| | |
|---|---|
| Class | IAW301 |
| Name | Trần Ngọc Anh |
| IC No. | HE151461 |
| Date & Time | 18/5/2022 |

# LAB 5
# XPATH Injection

## 1) XPATH Injection là gì ?

- Trước tiên ta phải đi tìm hiểu XML là gì? XML là một ngôn ngữ mô tả dữ liệu và trước kia nó thường được dùng để thay thế cho các hệ quản trị cơ sở dữ liệu hiện tại nhưng giờ thì không dùng nữa và dữ liệu được lưu dưới dạng XML. Nó dùng các thẻ tag để mô tả dữ liệu mà nó chứa.
- Nhưng về sau, người ta muốn XML không chỉ dùng để chứa dữ liệu nữa mà còn cho phép các ứng dụng khác truy xuất dữ liệu ra từ các file .xml nên từ đó XPath được tạo ra để phục vụ yêu cầu đó.

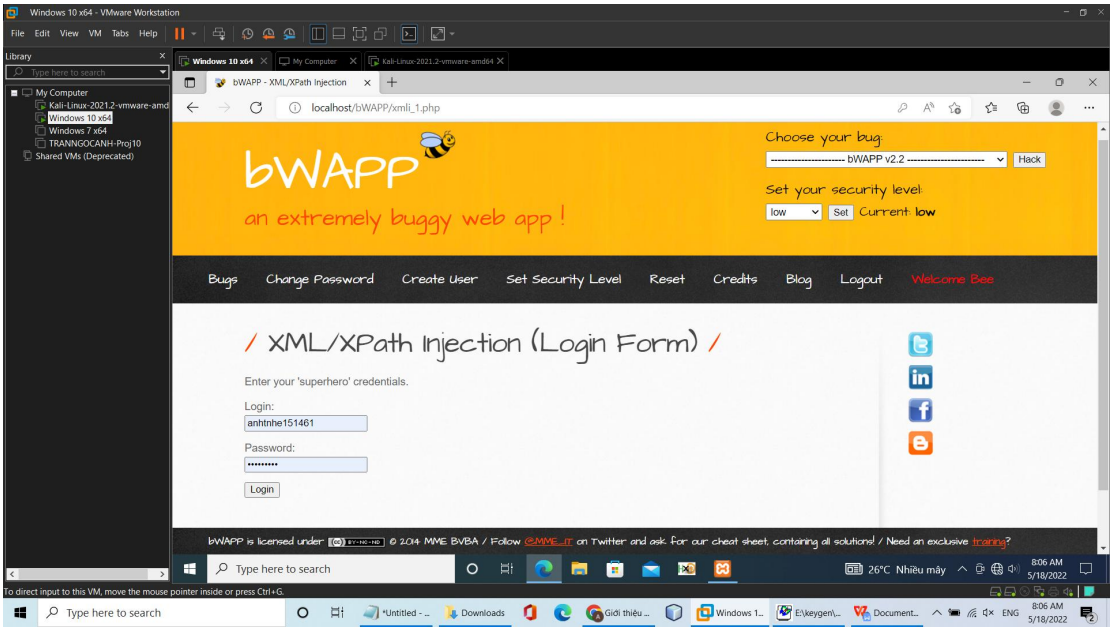
---> XPATH Injection là lợi dụng cơ chế trên để chèn các payload khai thác những thông tin mong muốn.

## 2) Tiến hành làm lab

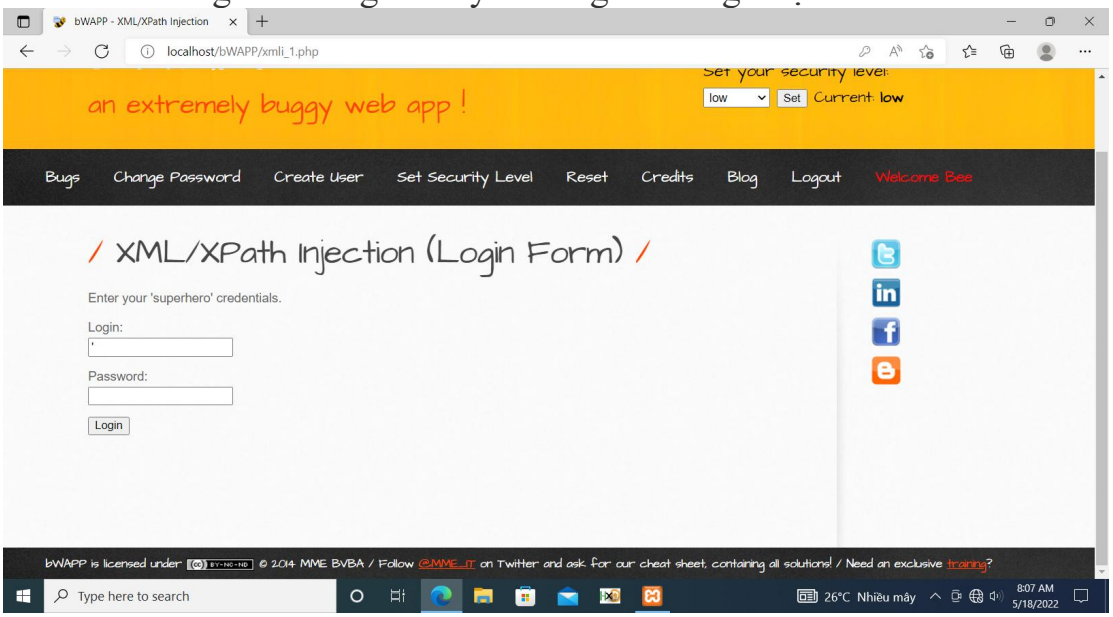
- Chọn chỗ set your security level là low. Click set.

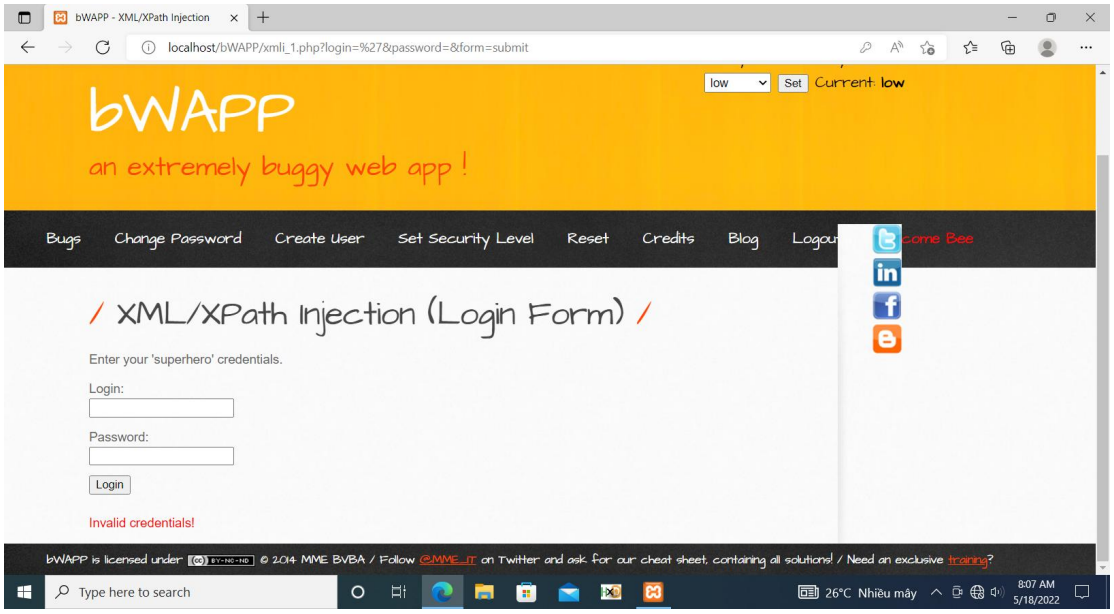
Chọn XML/Xpath Injection (Login Form). Click hack để tiến hành.

Chúng ta thấy giao diện lab Xpath injection là giao diện login form.

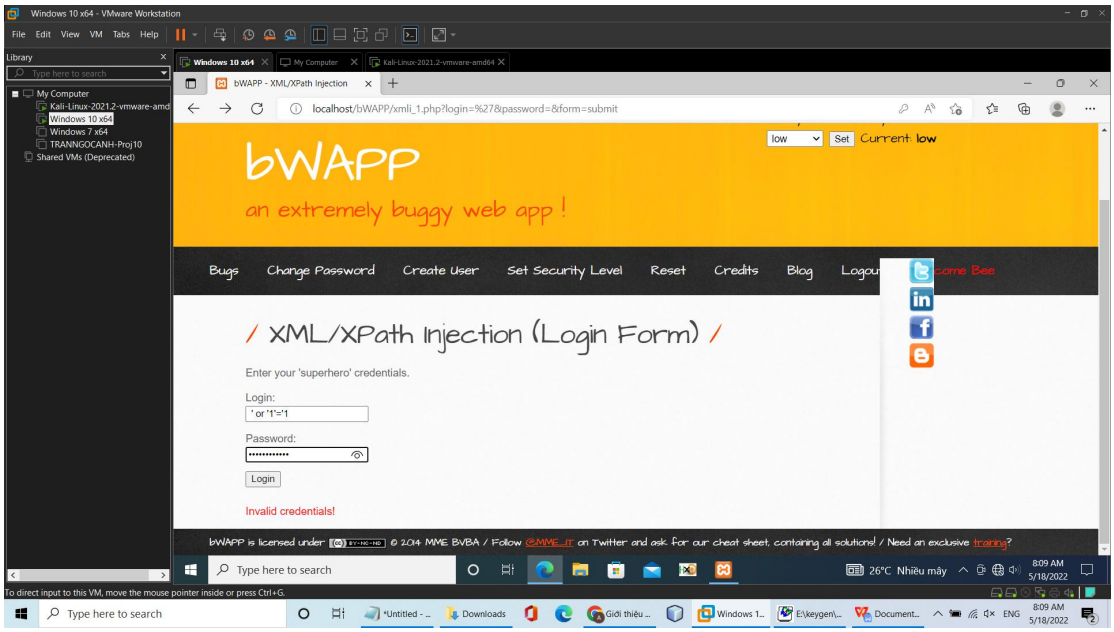


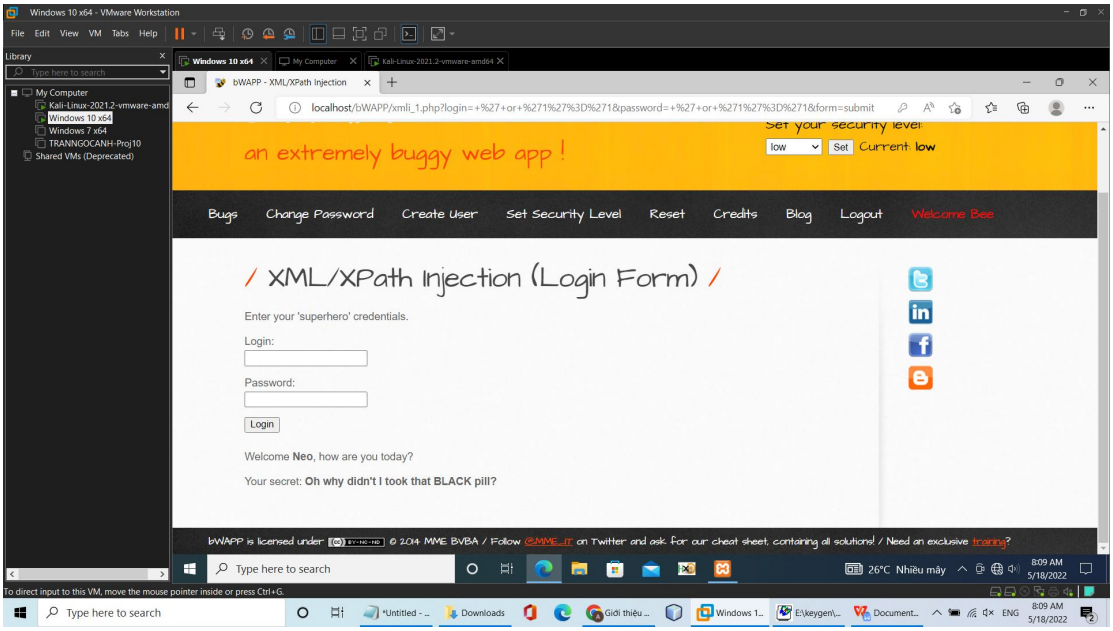

- Gõ ‘ click login. Chúng ta thấy báo login không được.






Chúng ta gõ : ' or '1'='1 (Cho cả user và pass và click login) . Chúng ta thấy bWAPP thông báo welcome Neo. Ta đã bypass login thành công với kỹ thuật Xpath injection.






## 3) Cách phòng ngừa lỗ  hổng XPATH Injection

- Xác thực đầu vào :

+ Quá trình xác thực nhằm xác minh xem loại input do người dùng gửi có hợp lệ hay không. Xác thực đầu vào đảm bảo đó là kiểu, độ dài, định dạng… được chấp nhận. Chỉ các giá trị qua được xác thực mới có thể được xử lý.

+ Ví dụ : Sử dụng biểu thức chính quy làm whitelist cho các dữ liệu có cấu trúc.

- Tham số hóa truy vấn :

+ Ví dụ : Không cộng chuỗi để tạo truy vấn SQL.

- Sử dụng Escaping :

+ Luôn sử dụng các hàm character-escaping cho input do user cung cấp, được cấp bởi mỗi hệ thống quản lý Cơ sở dữ liệu (DBMS). Nó sẽ giúp tránh các ký tự có thể dẫn đến lệnh SQL không mong muốn (ví dụ như dấu ‘ , ” , /, …).