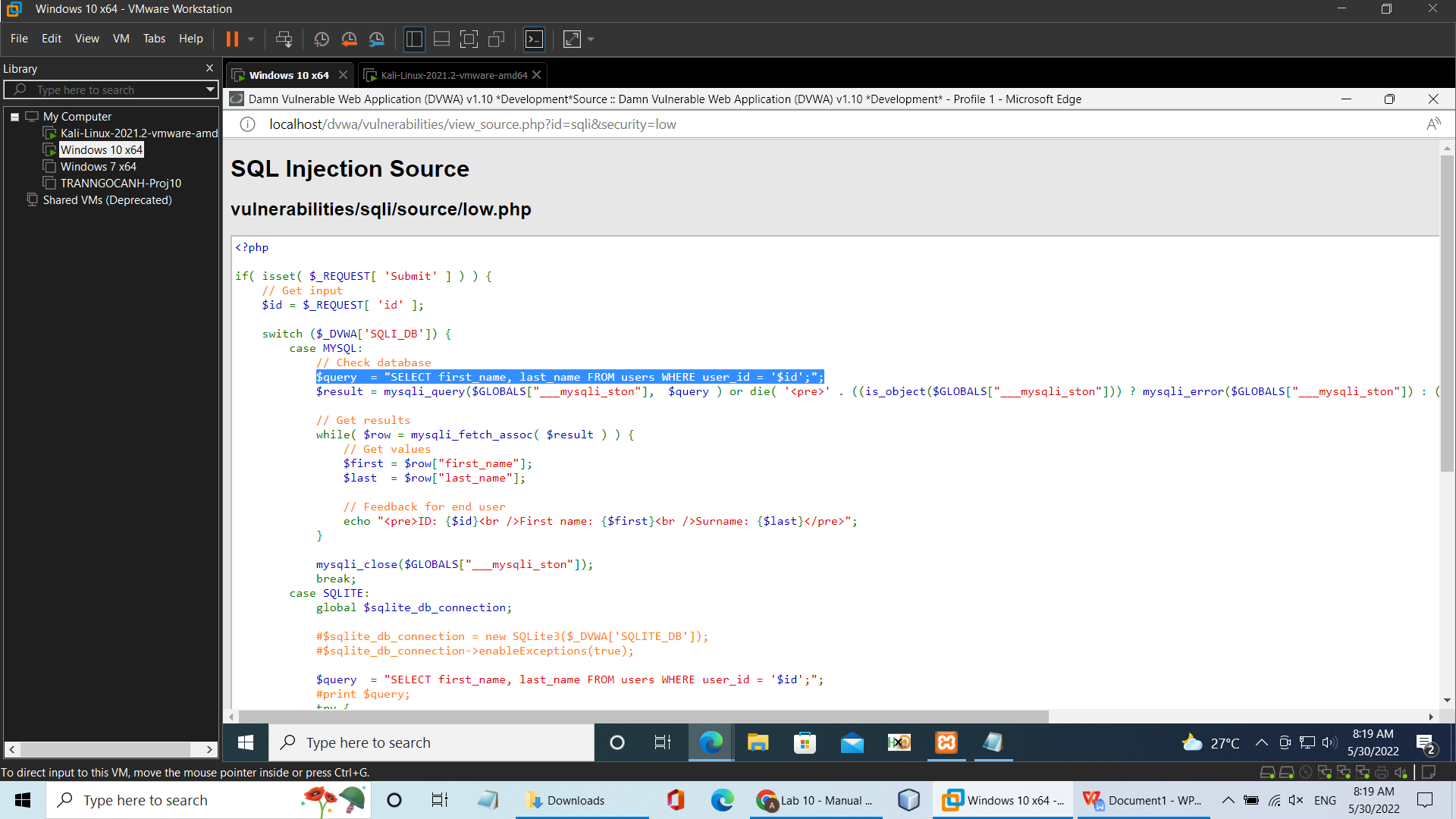
|  |  |
| --- | --- |
| Class | IAW301 |
| Name | Trần Ngọc Anh |
| IC No. | HE151461 |
| Date & Time | 30/5/2022 |

**LAB 10**

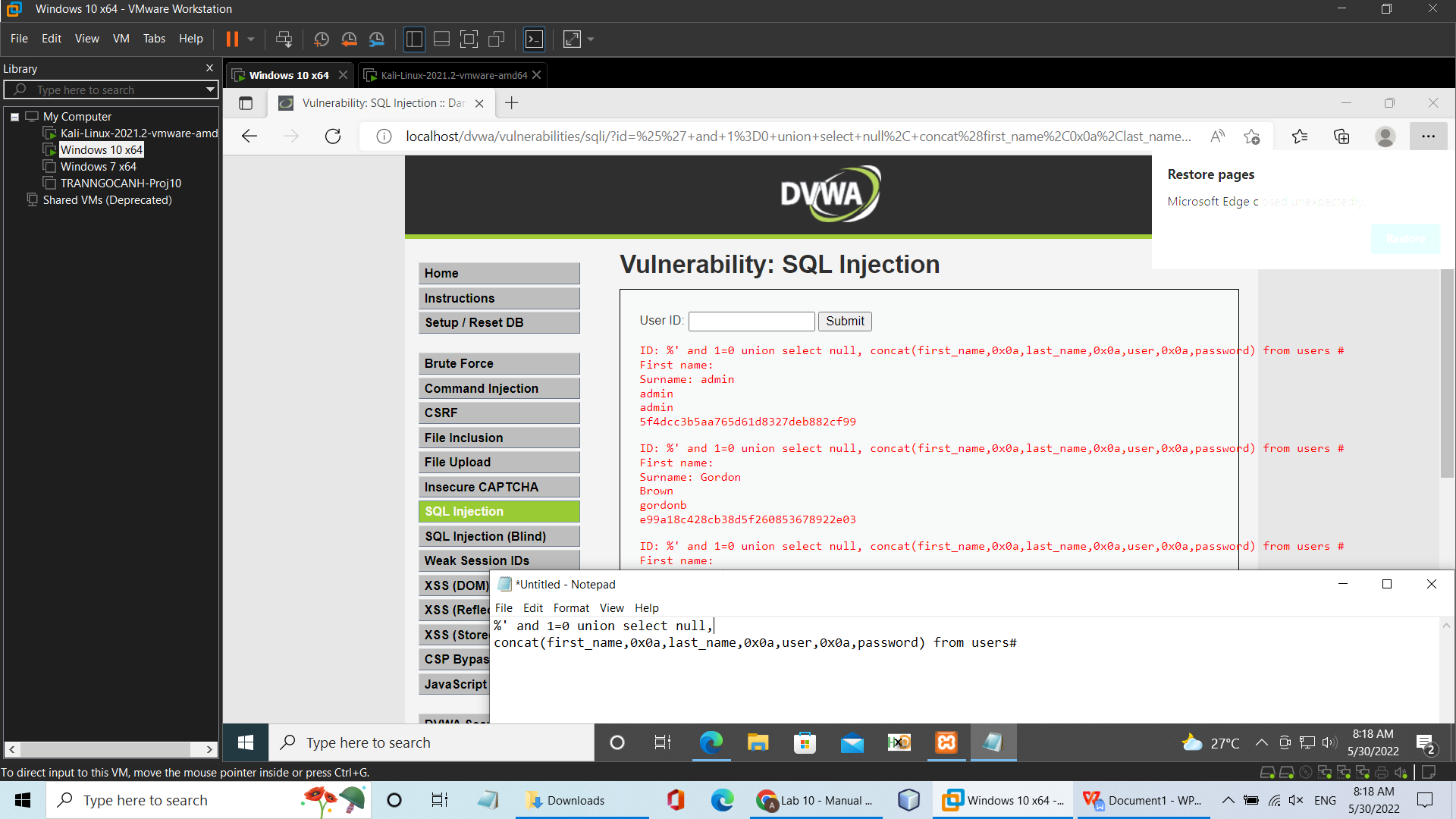
**Manual SQL Injection**

1. **Low:**

- Nhìn qua source code chúng ta thấy không có việc check id đầu vào do người dùng nhập mà đã nối id đó với câu truy vấn sql để thực thi.



- Vì vậy chúng ta chèn một đoạn mã để lấy các thông tin như là firstname, lastname, user và password có trong bảng users.



1. **Medium:**

- Ở mức medium chúng ta không thể inject trực tiếp do đầu vào đã được đưa vào một danh sách để chọn lựa. Vì vậy chúng ta sẽ dùng Burp Suite để bắt request và sửa thêm vào sau id một câu lệnh truy vấn với mục đích như mức Low và gửi đi.

