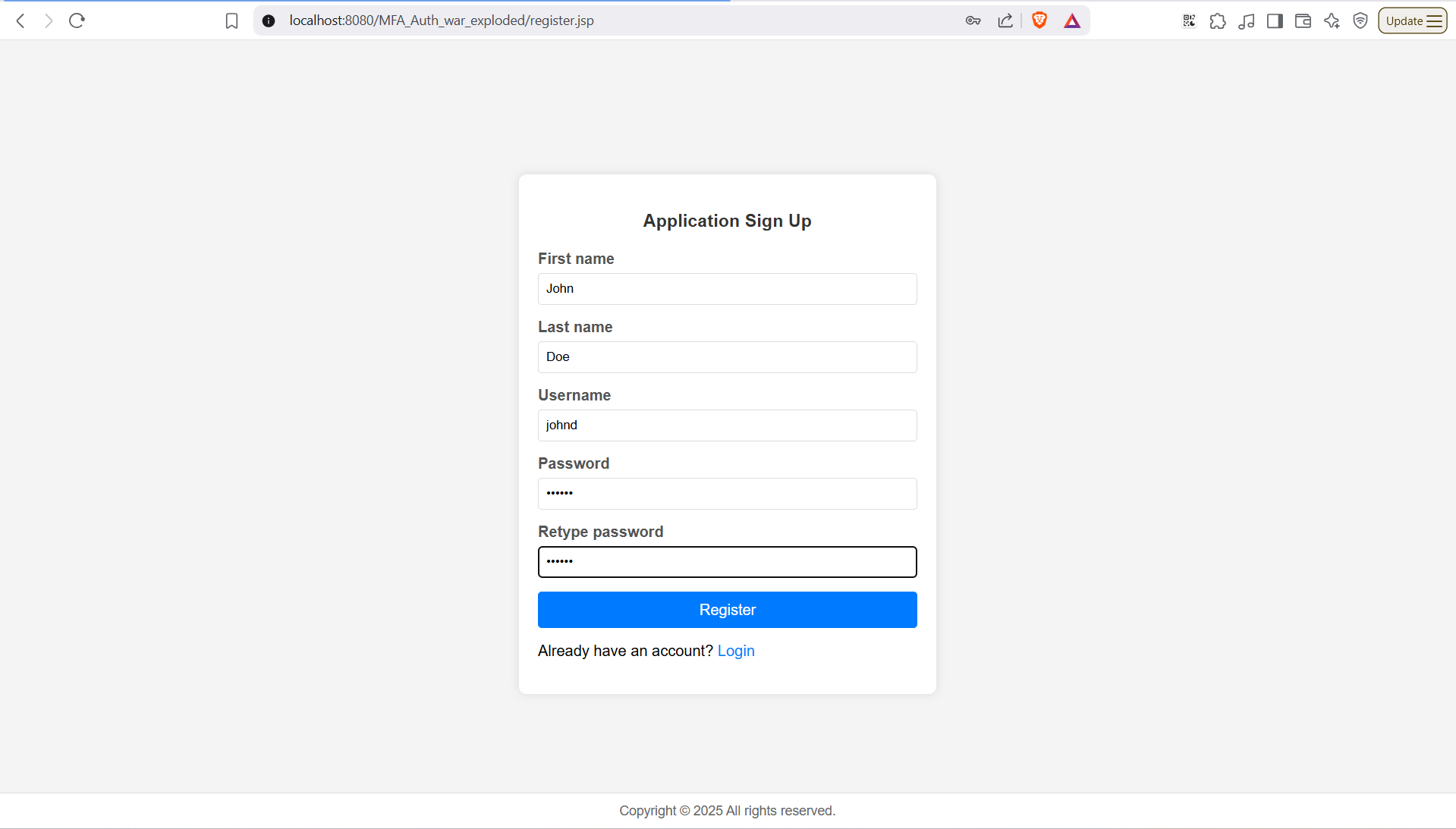
## Thực thi và Kiểm định kết quả

### UC\_REGISTER – Đăng ký

#### Luồng chính – Đăng ký thành công

1. Người dùng truy cập vào trang Đăng ký và nhập thông tin.

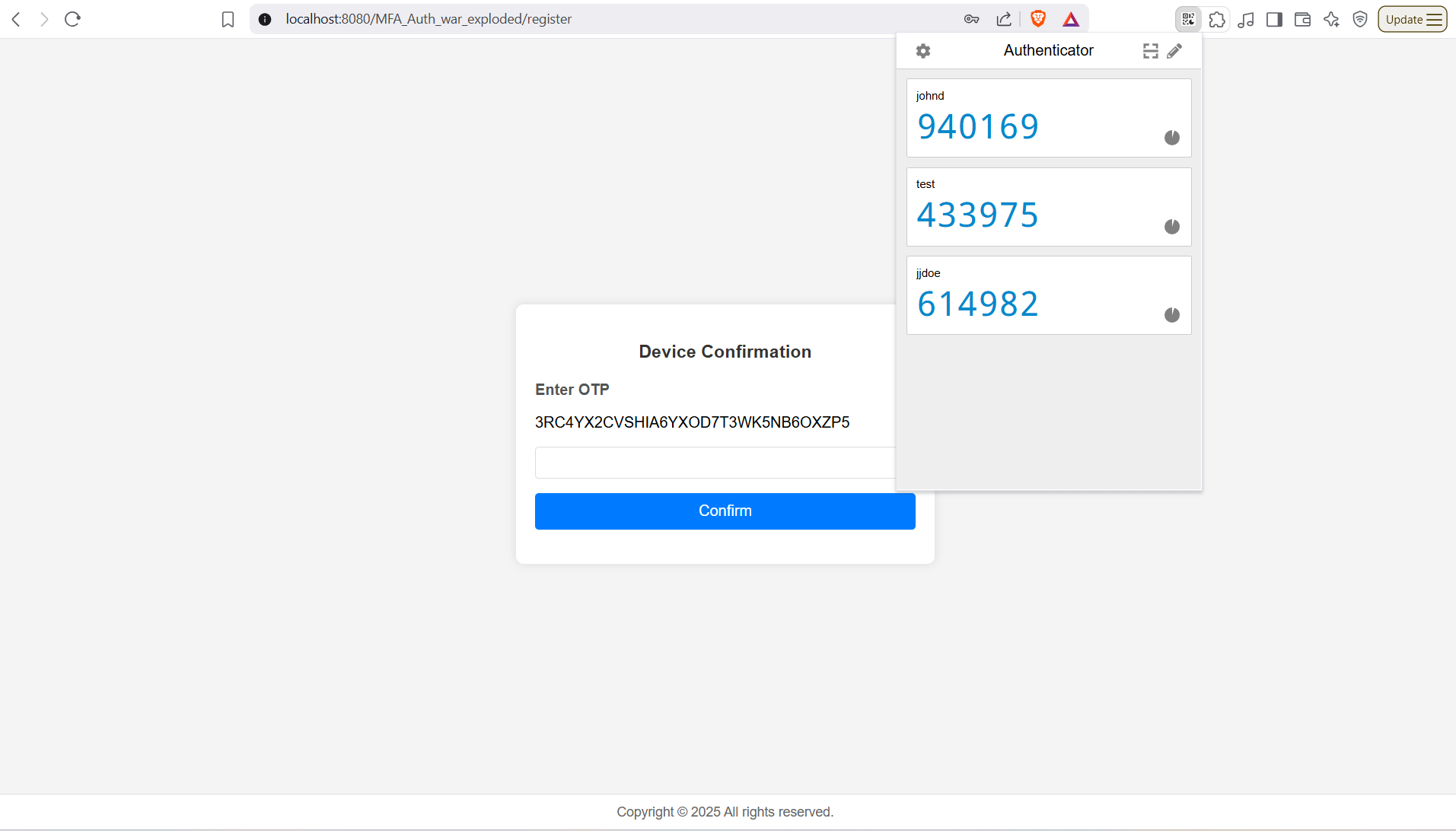
2. Người dùng đăng ký thông tin và nhấn nút Register



3. Thông tin đăng ký là hợp lệ, ứng dụng chuyển hướng trình duyệt của người dùng sang trang Xác nhận

4. Trang Xác nhận hiển thị chuỗi ký tự dưới dạng mã Base32 để người dùng khởi tạo bộ sinh OTP trên Google Authenticator

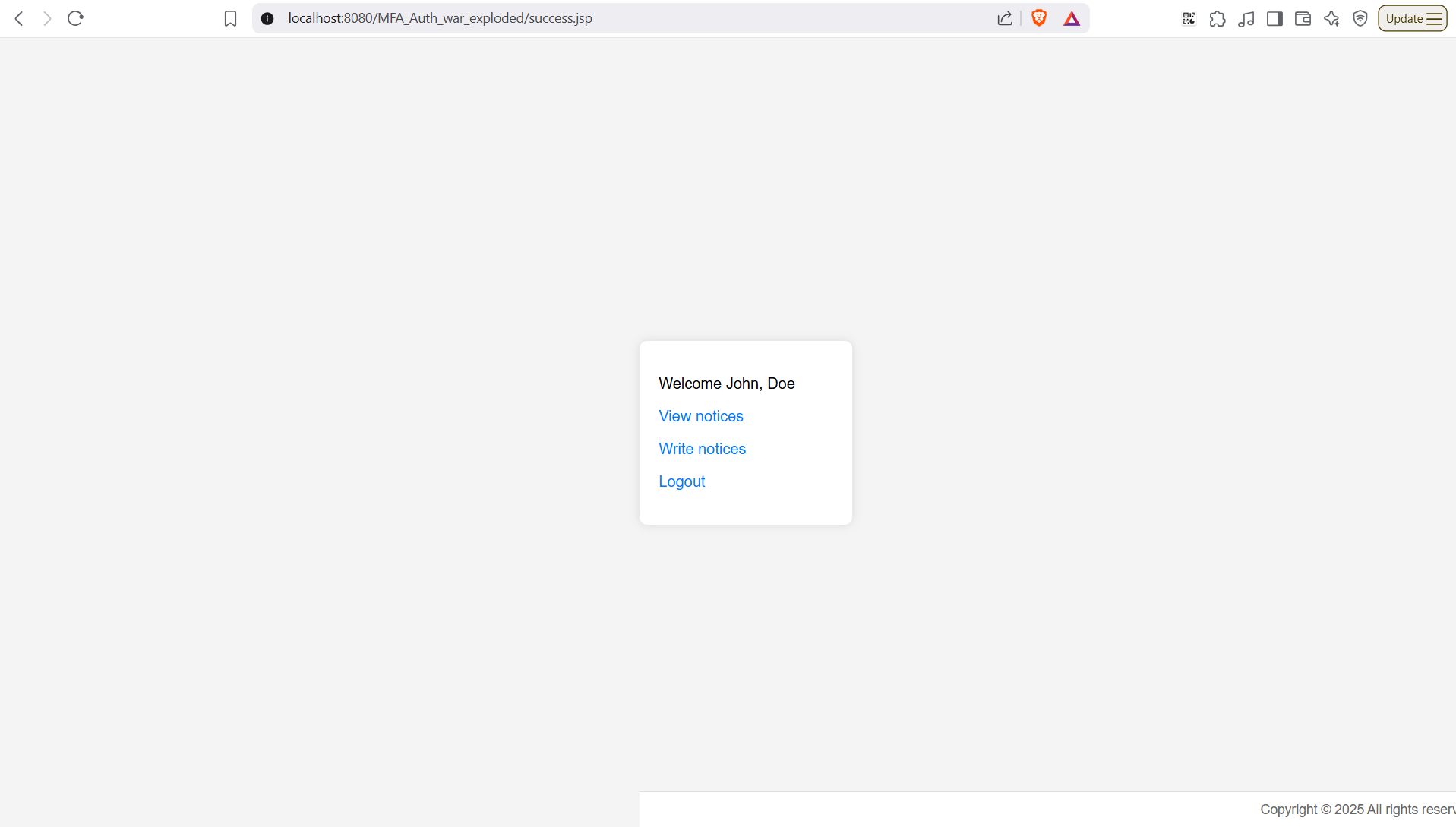
5. Người dùng thêm bộ sinh OTP trên Google Authenticator



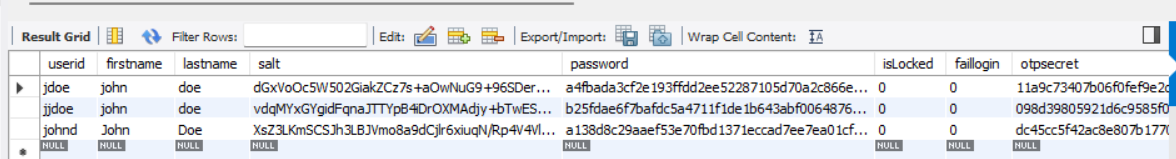
6. Người dùng điền mã OTP và nhấn nút Confirm

7. Nếu kiểm tra mã OTP hợp lệ, hệ thống chuyển hướng trình duyệt của người dùng tới trang Chào mừng

8. Trang Chào mừng hiển thị thông báo đăng nhập thành công và tên đầy đủ



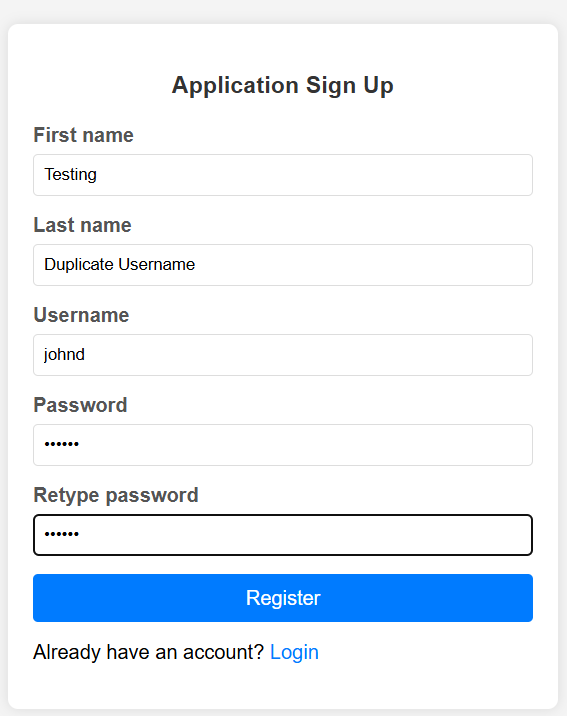
User mới được thêm vào database thành công.

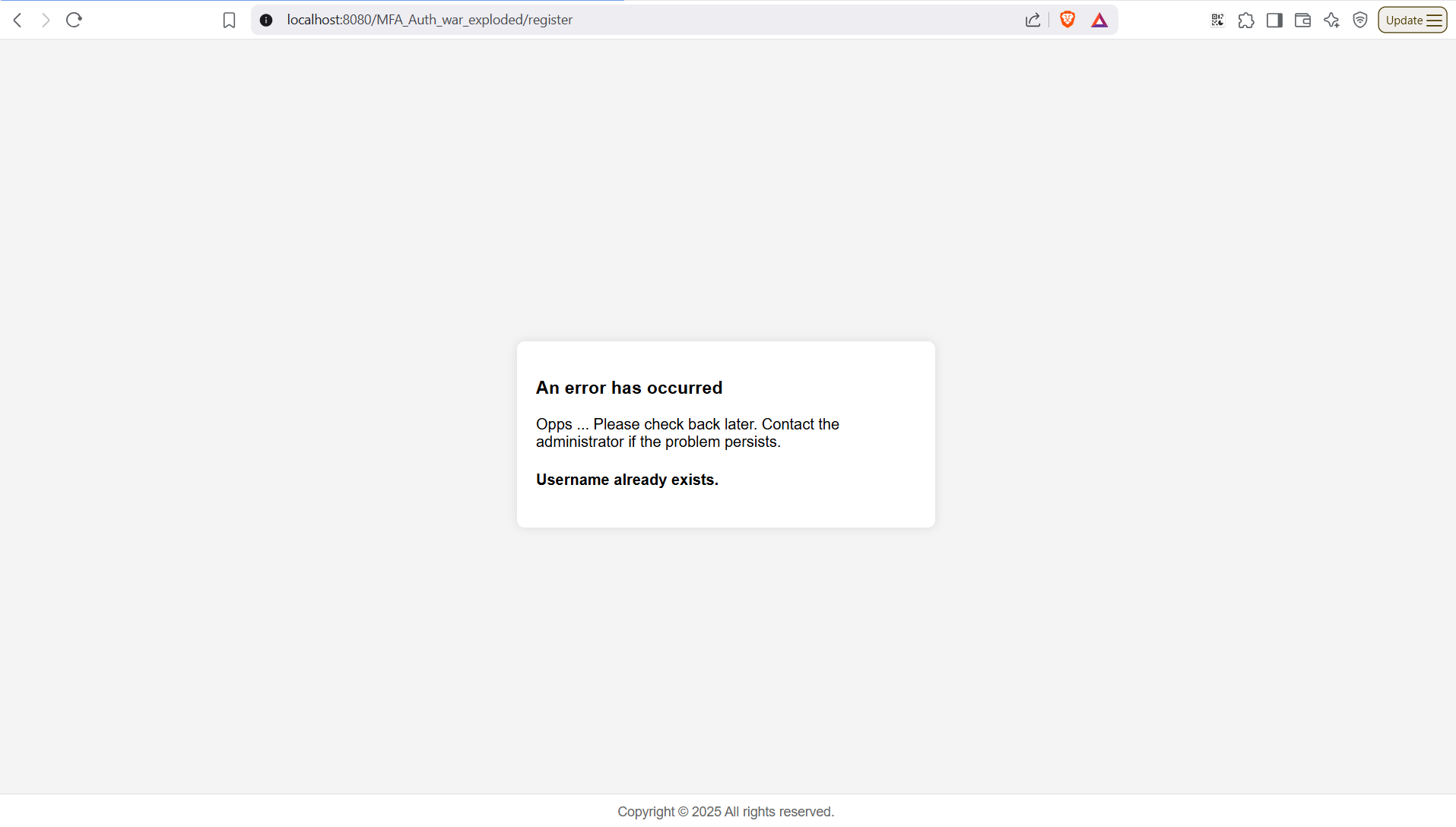


#### Luồng phụ 1- thông tin không hợp lệ, báo lỗi

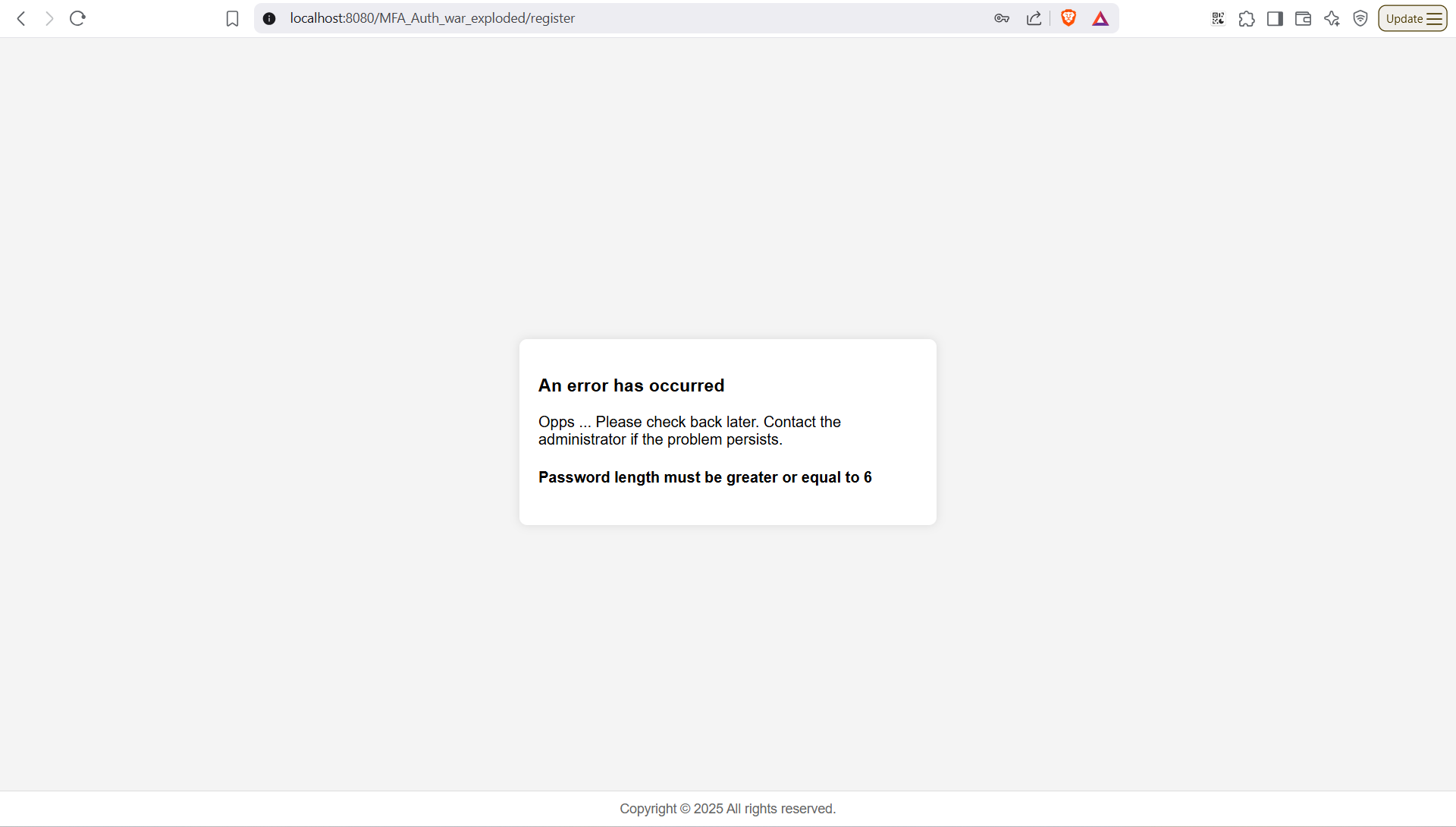
Nếu thông tin không hợp lệ, chuyển hướng trình duyệt sang trang Báo lỗi

* Trường hợp username đã tồn tại (*johnd*)



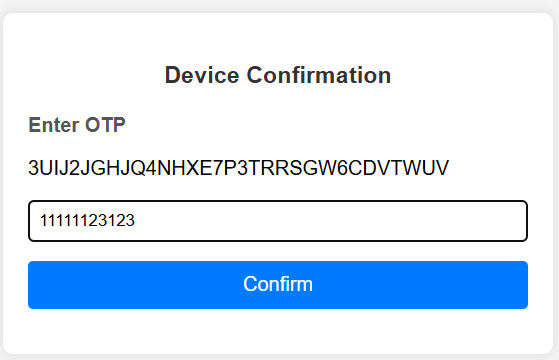


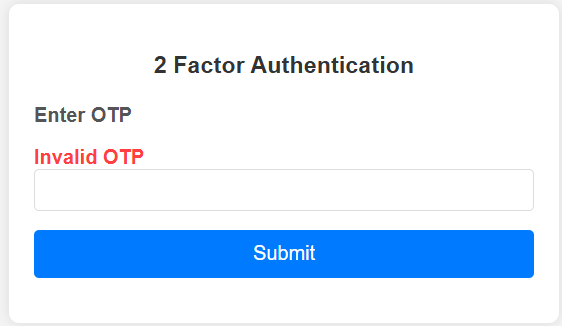
* Độ dài password không thỏa mãn >= 6



#### Luồng phụ 2 – Sai OTP, hiển thị lại trang xác nhận

Nếu mã OTP không hợp lệ, hiển thị lại trang Xác nhận





### UC\_LOGIN – Đăng nhập

#### Luồng chính - Người dùng đã đăng ký tài khoản đăng nhập thành công

1. Người dùng truy cập vào Trang chủ

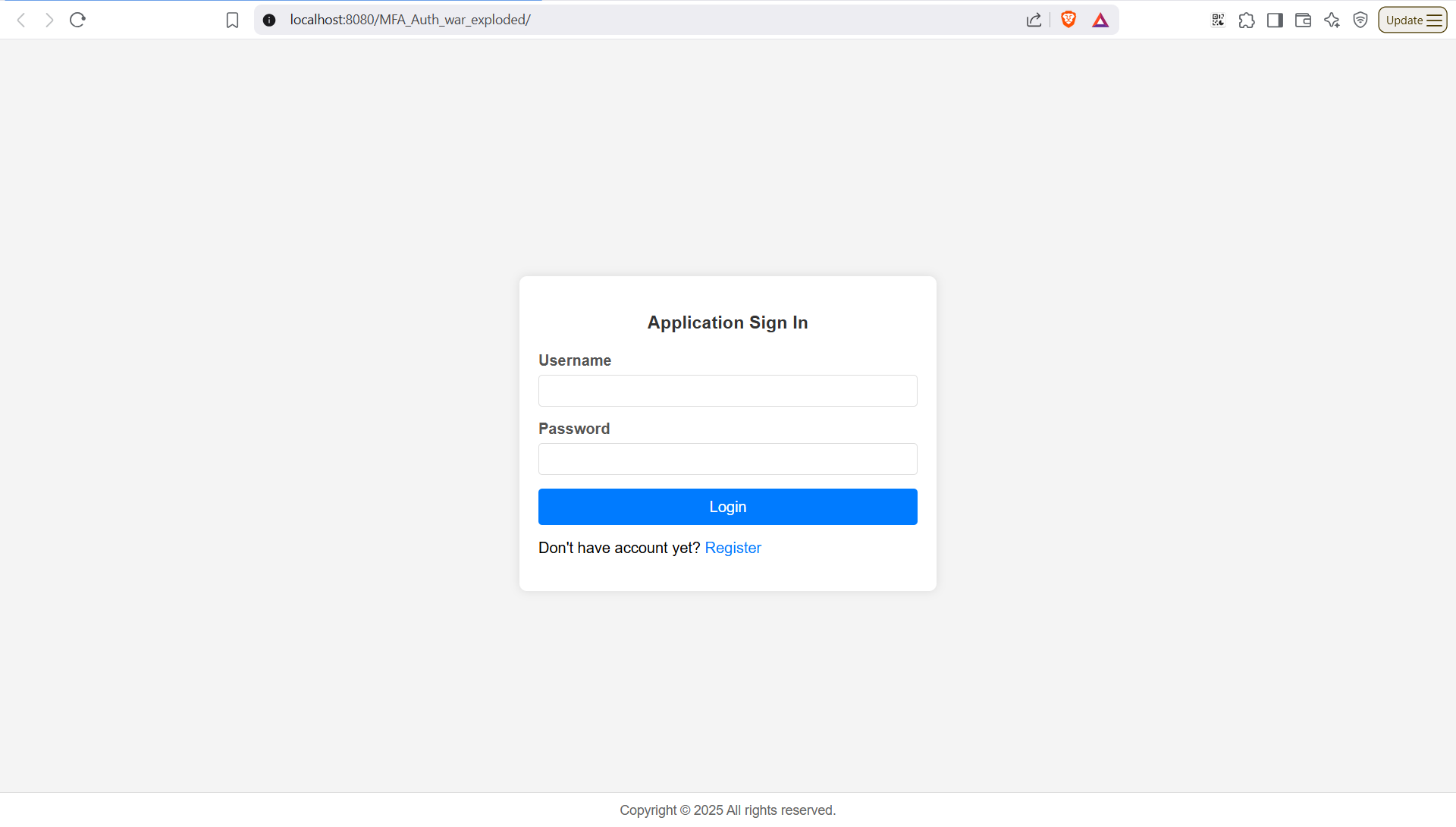
2. Người dùng nhập thông tin tài khoản và nhấn nút Login

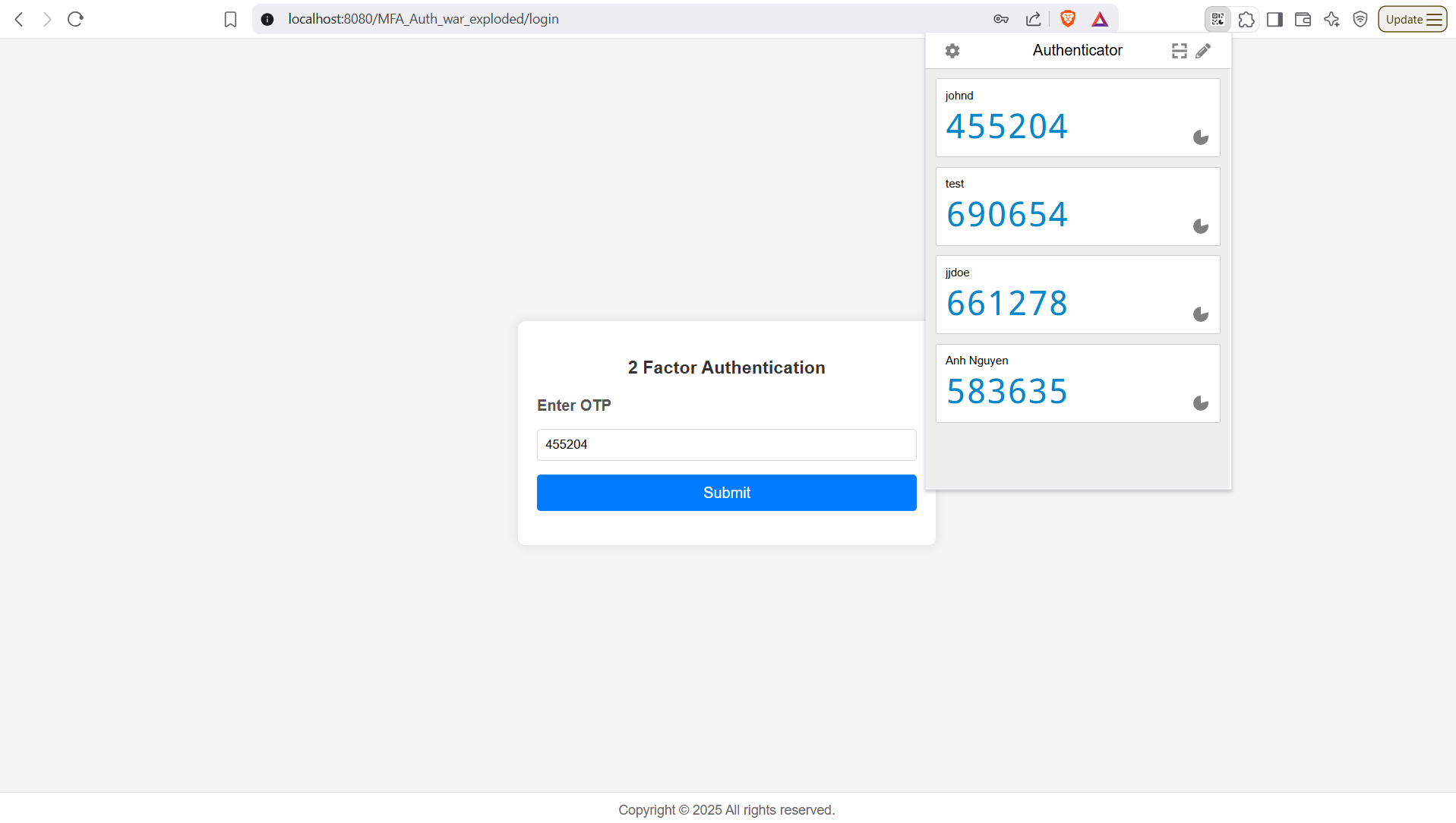
3. Nếu thông tin đăng nhập là hợp lệ, ứng dụng chuyển hướng trình duyệt của người dùng sang trang Đăng nhập bước 2

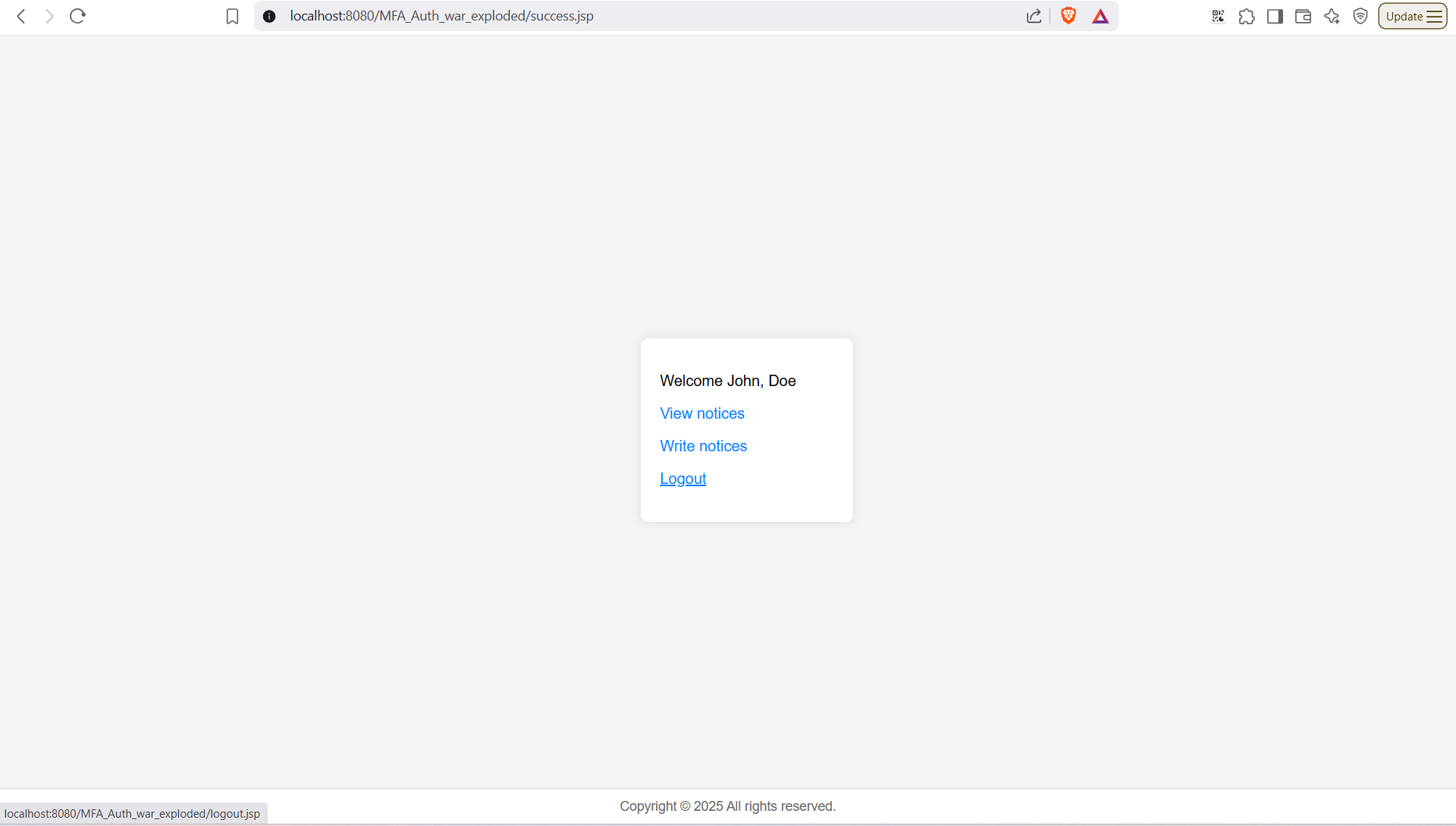
4. Người dùng điền mã OTP và nhấn nút Submit

5. Nếu kiểm tra mã OTP hợp lệ, hệ thống chuyển hướng trình duyệt của người dùng tới trang Chào mừng

6. Trang Chào mừng hiển thị thông báo đăng nhập thành công và tên đầy đủ

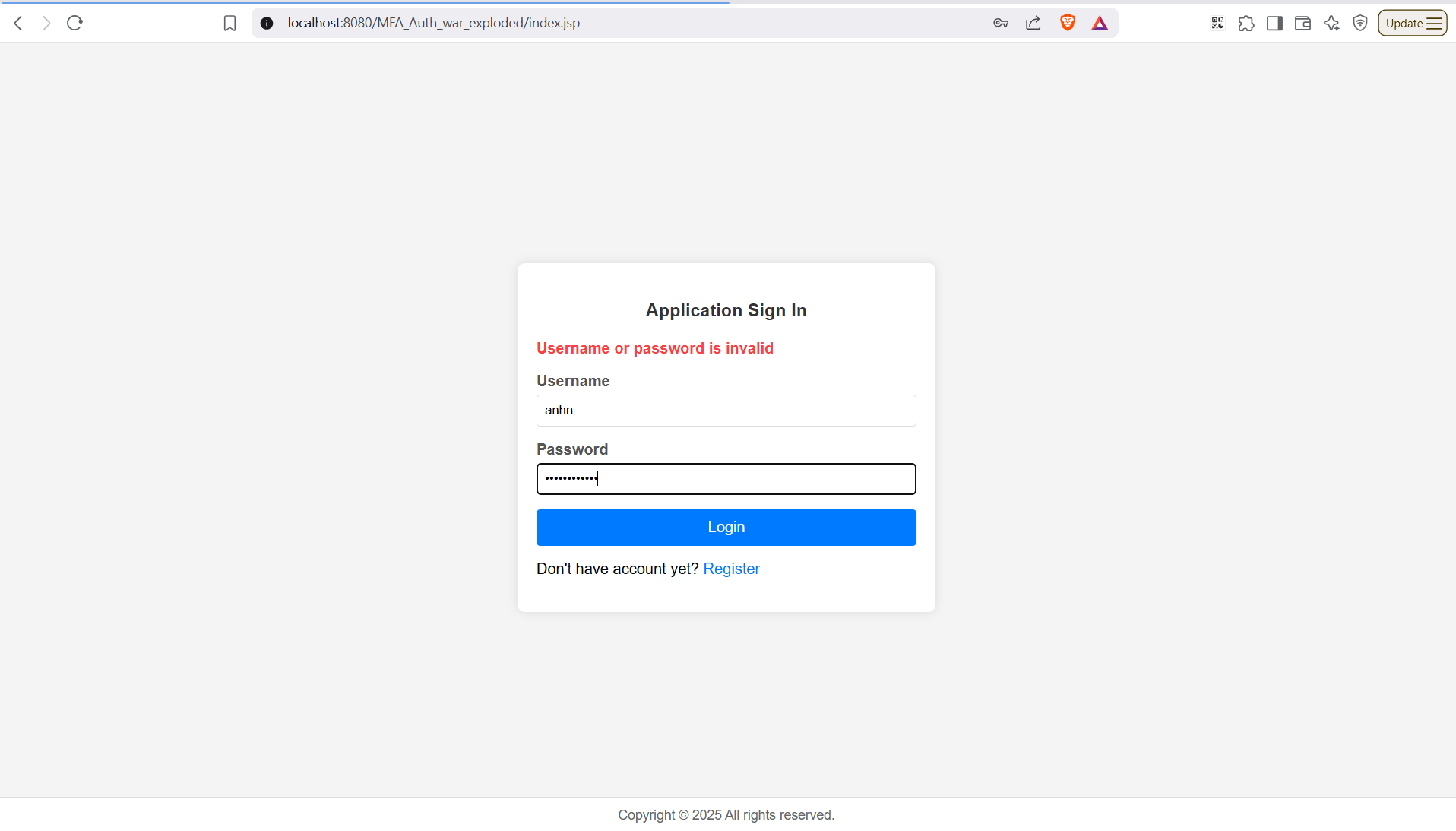




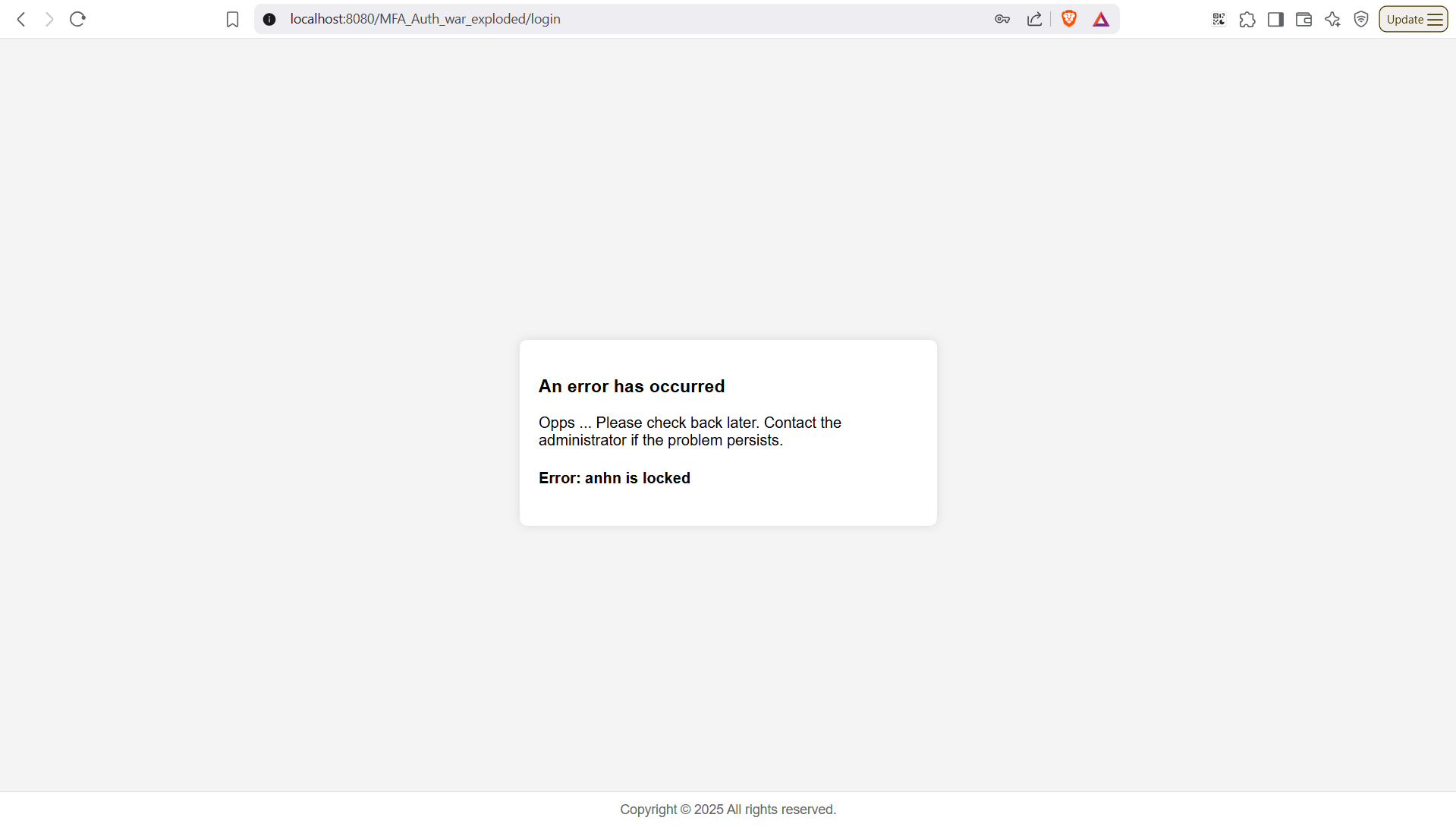


#### Luồng phụ 1 - Nếu tài khoản bị khóa, chuyển sang trang Báo lỗi - Nếu thông tin không hợp lệ, chuyển hướng trình duyệt sang Trang chủ

Sai mật khẩu

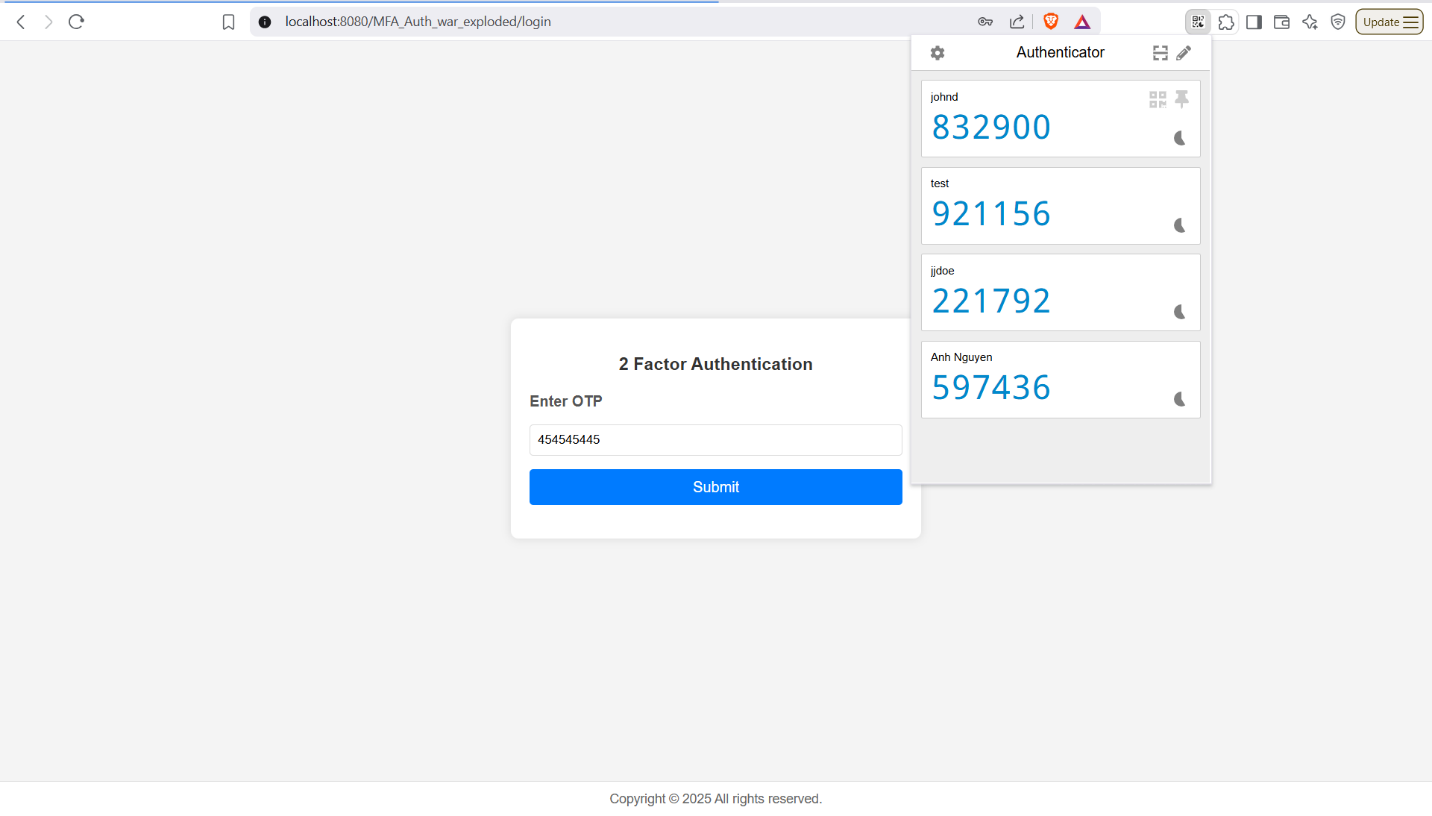


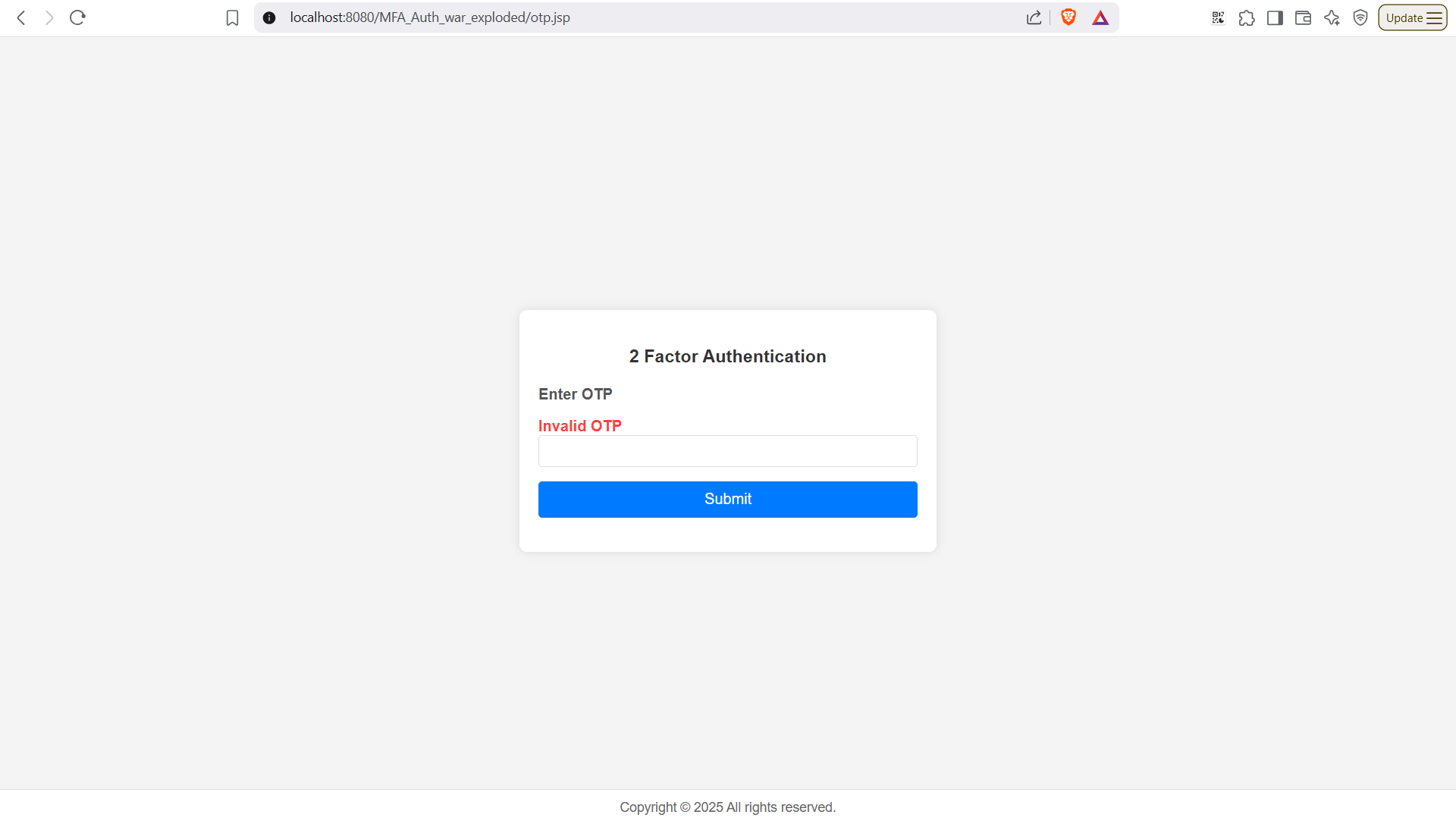
Tài khoản bị khóa do nhập sai quá 5 lần.



#### Luồng phụ 2 - Nếu mã OTP không hợp lệ, hiển thị lại trang Đăng nhập bước 2

Sai OTP



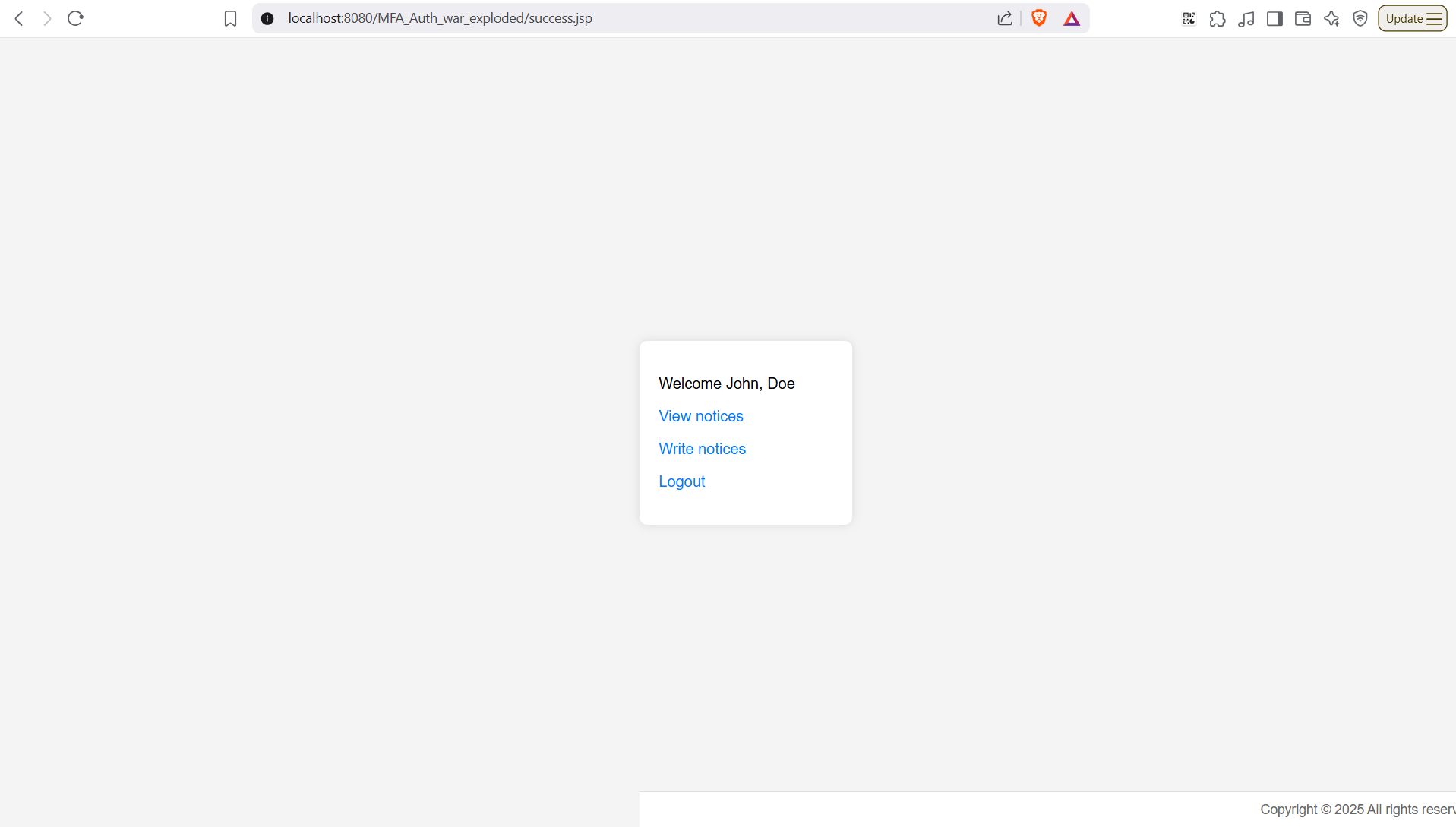


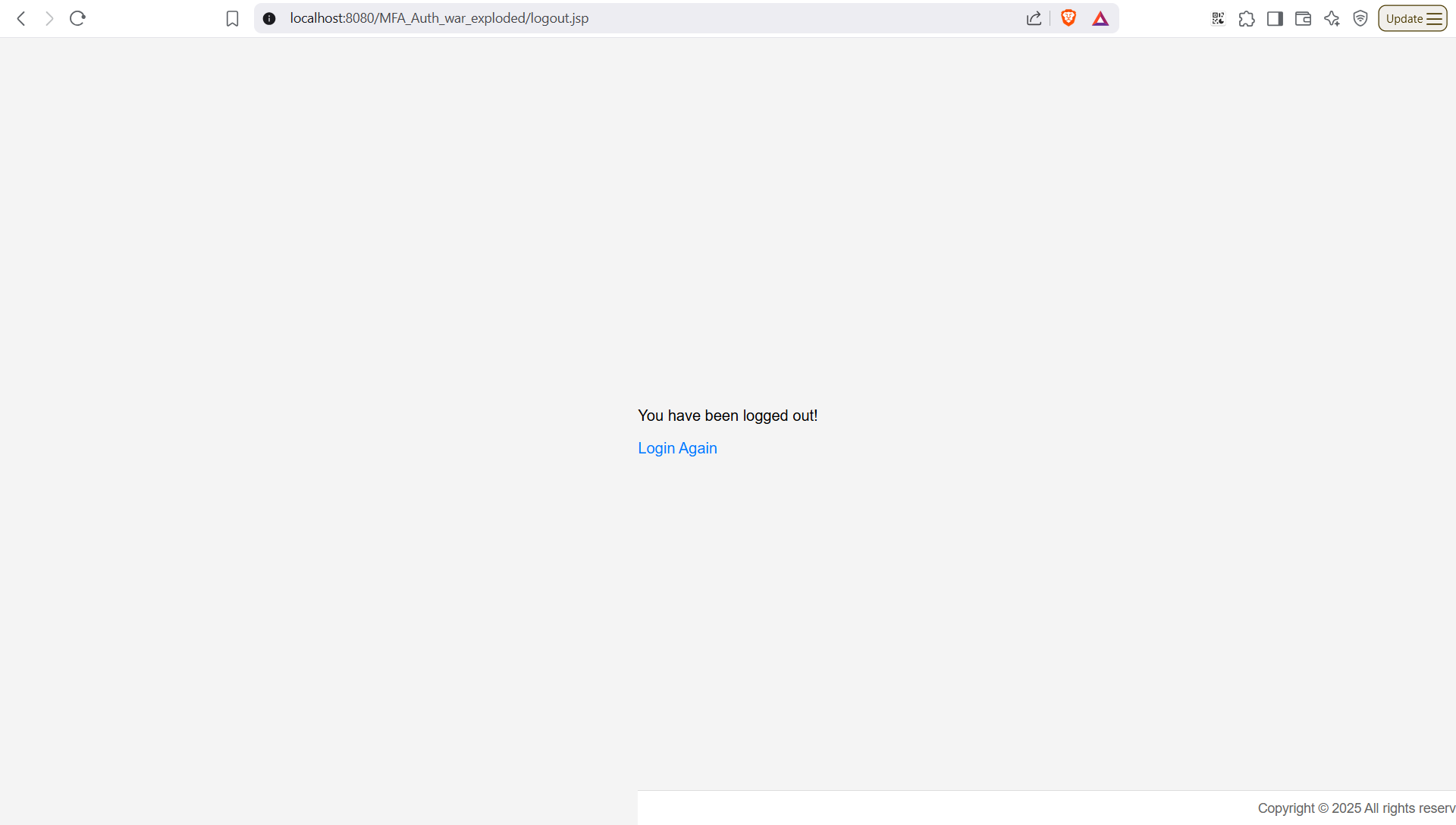
### UC\_LOGOUT – Đăng xuất

#### Luồng chính

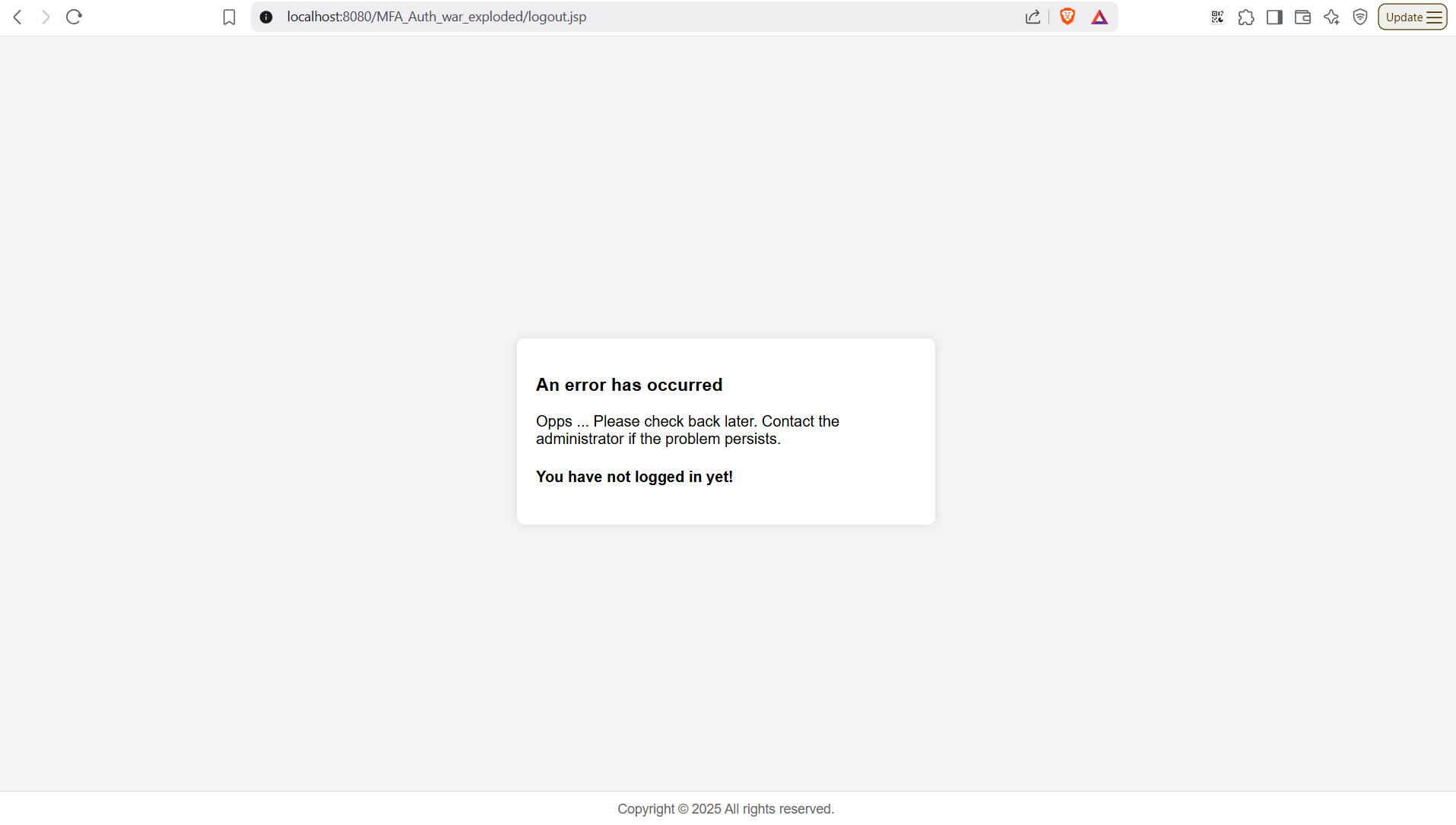
1. Người dùng truy cập vào trang Đăng xuất

2. Ứng dụng xóa phiên của người dùng và chuyển hướng truy cập của trình duyệt sang Trang chủ





#### Luồng phụ 1 - Nếu người dùng chưa đăng nhập, chuyển hướng truy cập sang trang Báo lỗi



### UC\_ACC\_LABEL – Gán nhãn bảo mật

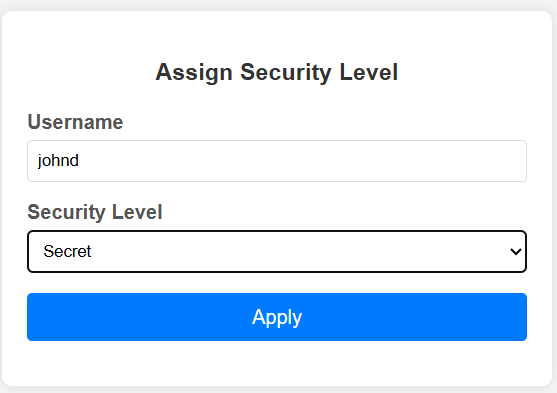
#### Luồng chính

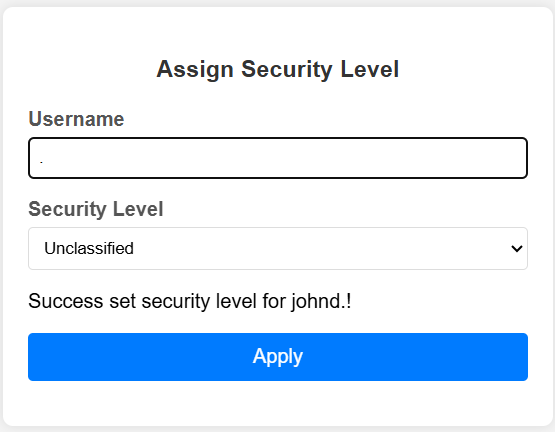
1. Quản trị viên truy cập vào trang Gán nhãn

2. Quản trị viên điền tên tài khoản và chọn nhãn bảo mật

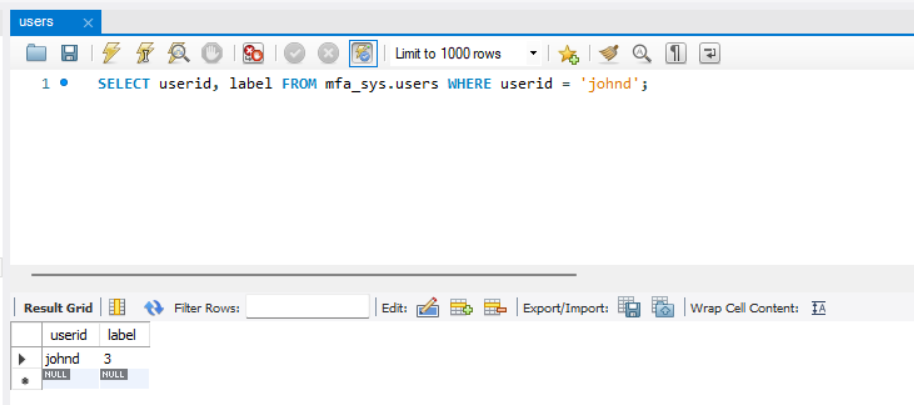
3. Quản trị viên nhấn nút Apply

4. Hệ thống thông báo thành công



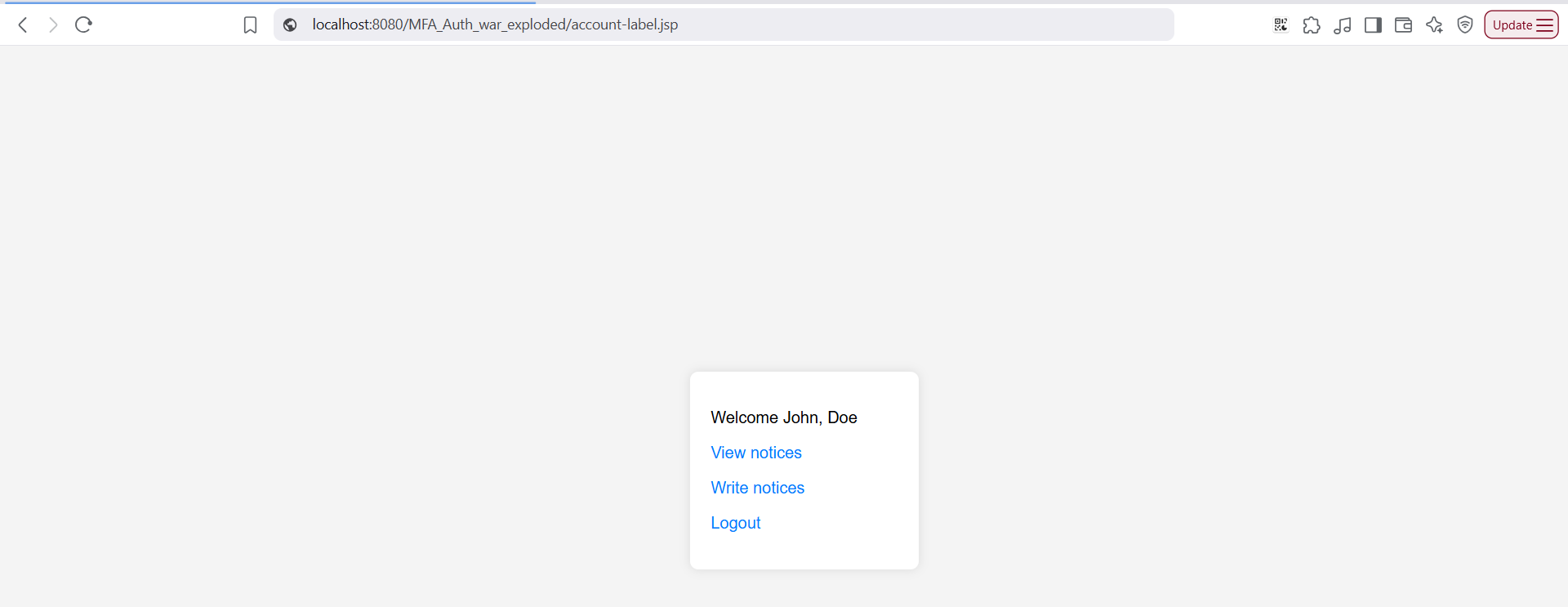


Johnd được set security level thành 3 – Secret thành công trong database.

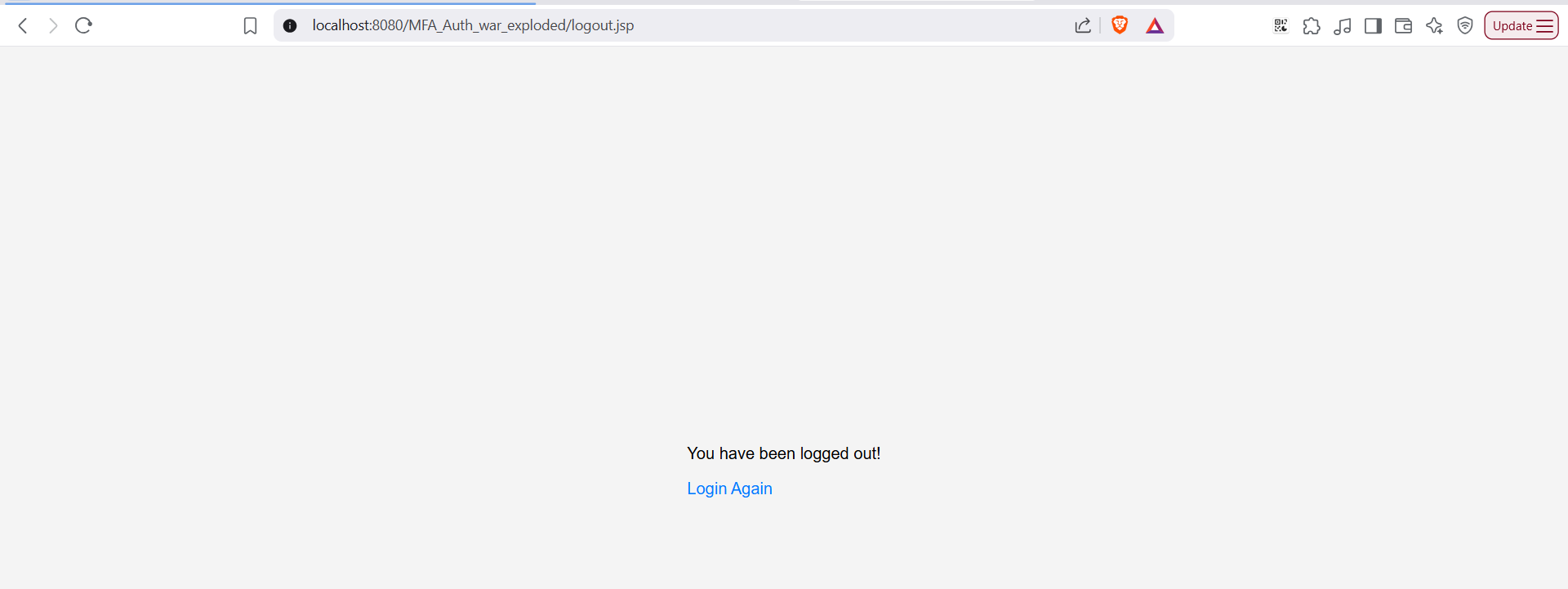


#### Luồng phụ 1 - Nếu người dùng đăng nhập với tài khoản không phải là admin, chuyển hướng trình duyệt truy cập sang trang Đăng xuất

Login bằng tài khoản không phải admin và cố gắng truy cập bằng đường link tới trang account label

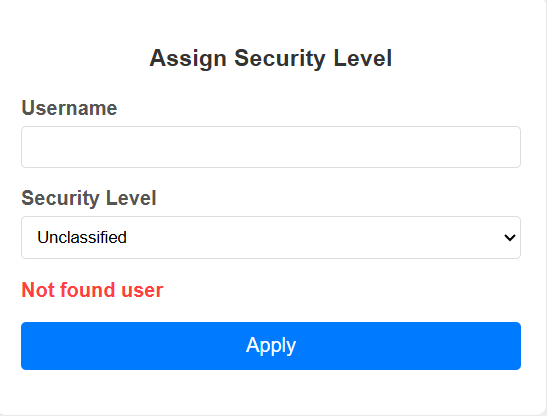


Chuyển hướng qua trang logout.



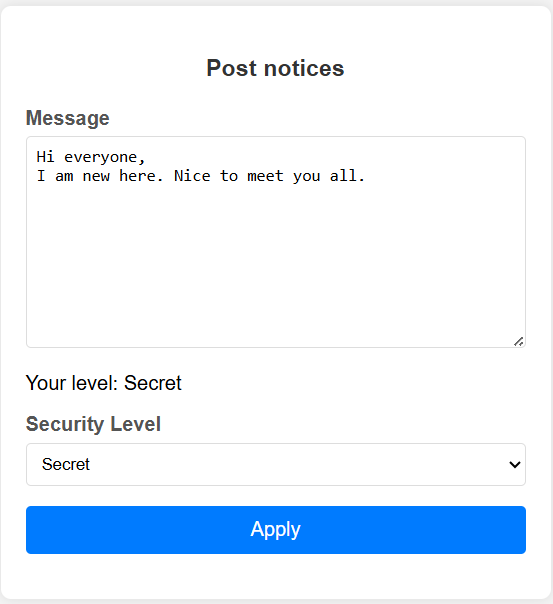
#### Luồng phụ 2 - Nếu người dùng chưa đăng nhập, chuyển hướng trình duyệt truy cập sang Trang chủ

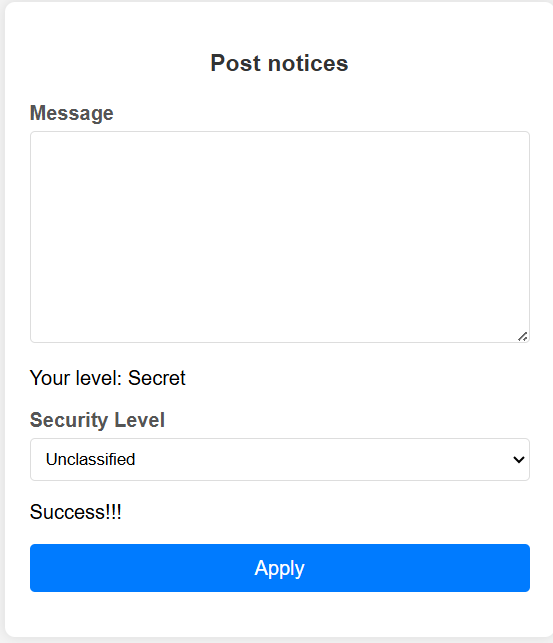
#### Luồng phụ 3 - Nếu tài khoản không tồn tại, chuyển hướng trình duyệt truy cập sang trang Báo lỗi



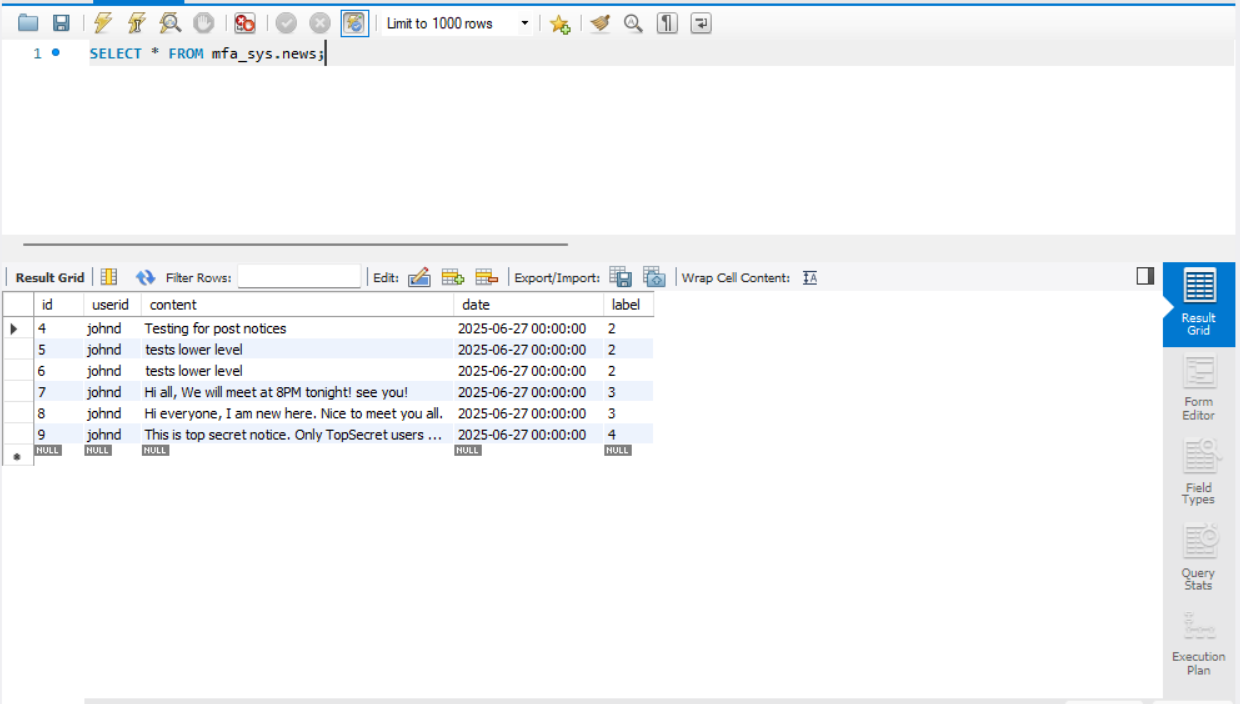
### UC\_POST - Đăng tin

#### Luồng chính



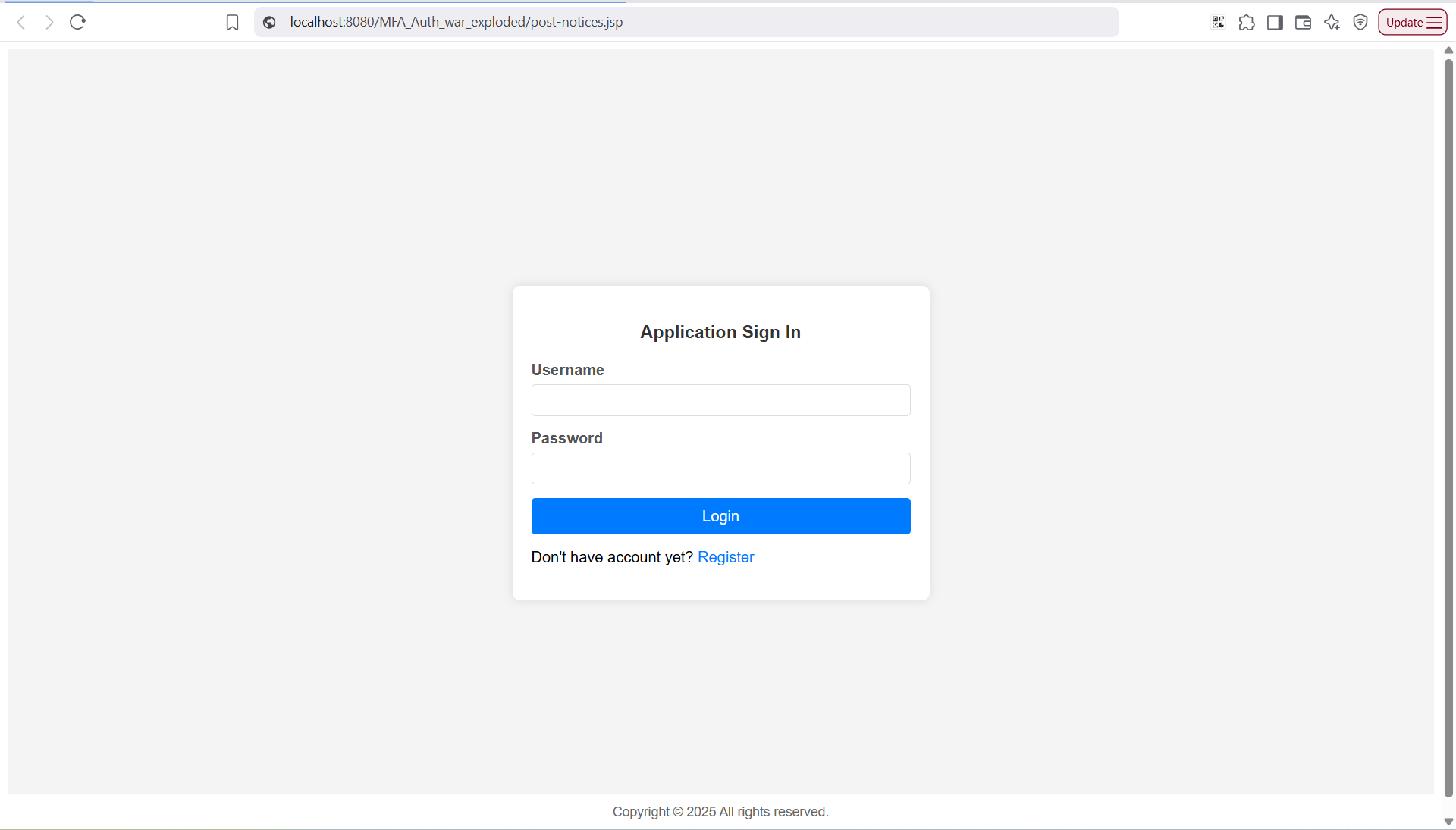


Insert vào database thành công notice có id bằng 8.

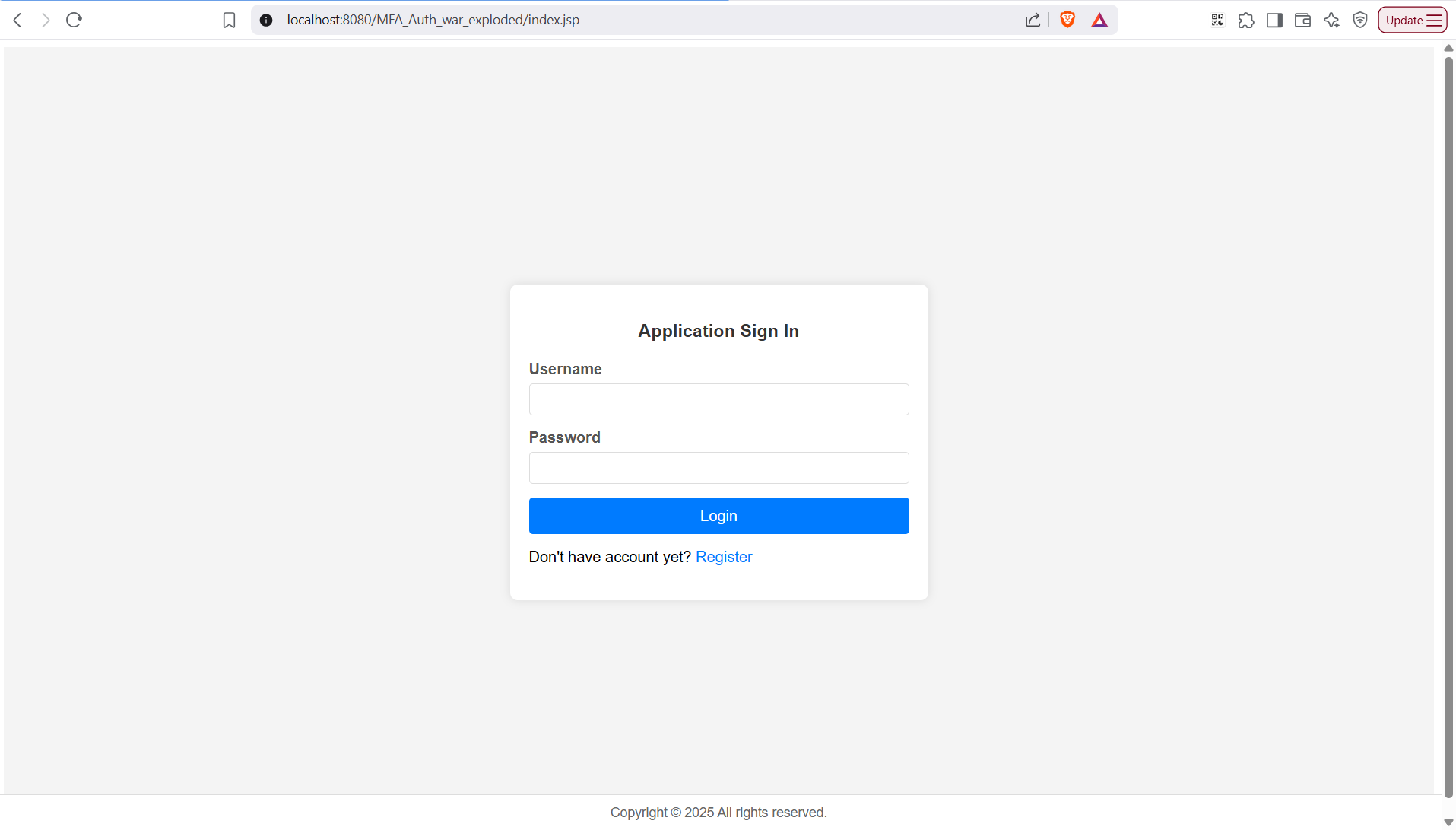


#### Luồng phụ 1 - Nếu người dùng chưa đăng nhập, chuyển hướng trình duyệt truy cập sang Trang chủ

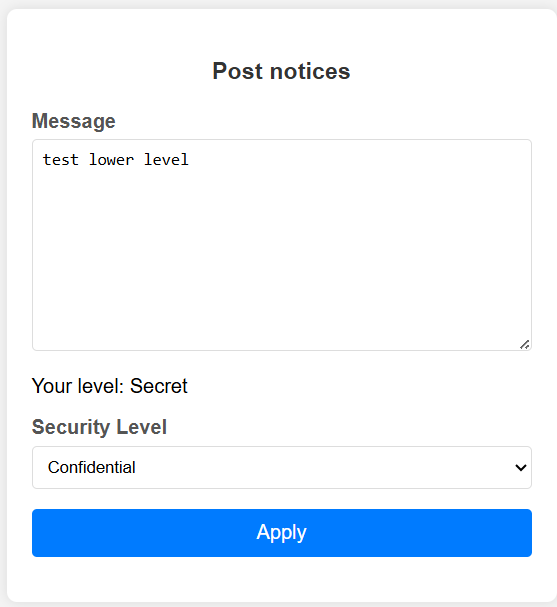
Cố gắng truy cập bằng URL khi chưa login

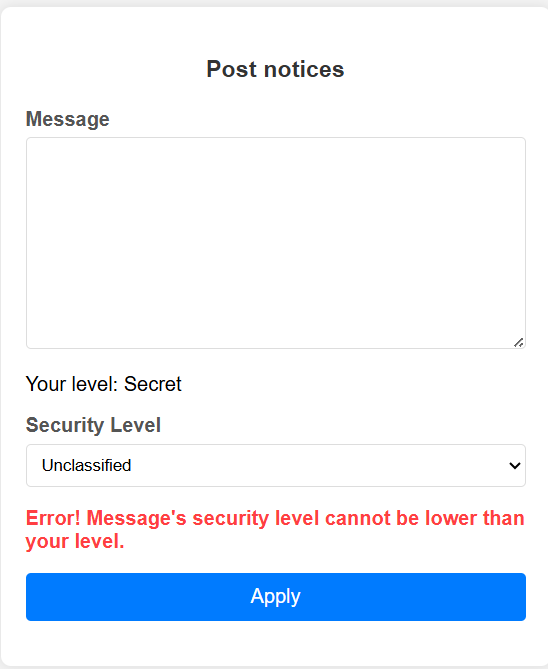


Redirect về trang login.



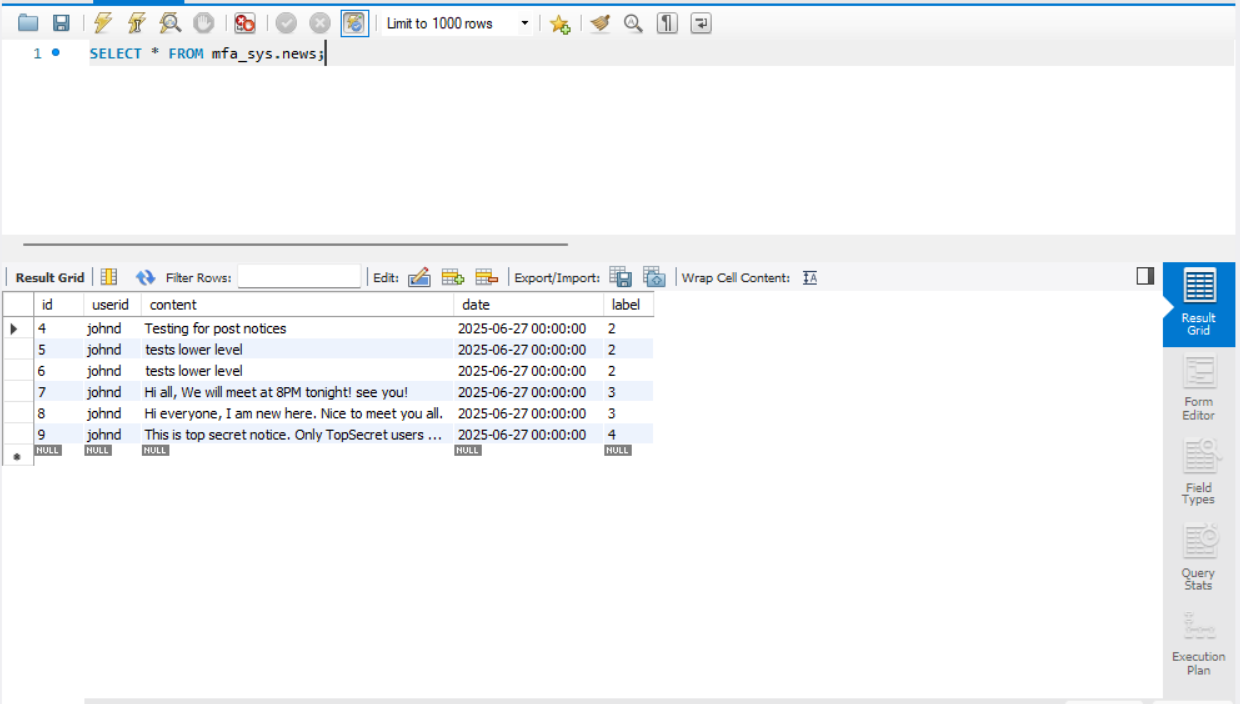
#### Luồng phụ 2 - Nếu nhãn bảo mật gán là không phù hợp theo mô hình Bell-Lapadula, chuyển hướng trình duyệt truy cập sang trang Báo lỗi



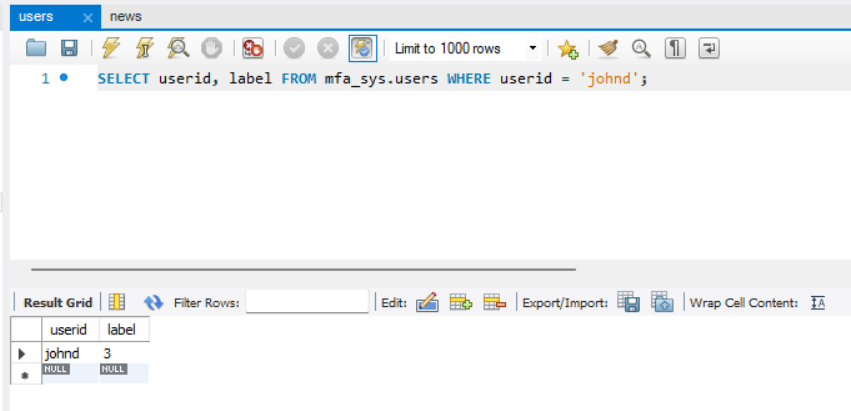


### UC\_READ – Đọc tin

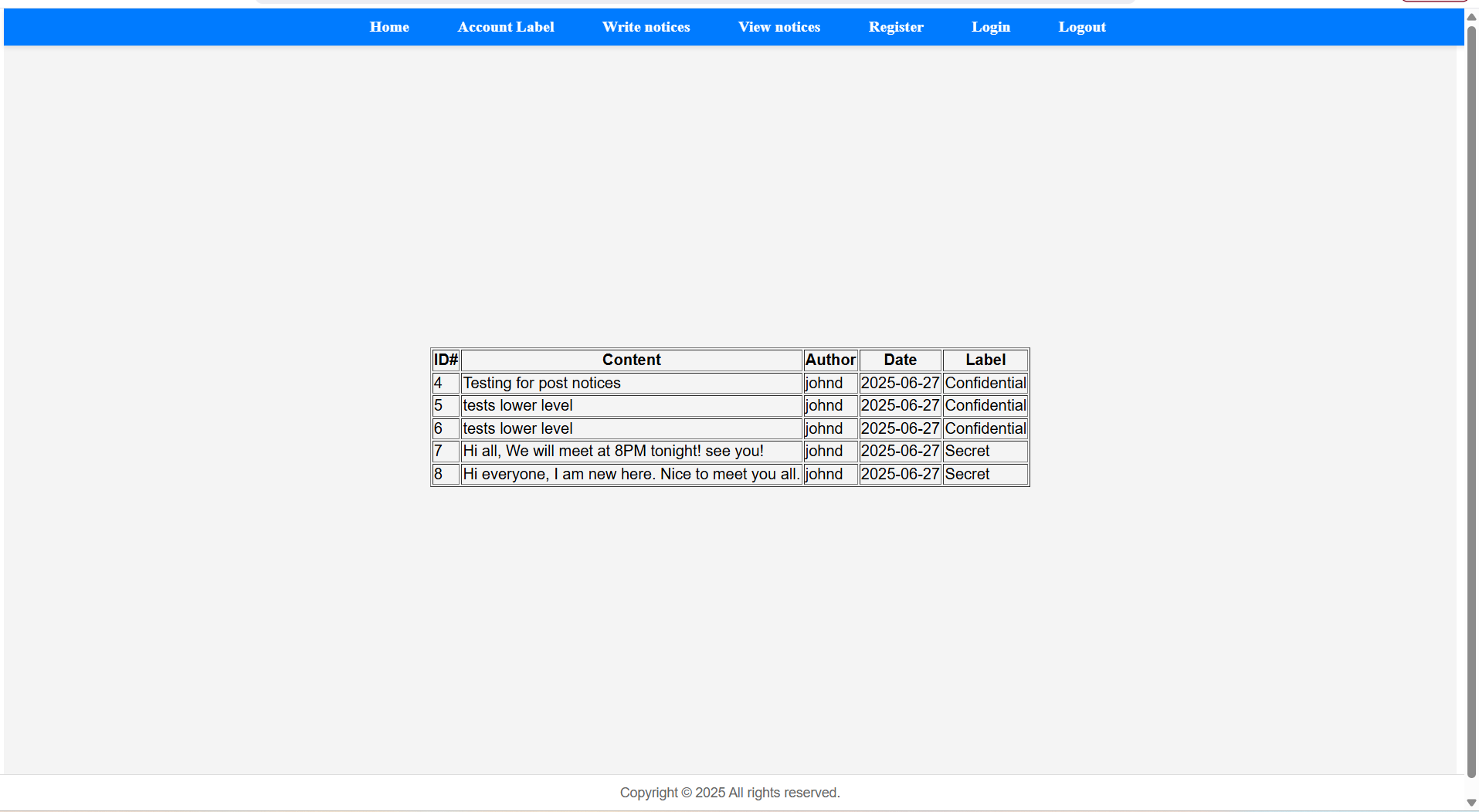
#### Luồng chính

Trong database đang có danh sách như sau:  


User có Security level là 3 – Secret

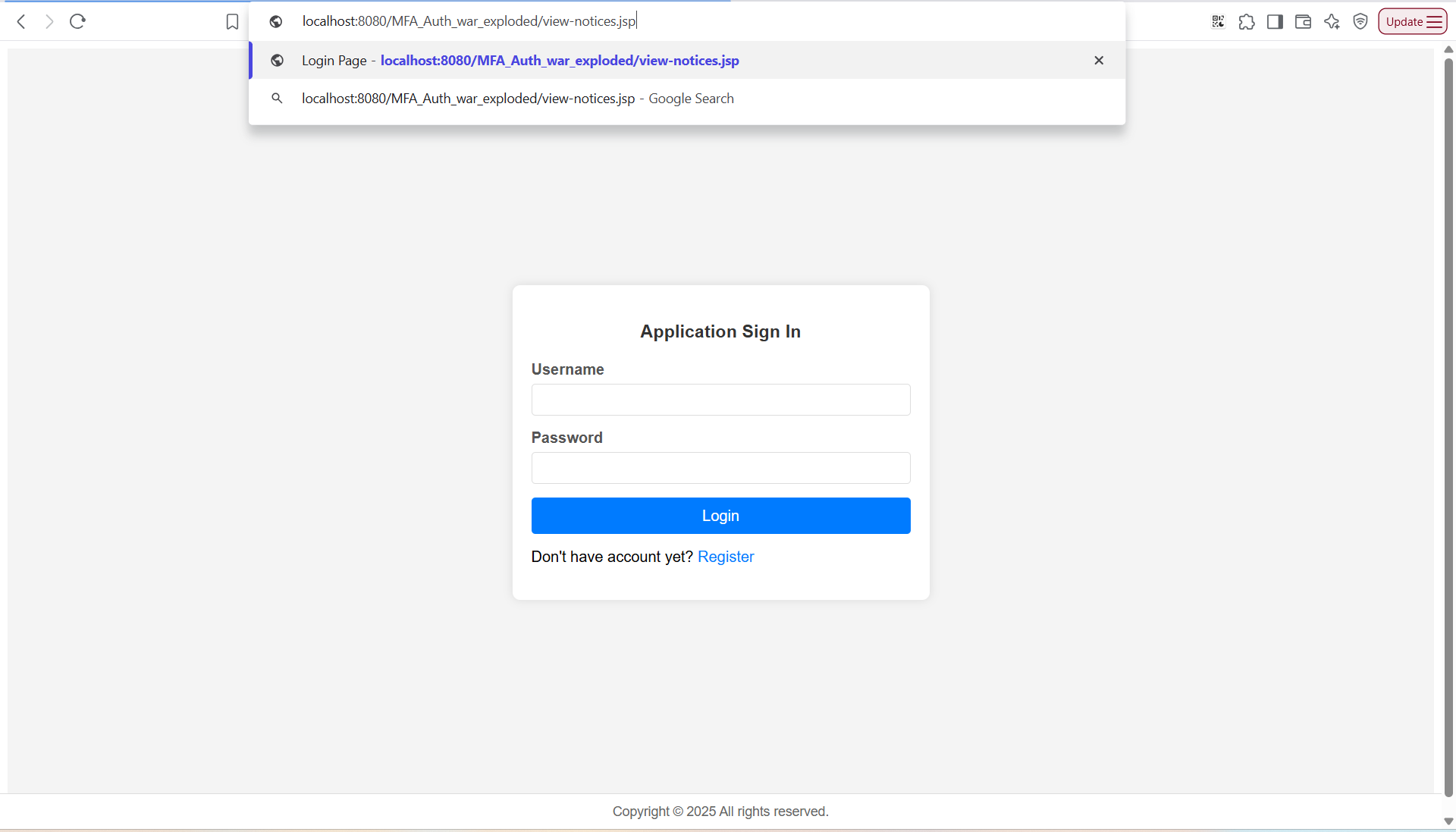


Như vậy, theo mô hình Bell-Lapadula, người dùng có tài khoản johnd sẽ có thể xem được tin đăng có nhãn bảo mật thấp hơn hoặc bằng nhãn bảo mật của người đó.

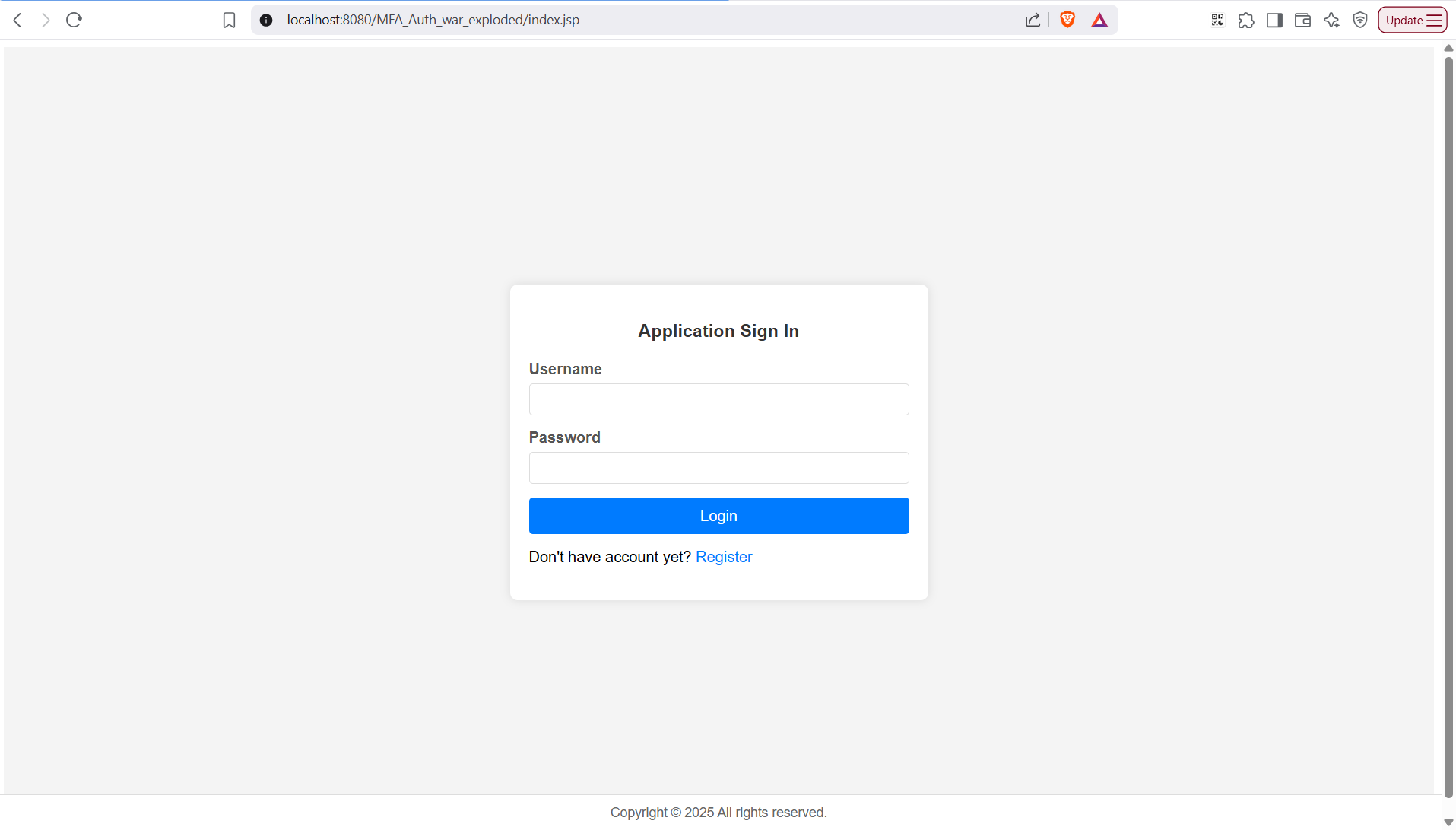


#### Luồng phụ 1 - Nếu người dùng chưa đăng nhập, chuyển hướng trình duyệt truy cập sang Trang chủ

Cố gắng truy cập bằng URL khi chưa login



Redirect qua trang login.



## Đề xuất giải pháp cải tiến

Mặc dù hệ thống đã có xác thực hai bước bao gồm mật khẩu và OTP nhưng yêu cầu dành cho mật khẩu chỉ mới là dài ít nhất 6 ký tự. Đề xuất đầu tiên là tăng yêu cầu về độ phức tạp của mật khẩu bằng cách:

* Tăng từ 6 ký tự tối thiểu lên 8 ký tự.
* Mật khẩu phải chứa ít nhất một ký tự thường, một ký tự in hoa, một ký tự đặc biệt và một số.

Hiện tại OTP Secret đang được sử dụng vô thời hạn, chưa có cơ chế để renew lại OTP secret và nó cũng đang được lưu trữ dạng plain text trong database. Đây cũng là một rủi ro tiềm tàng. Đề xuất việc xem xét rotate/renew lại OTP secret hoặc mã hóa OTP secret trước khi lưu trữ vào database.