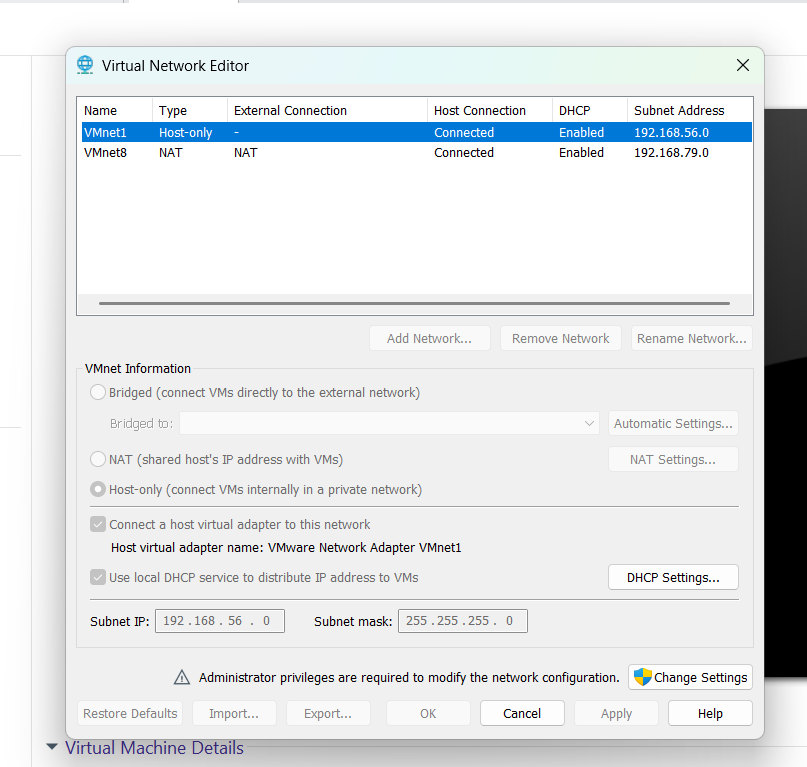
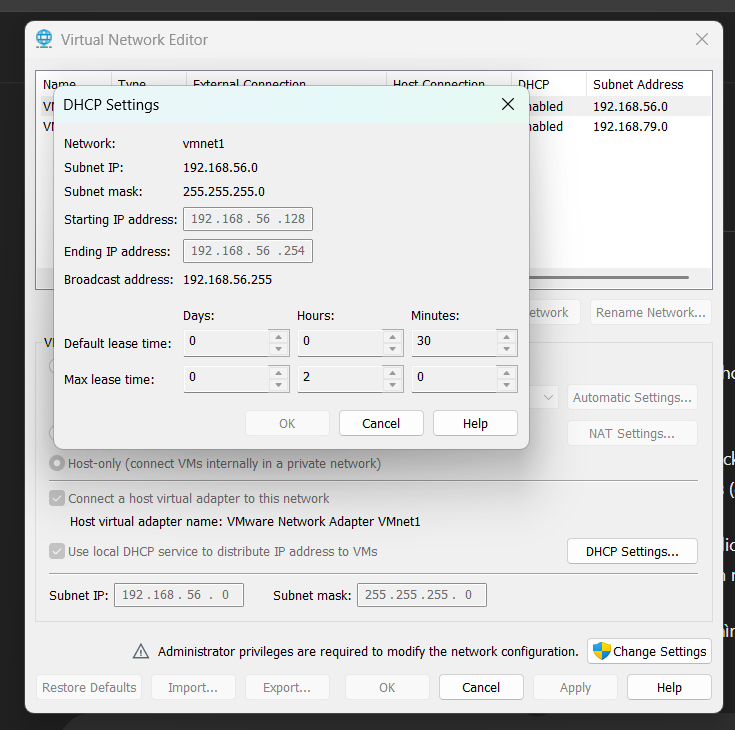
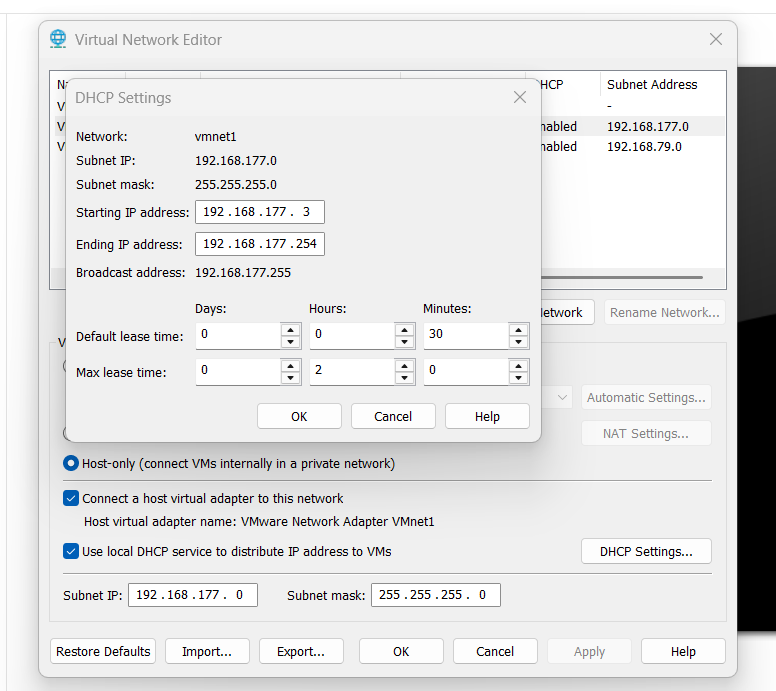
**TRẦN MINH HỢP - 1050080180 - 10\_ĐH\_CNPM3**

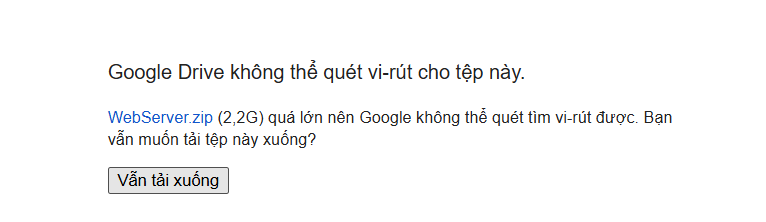
**BÁO CÁO BÀI THỰC HÀNH SỐ 8**

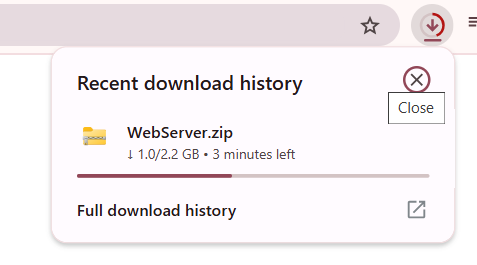
**KIỂM THỬ LỖ HỔNG SQL INJECTION**











Câu 1(3.5 điểm)

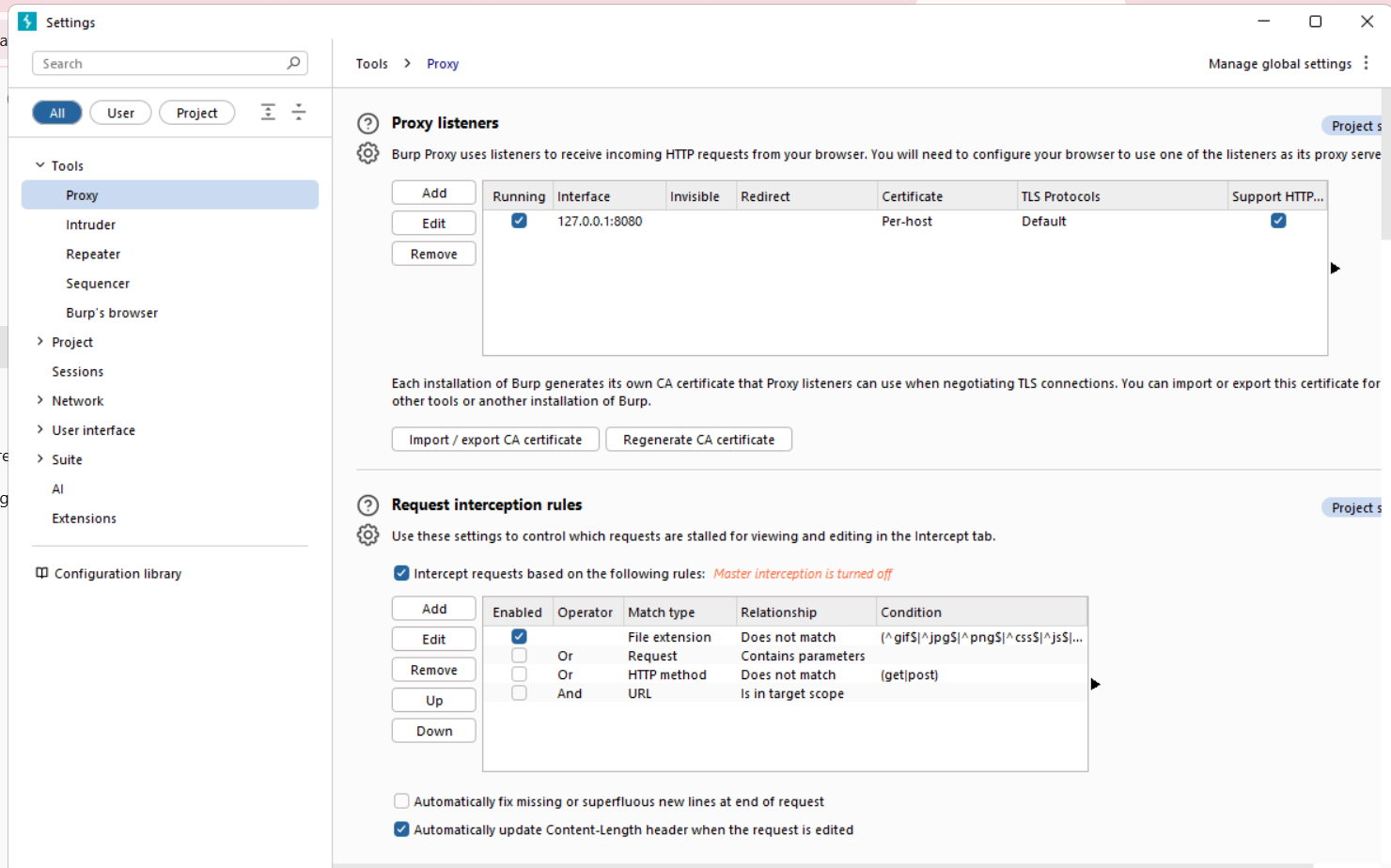
Kiểm thử lỗ hổng SQL Injection trên trang web <http://webvul.bkcs.vn/register.php>

- Xác định các tham số đầu vào và cách thức chúng được gửi tới server **(0.25 điểm)**

Bước 1: Cấu hình BurpSuite và trình duyệt

Mở BurpSuite .

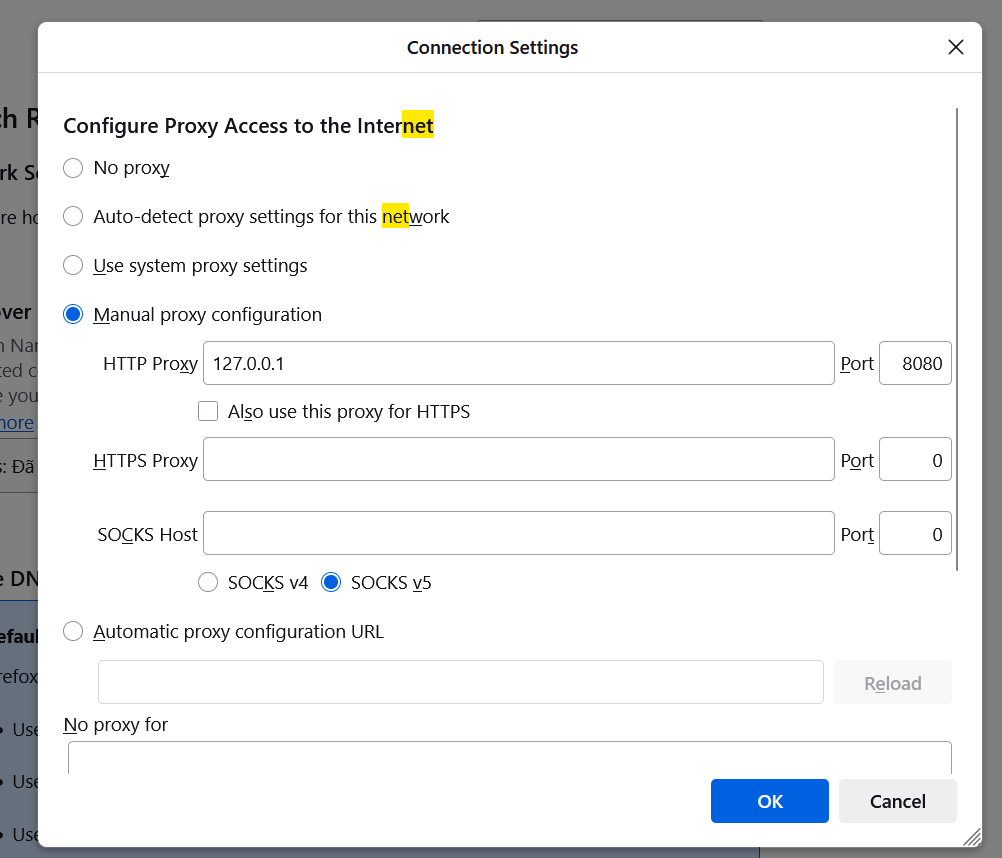
Vào tab Proxy → Options → đảm bảo đang bật proxy ở 127.0.0.1:8080.



Mở Firefox hoặc Chrome, vào Cài đặt proxy, cấu hình thủ công:

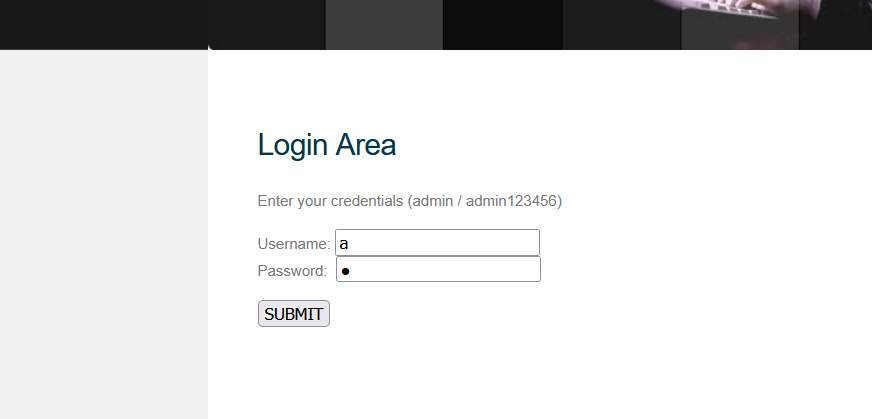
HTTP Proxy: 127.0.0.1

Port: 8080



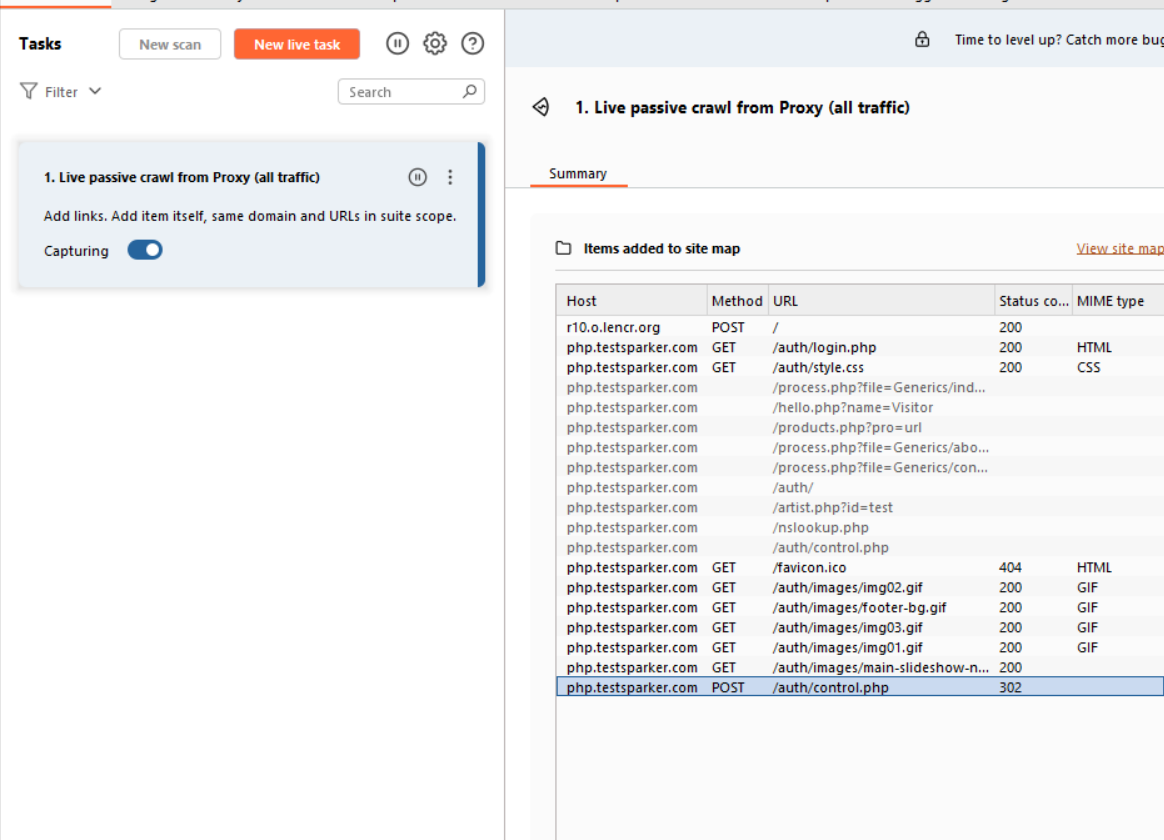
Bước 2: Truy cập <http://php.testsparker.com/auth/login.php>

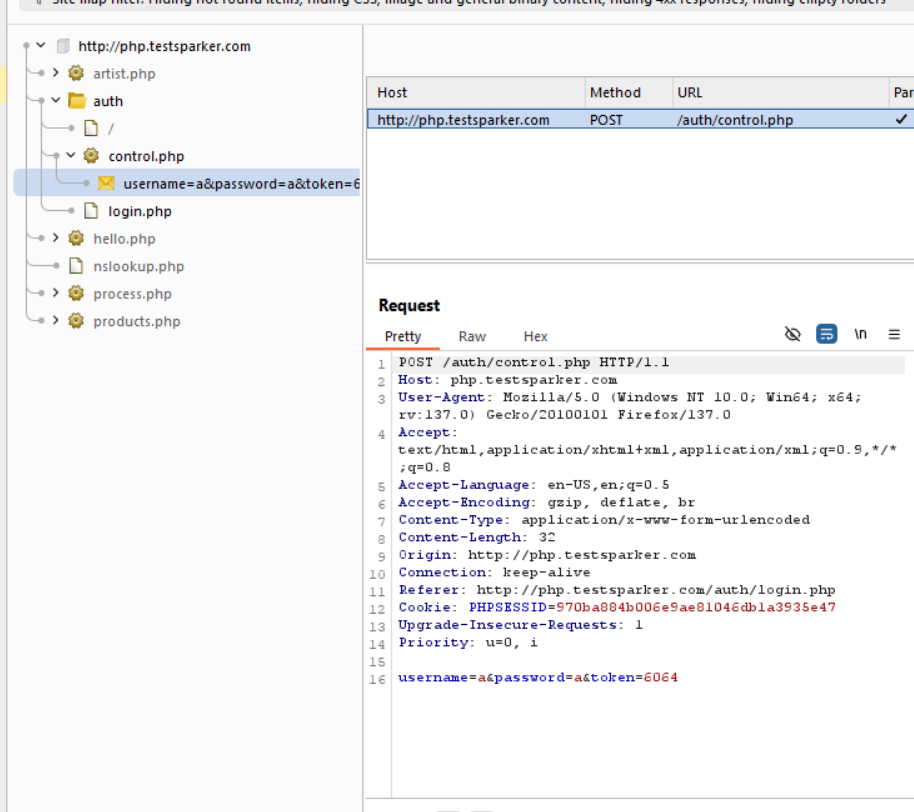
Đăng nhập 1 tài khoản bất kỳ:



Quan sát trong Burp:

Thấy HTTP POST request đến /auth/login.php





Kết luận:

Tham số đầu vào: username, password

Dữ liệu gửi bằng phương thức POST.

- Phân tích và phán đoán kiểu truy vấn **(0.25 điểm)**

**SELECT \* FROM users WHERE username = '$username' AND password = '$password';**

- Phân tích và phán đoán vị trí của các giá trị tham số đầu vào được sử dụng trong câu truy vấn **(0.5 điểm)**

- Xác định mức độ ảnh hưởng của lỗ hổng trên mỗi giá trị đầu vào **(2.5 điểm)**

*Lưu ý:*

*- Nói rõ mục đích sử dụng các giá trị kiểm thử*

*- Giải thích rõ các phán đoán và suy luận từ kết quả khi sử dụng mỗi giá trị kiểm thử*

# Câu 2 (3.5 điểm)

Kiểm thử lỗ hổng SQL Injection trên trang web <http://webvul.bkcs.vn/login.php>

- Xác định các tham số đầu vào và cách thức chúng được gửi tới server **(0.25 điểm)**

- Phân tích và phán đoán kiểu truy vấn, phân tích và phán đoán vị trí của các tham số đầu vào được sử dụng trong câu truy vấn **(0.25 điểm)**

- Xác định mức độ ảnh hưởng của lỗ hổng trên mỗi giá trị đầu vào **(3 điểm)**

*Lưu ý:*

*- Nói rõ mục đích sử dụng các giá trị kiểm thử*

*- Giải thích rõ các phán đoán và suy luận từ kết quả khi sử dụng mỗi giá trị kiểm thử*

# Câu 3 (3 điểm)

Kiểm thử lỗ hổng SQL Injection trên trang web <http://webvul.bkcs.vn/index.php>

- Xác định các tham số đầu vào và cách thức chúng được gửi tới server **(0.25 điểm)**

- Phân tích và phán đoán kiểu truy vấn, vị trí của các tham số đầu vào được sử dụng trong câu truy vấn **(0.25 điểm)**

- Xác định mức độ ảnh hưởng của lỗ hổng trên mỗi giá trị đầu vào **(2.5 điểm)**

*Lưu ý:*

*- Nói rõ mục đích sử dụng các giá trị kiểm thử*

**-** *Giải thích rõ các phán đoán và suy luận từ kết quả khi sử dụng mỗi giá trị kiểm thử*