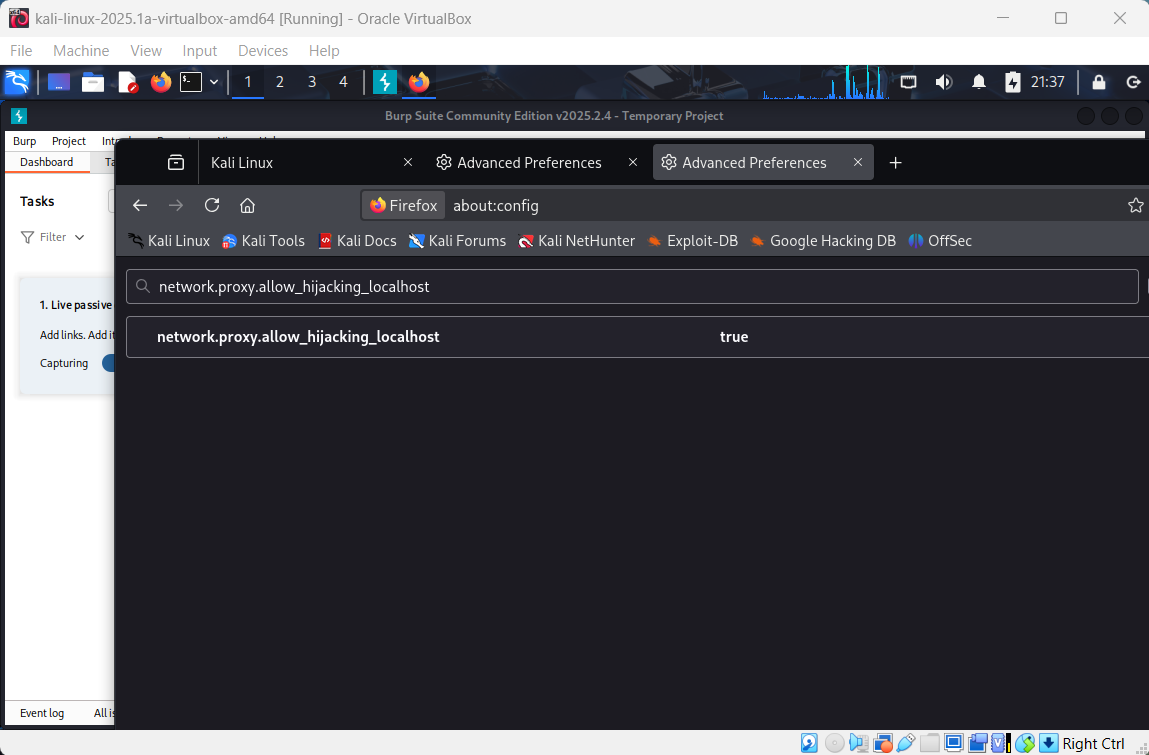
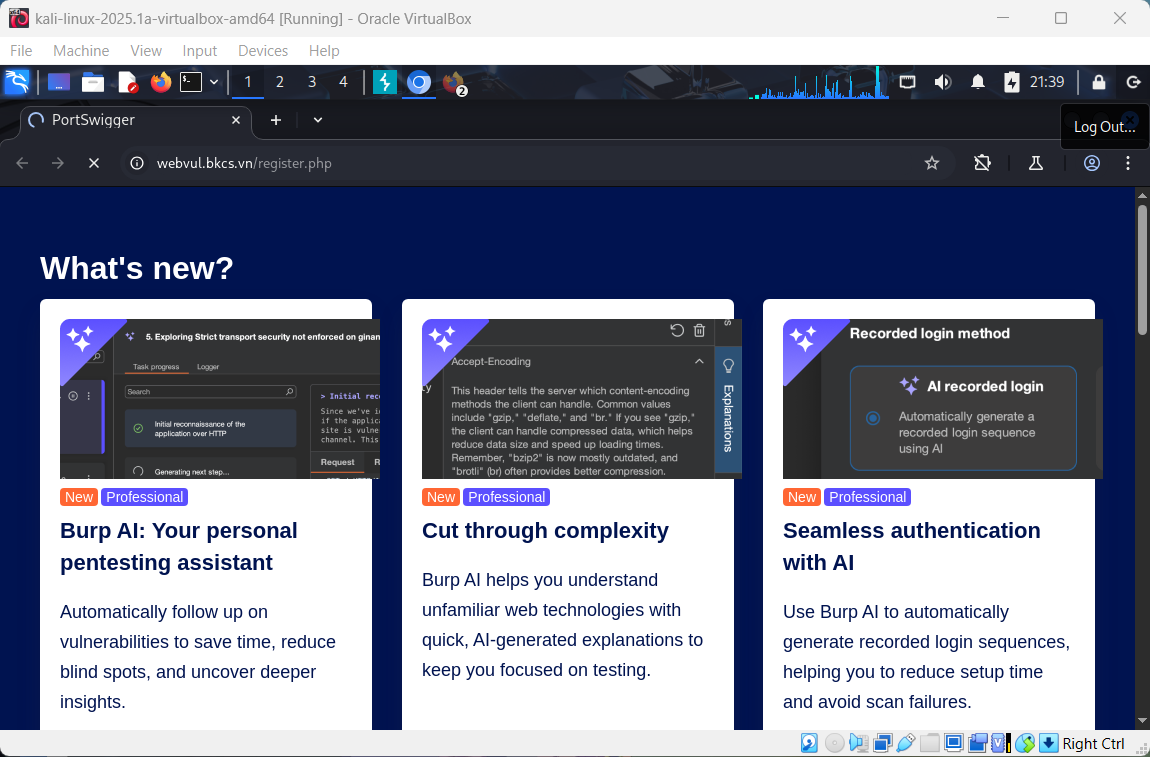
**BÁO CÁO BÀI THỰC HÀNH SỐ 8**

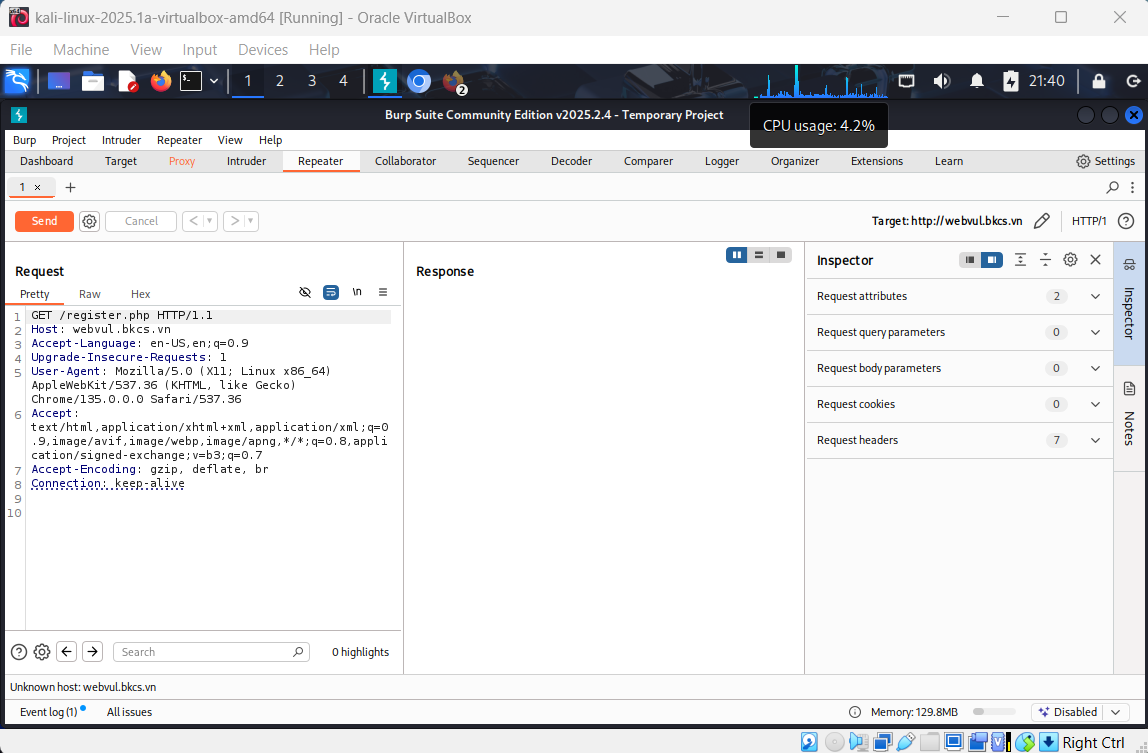
**KIỂM THỬ LỖ HỔNG SQL INJECTION**

**Họ và tên:** Trương Đan Huy

**Câu 1:**

****

****

****

**Trang web:** http://webvul.bkcs.vn/register.php

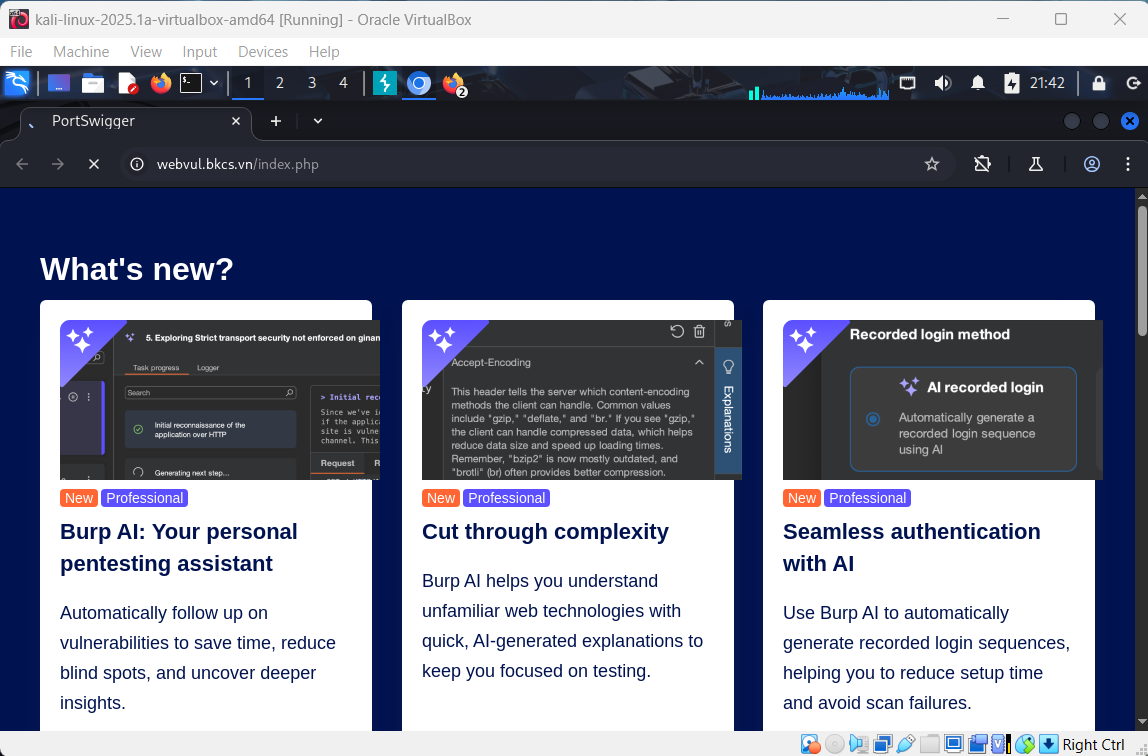
**Xác định các tham số đầu vào**

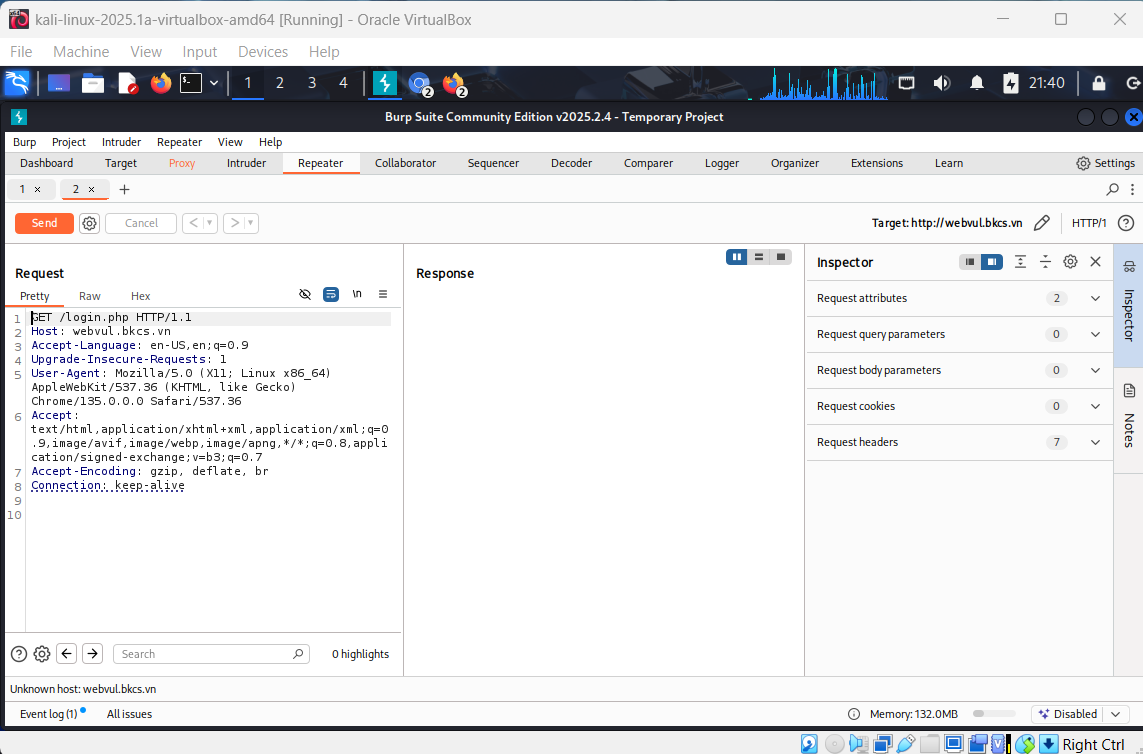
* Các tham số đầu vào: username, password, confirm\_password, email
* Phương thức gửi: POST

**Vị trí giá trị đầu vào trong truy vấn (0.5 điểm)**

* username, password, email được chèn trực tiếp vào câu truy vấn trên
* Nếu không có lọc đầu vào, có thể thực hiện tấn công SQL Injection.

**Câu 2:**

****

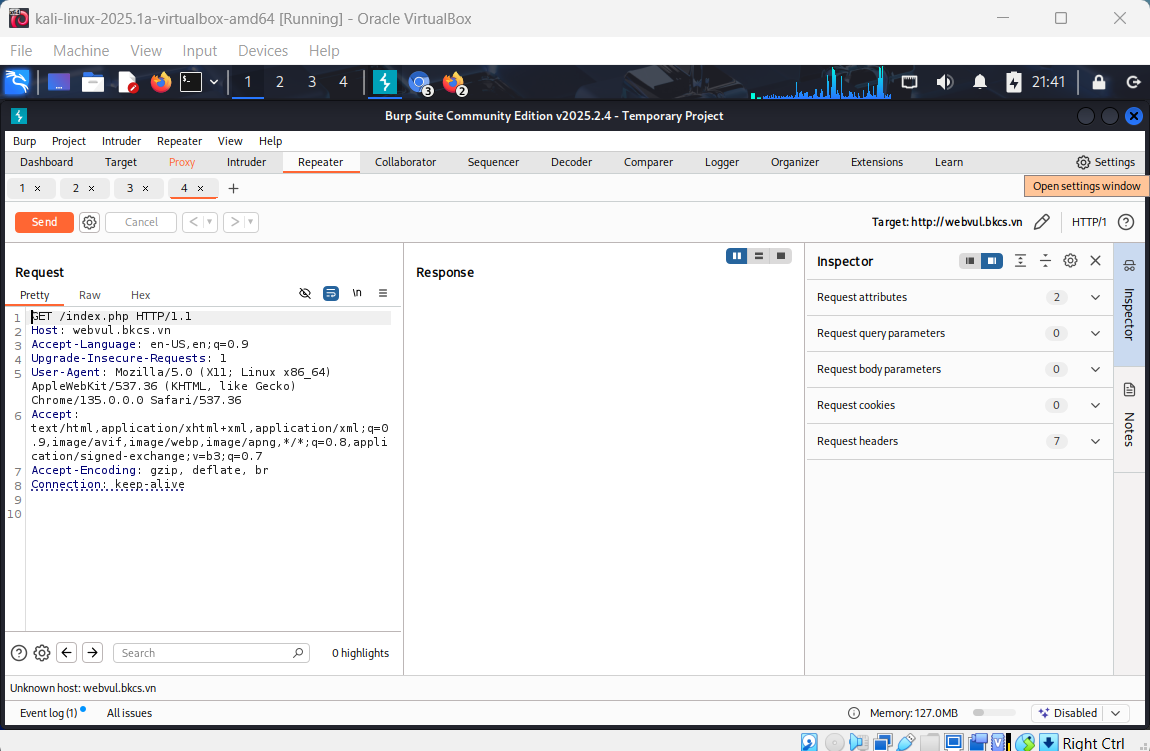
****

**Trang web:** http://webvul.bkcs.vn/login.php

**Xác định tham số, phương thức**

* Tham số: username, password
* Phương thức: POST

**Câu 3:**

****

**Trang web:** http://webvul.bkcs.vn/index.php

**Tham số và cách gửi**

* Trang chủ có thể sử dụng tham số truy vấn qua URL, ví dụ: ?id=1
* Gửi bằng: GET