**BÁO CÁO BÀI THỰC HÀNH SỐ 8**

**KIỂM THỬ LỖ HỔNG SQL INJECTION**

***Họ và tên: Trần Quốc Bảo***

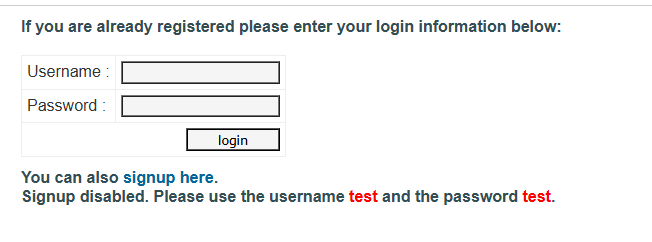
***Yêu cầu kết quả thực hành:***

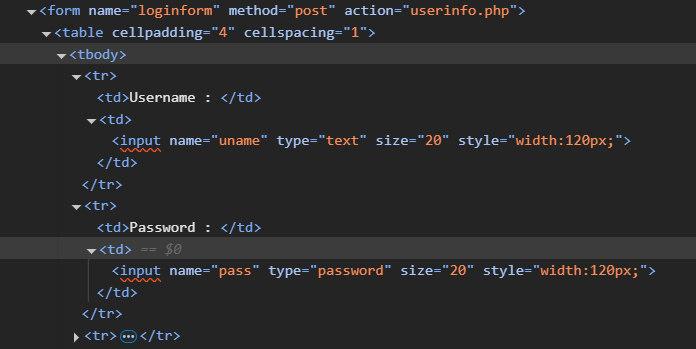
Báo cáo kết quả thực hành  có tên theo định dạng HoTenSV\_MSSV\_Lab08.docx

**Câu 1*(3.5 điểm)***

Kiểm thử lỗ hổng SQL Injection trên trang web [login page](http://testphp.vulnweb.com/login.php)

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



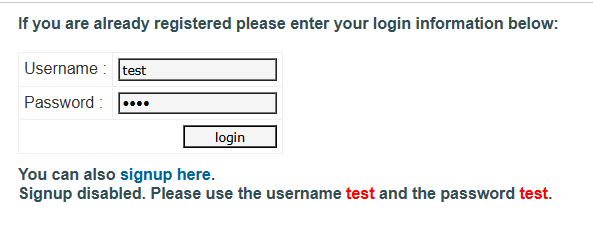


Ta có thể thấy tham số đầu vào là uname và pass. Phương thức gửi tới server là phương thưc POST

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

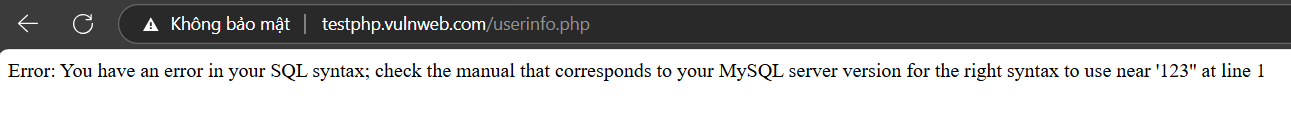
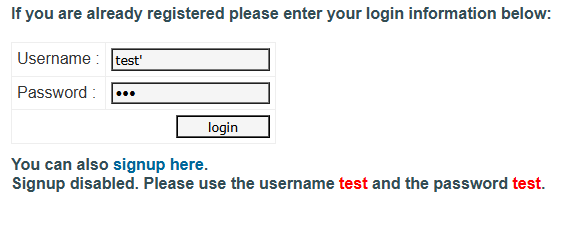
Trang login.php được dùng để xác thực thông tin đăng nhập của người dùng. Dựa trên chức năng này, server sẽ thực hiện truy vấn SQL để kiểm tra thông tin đăng nhập. Truy vấn SELECT.

Phản hồi thành công cho thấy server đang so sánh dữ liệu đầu vào với cơ sở dữ liệu, thường thông qua truy vấn SELECT.

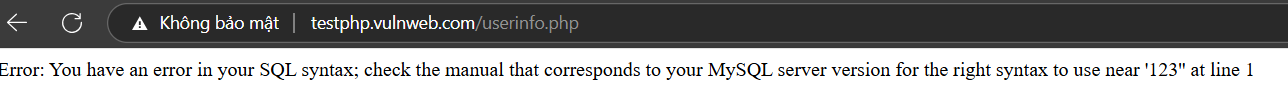


Phản hồi thành công cho thấy server đang so sánh dữ liệu đầu vào với cơ sở dữ liệu, thường thông qua truy vấn SELECT.

Kiểm tra với ký tự đặc biệt

Kết quả:



* Lỗi cú pháp SQL xác nhận kiểu truy vấn là SELECT và trang có khả năng bị SQL Injection
* 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)**

Tham số uname, pass vị trí nằm trong mệnh đề WHERE

* 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*