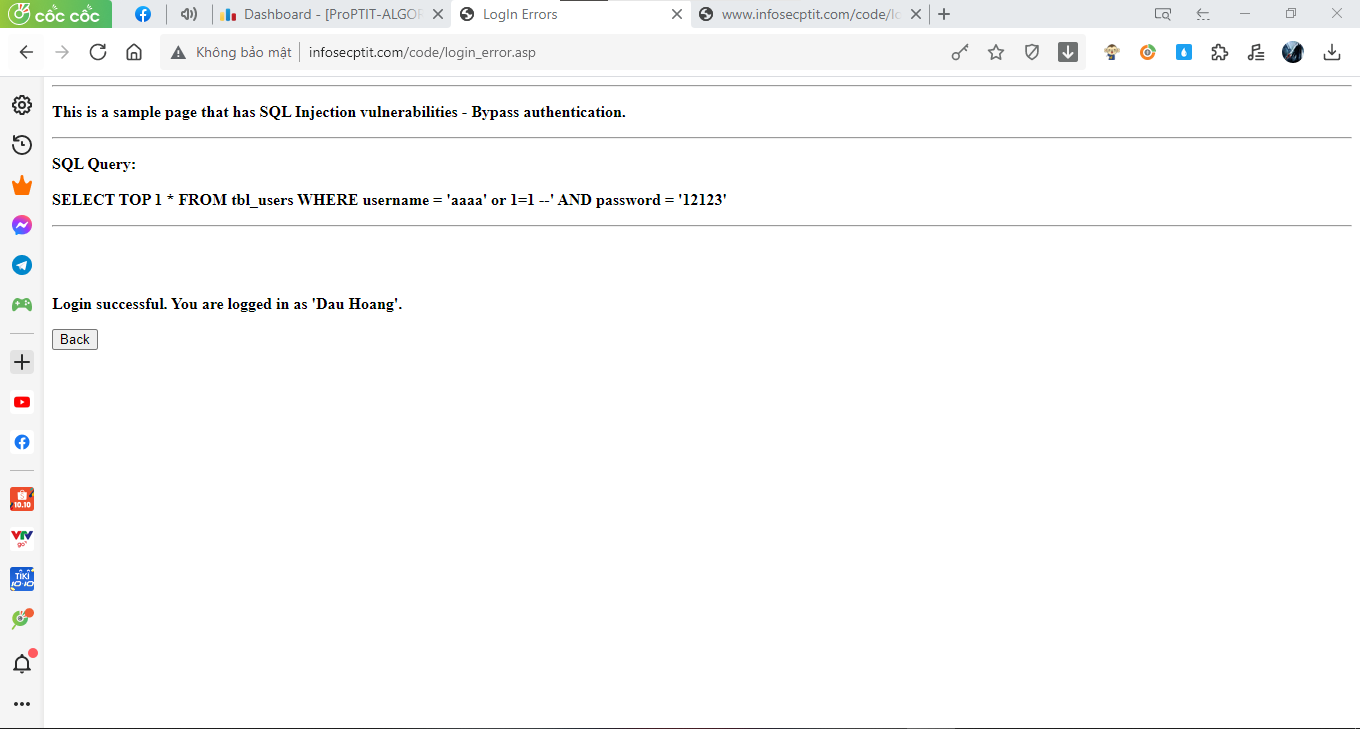
**Nguyễn Minh Phương – B19DCAT141**

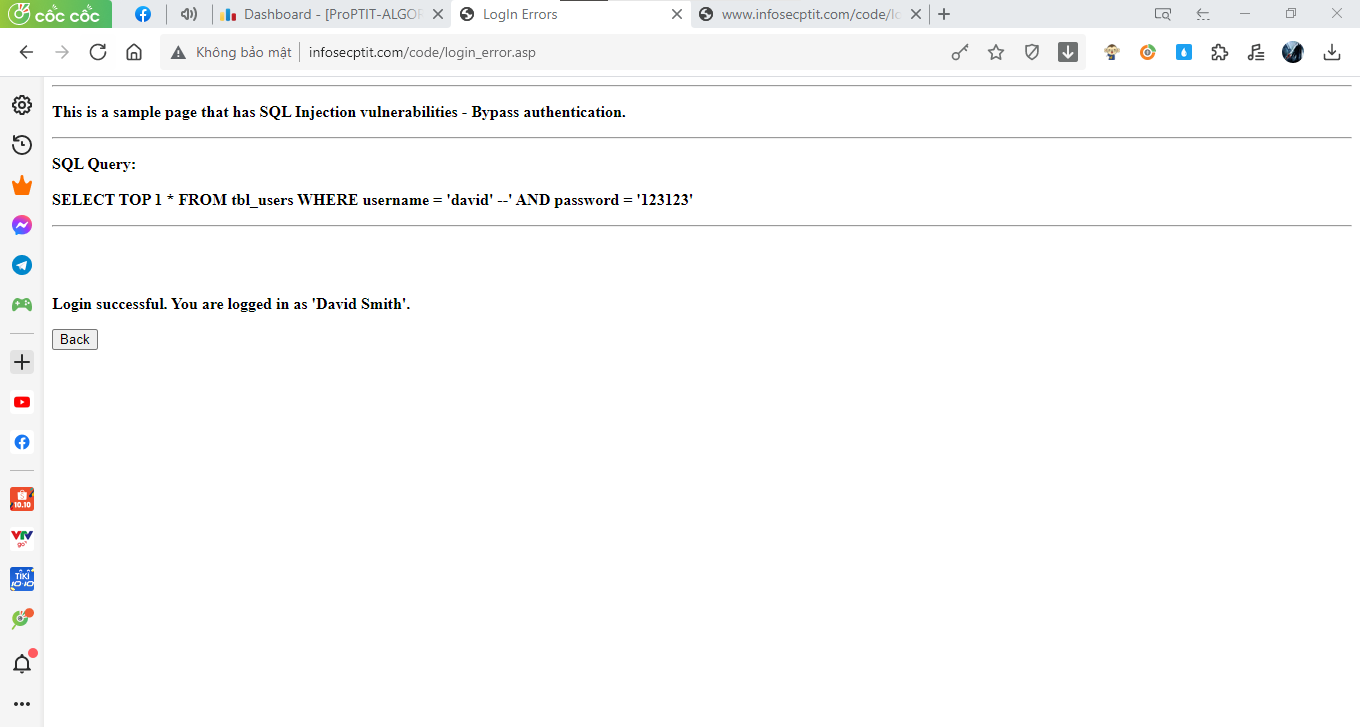
**Báo cáo bài Thực hành số 2**

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

* Đăng nhập tự do :

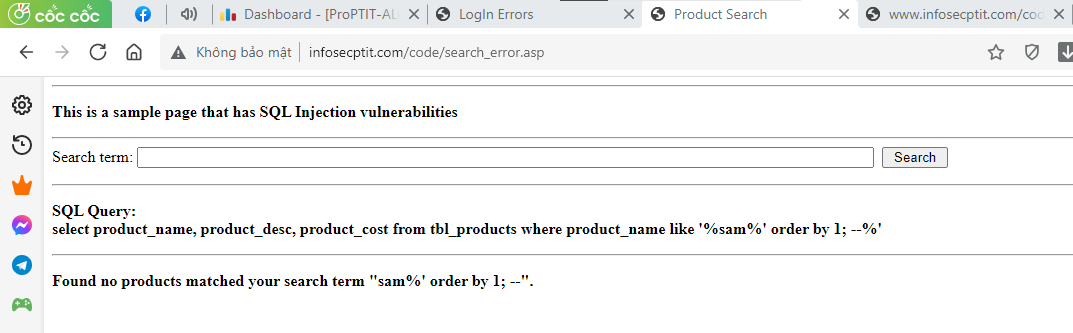


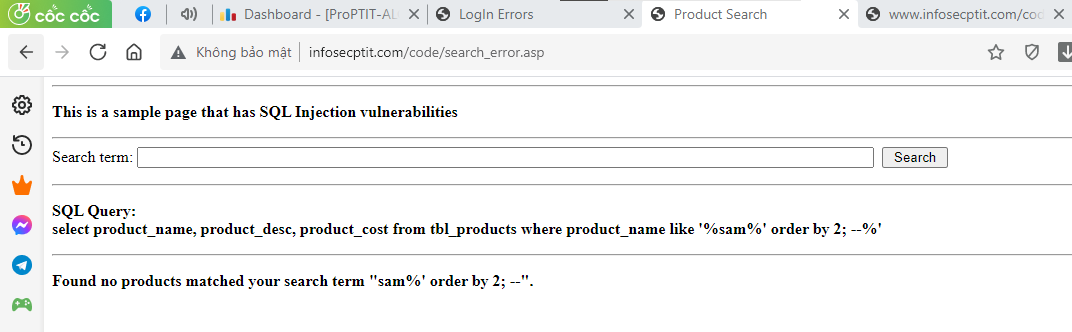
* Đăng nhập vào tài khoản một người dùng chỉ định:

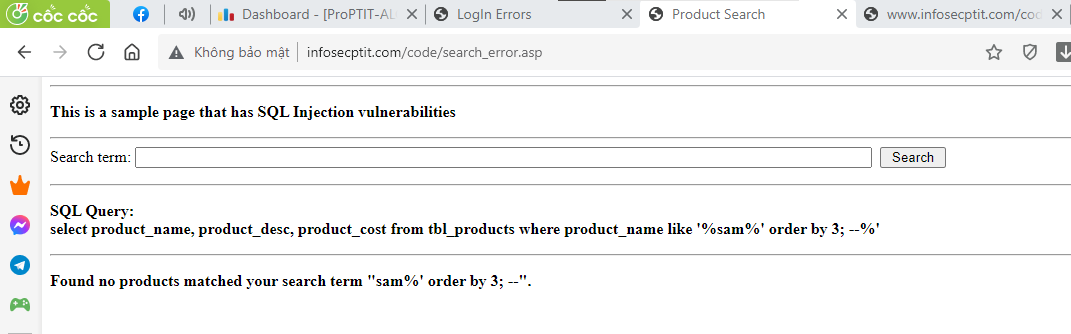


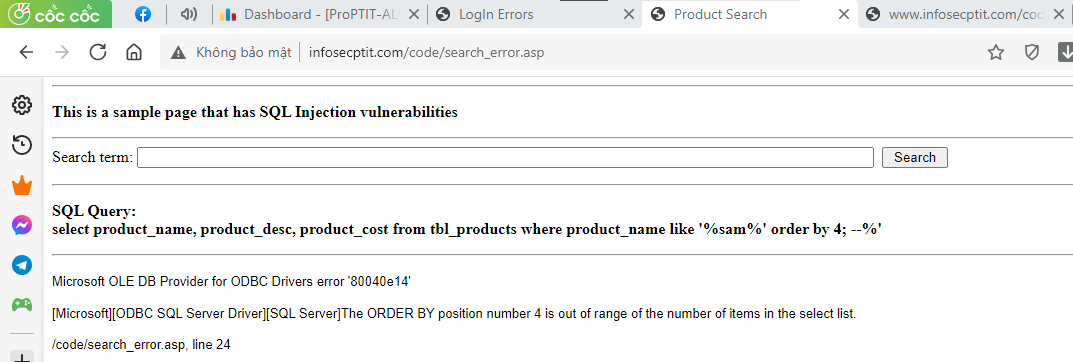
* Phân tích câu lệnh SQL: *SELECT TOP 1 \* FROM tbl\_users WHERE username = ’david’ --‘ AND password = ‘abc’*
* Trả về 1 giá trị đầu tiên trong bảng tbl\_users thỏa mãn điều kiện sau WHERE.
* Đầu vào *username* là *david’ --* thì dấu ‘ dùng để ngắt lệnh, dấu -- có tác dụng biến đoạn mã sau nó thành *comment* nên câu lệnh chỉ thực hiện so sánh điều kiện *username* và bỏ qua điều kiện *password.*
* Tài khoản người dùng ***david*** đã tồn tại nên sẽ ***Login successful***.

1. **Trích xuất dữ liệu từ CSDL:**

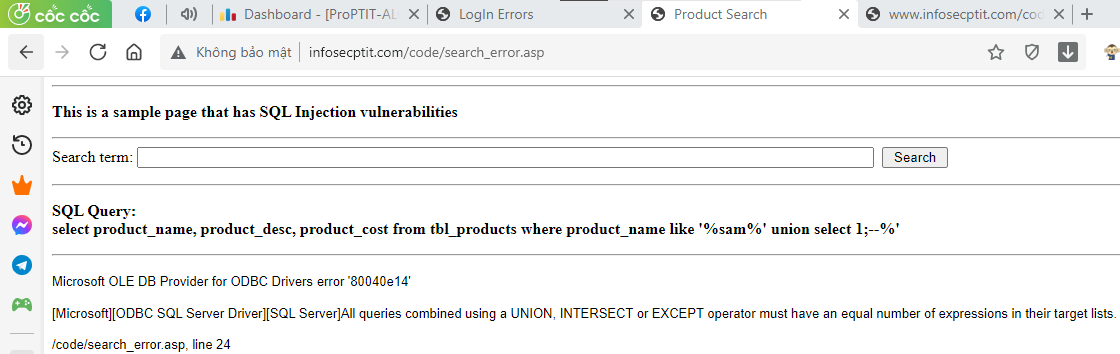
****

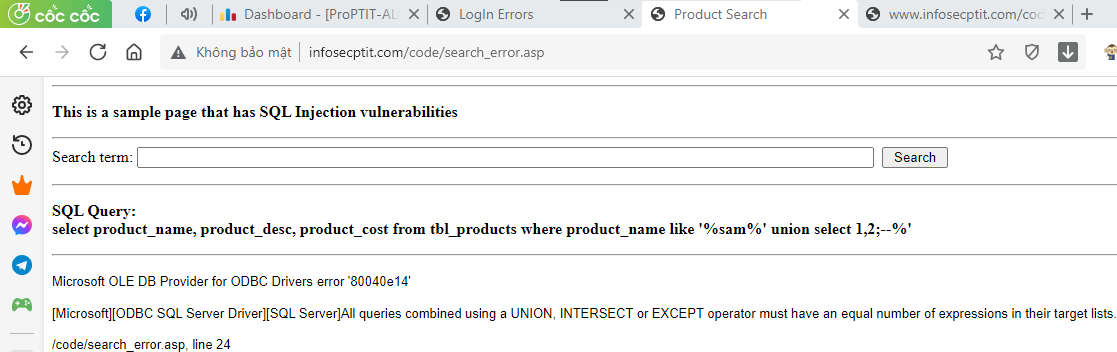
****

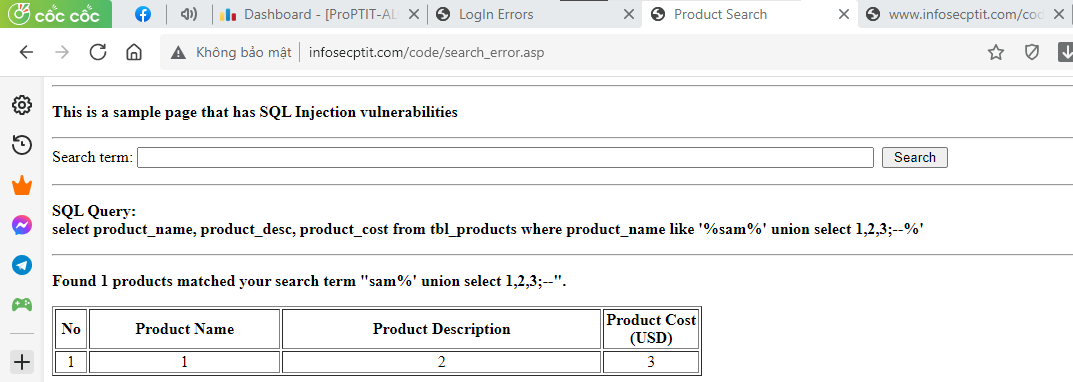
****

****

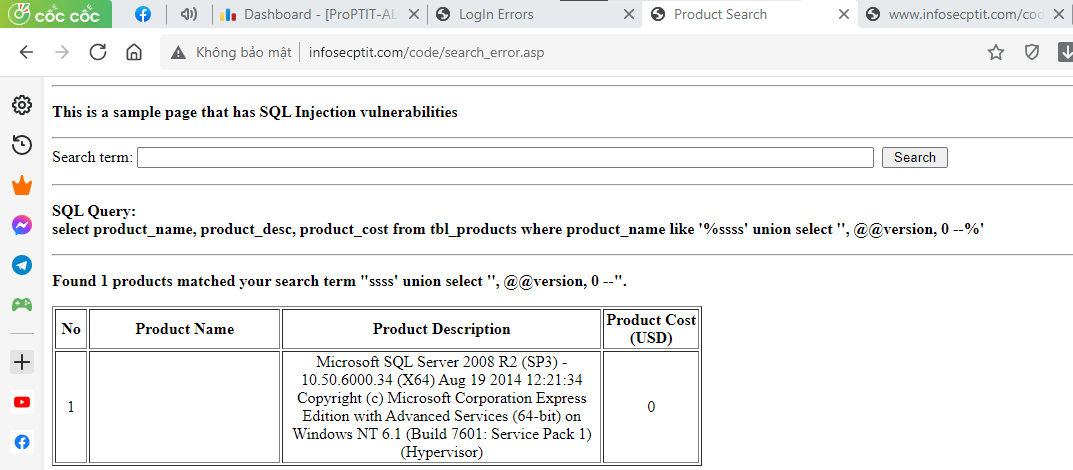
* Có 3 trường trong câu truy vấn của trang.

****

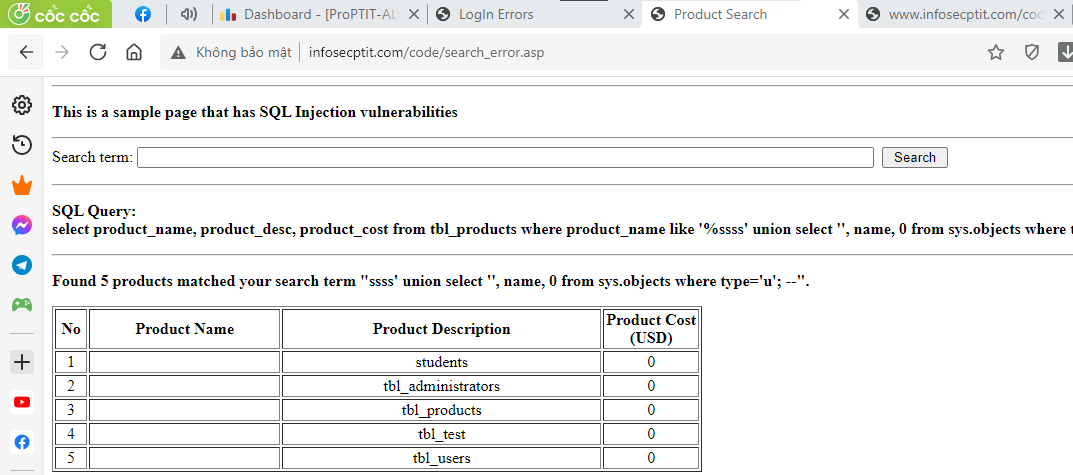
****

****

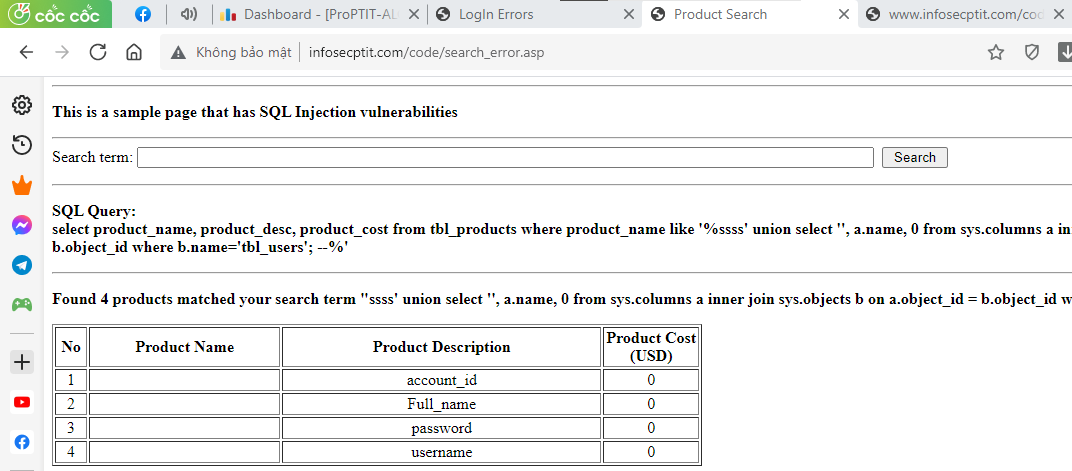
* Có 3 trường trong câu truy vấn của trang.
* Hiển thị thông tin hệ quản trị CSDL và hệ điều hành:



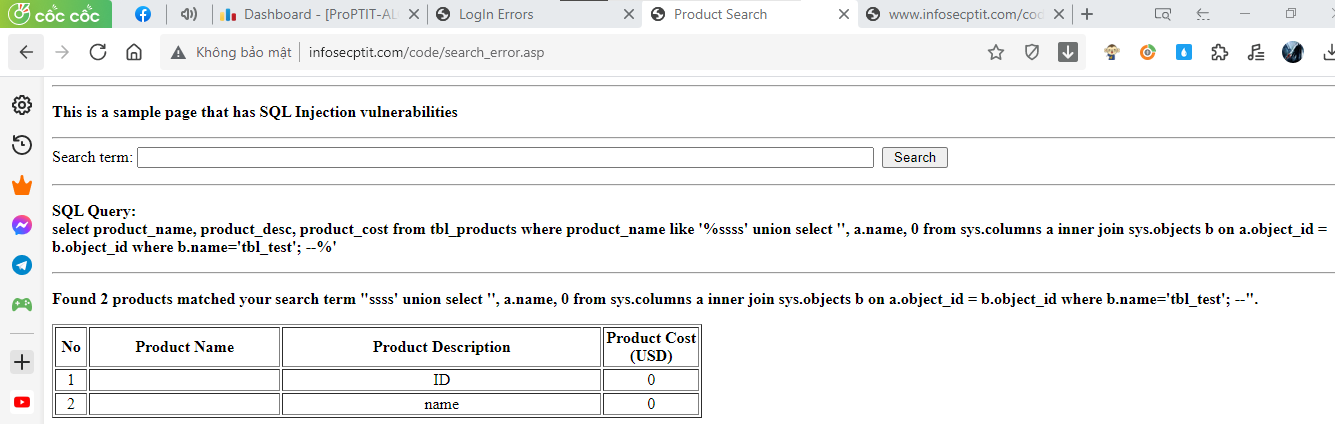
* Trích xuất danh sách các bảng của CSDL:



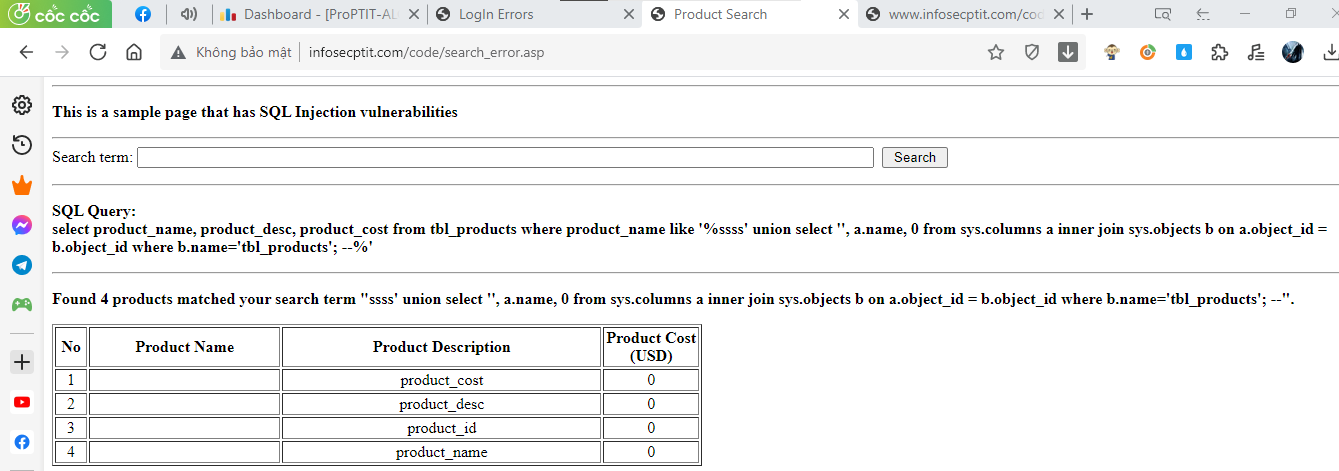
* Trích xuất danh sách các trường của một bảng:
* **tbl\_users**



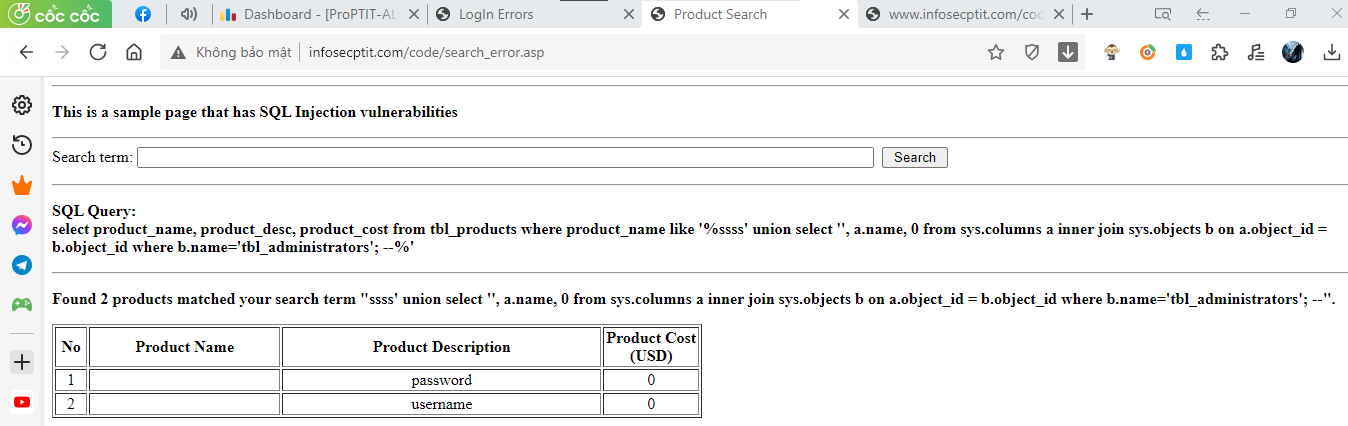
* **tbl\_test**

****

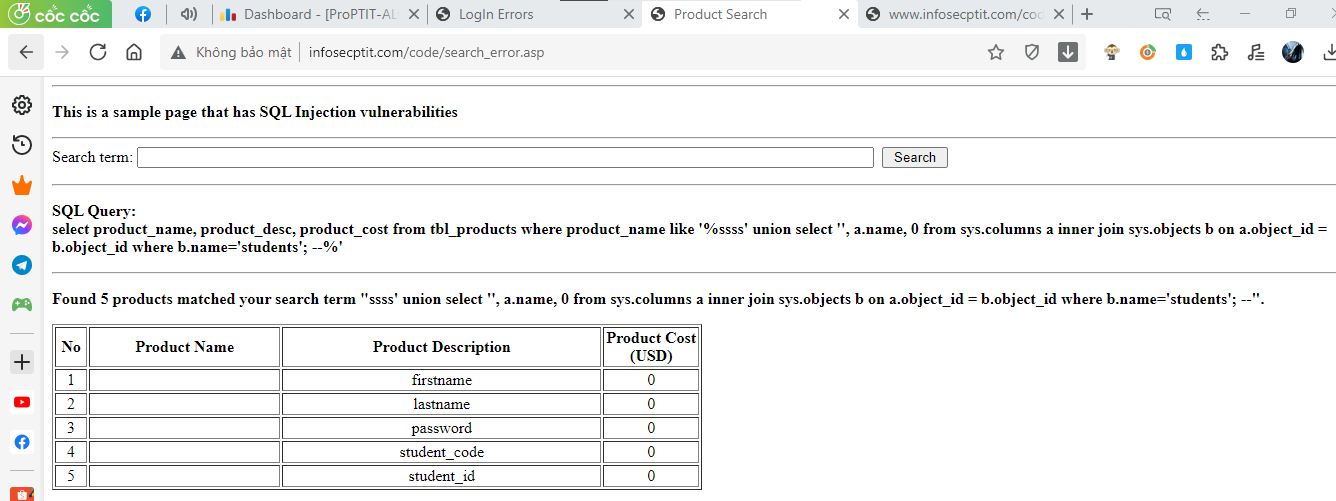
* **tbl\_products**

****

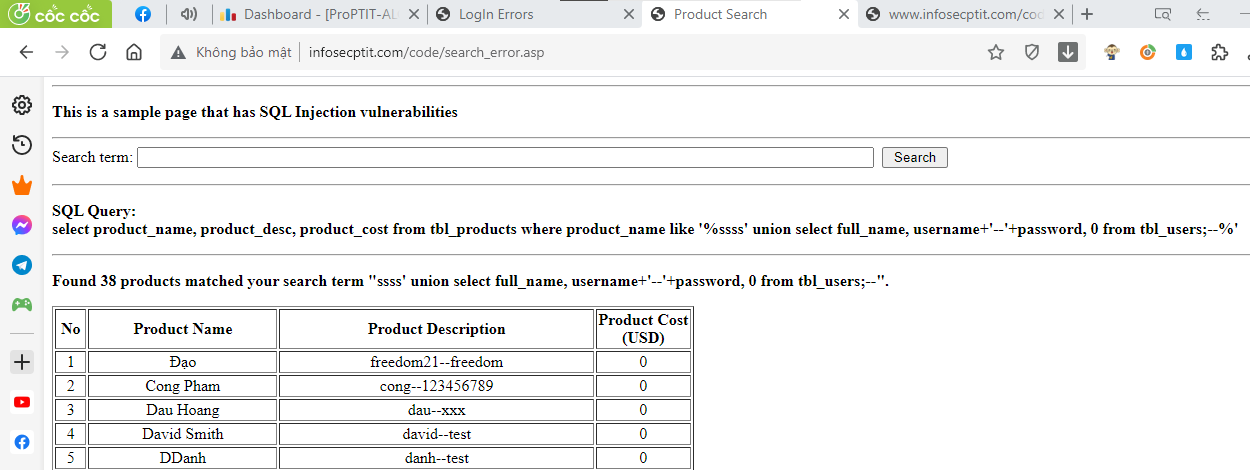
* **tbl\_administrators**

****

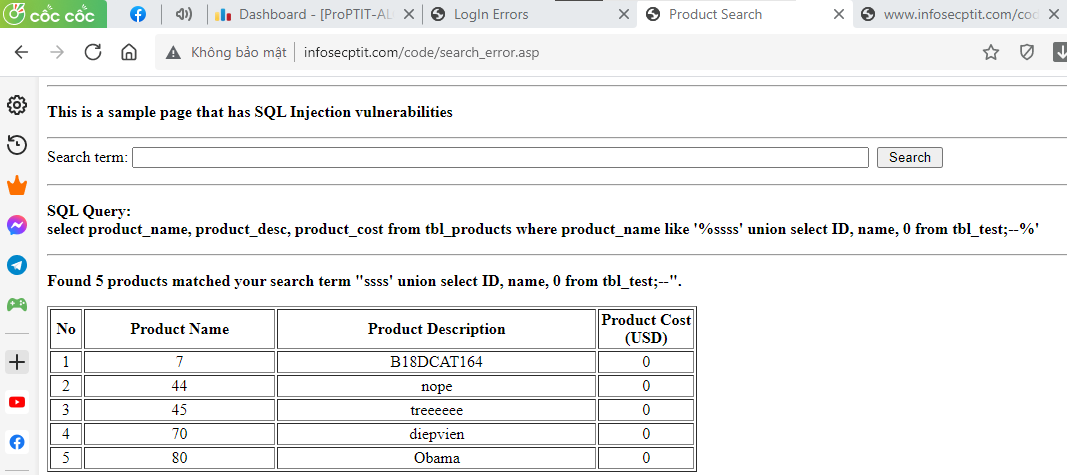
* **students**

****

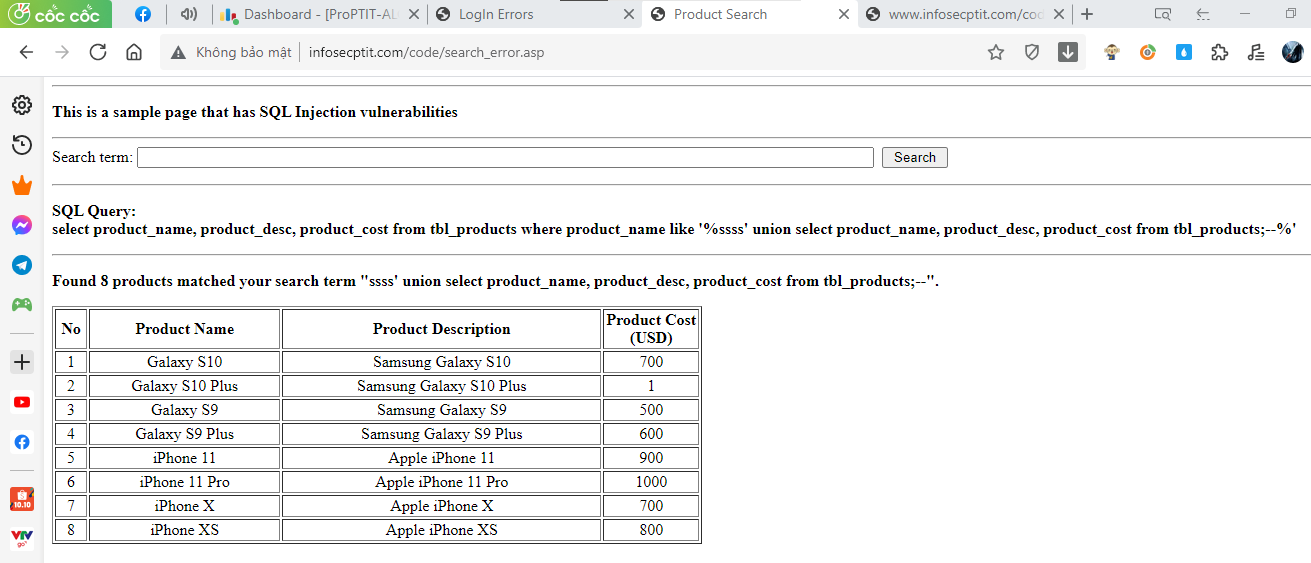
* Trích xuất dữ liệu bảng:
* **tbl\_users**



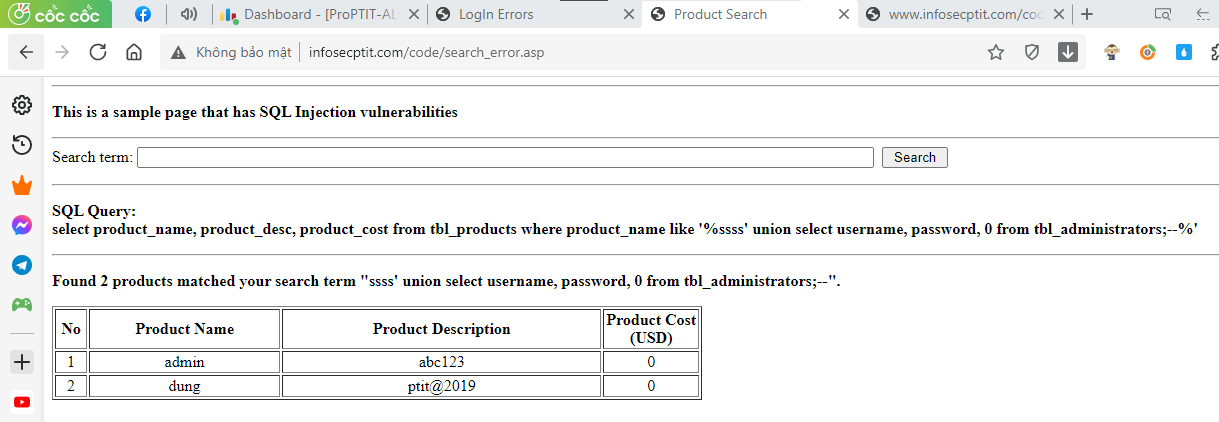
* **tbl\_test**

****

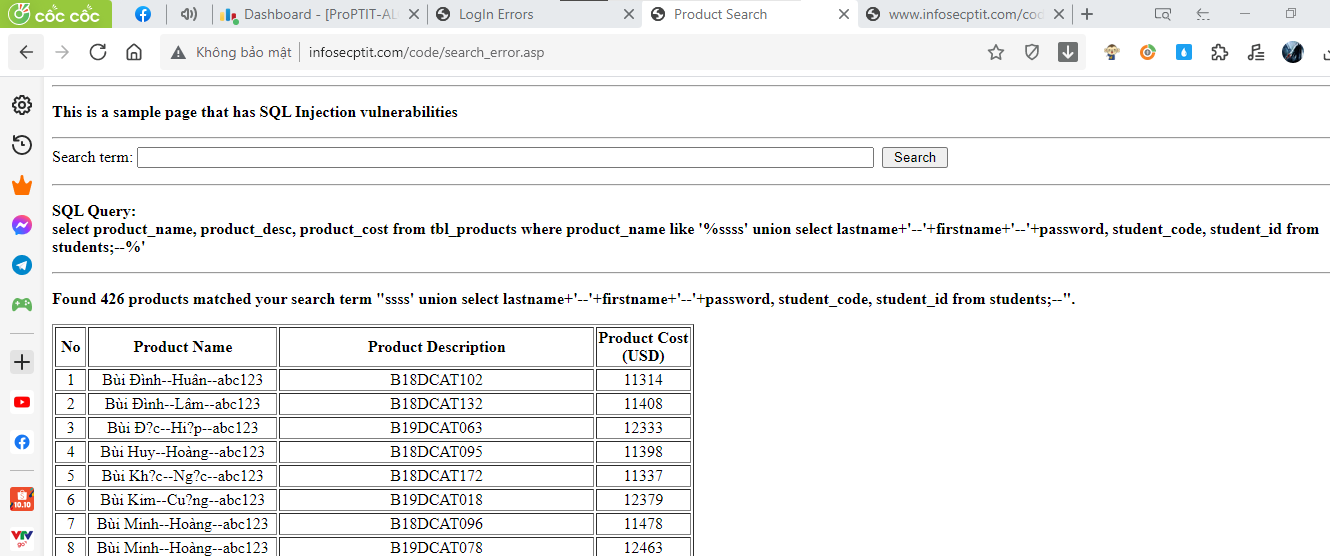
* **tbl\_products**



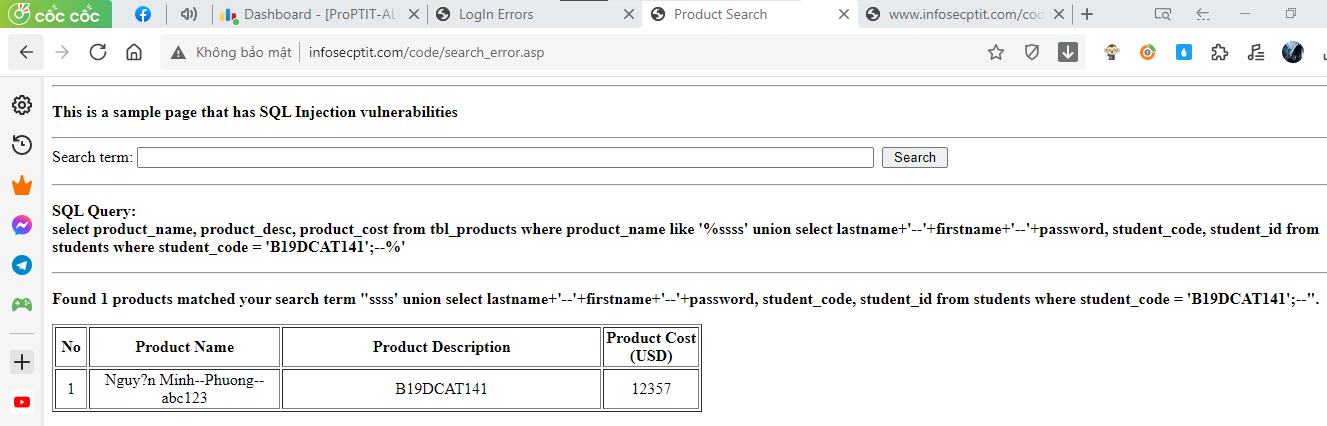
* **tbl\_administrators**



* **students**

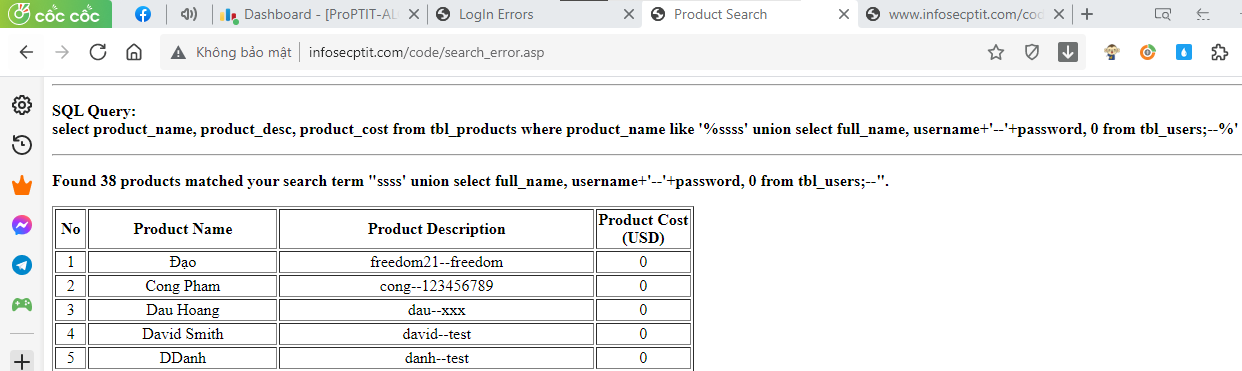
****

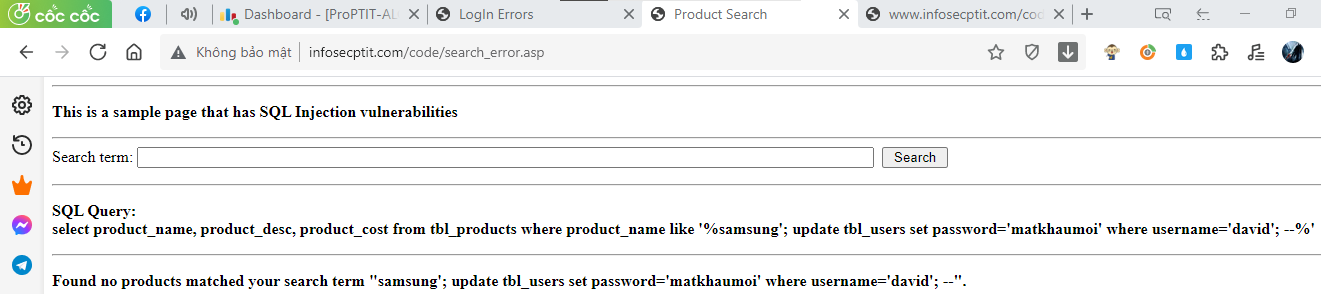
* **Trích xuất 1 bản ghi gồm tất cả các trường từ bảng students có mã sinh viên trùng với mã sv của mình và hiển thị toàn bộ thông tin trích xuất được lên màn hình**

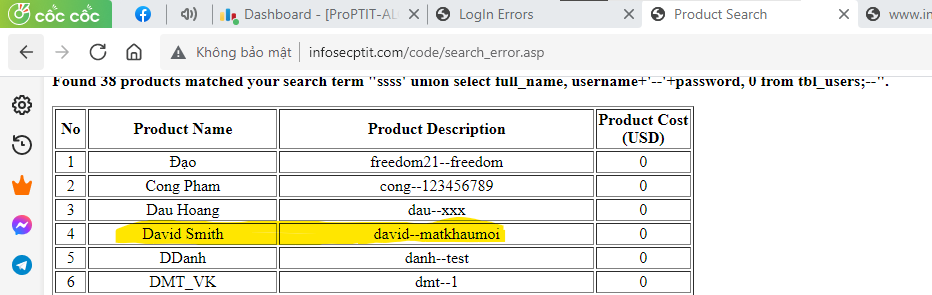
****

1. **Thêm, sửa, xóa dữ liệu:**

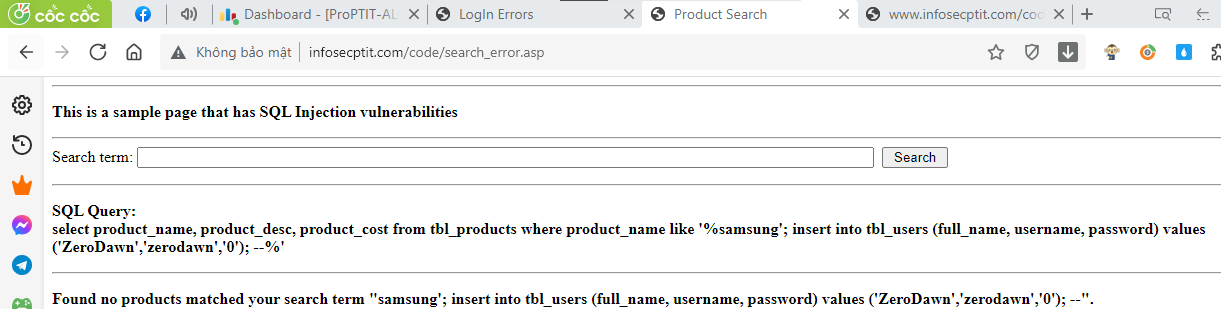
* Sửa dữ liệu:

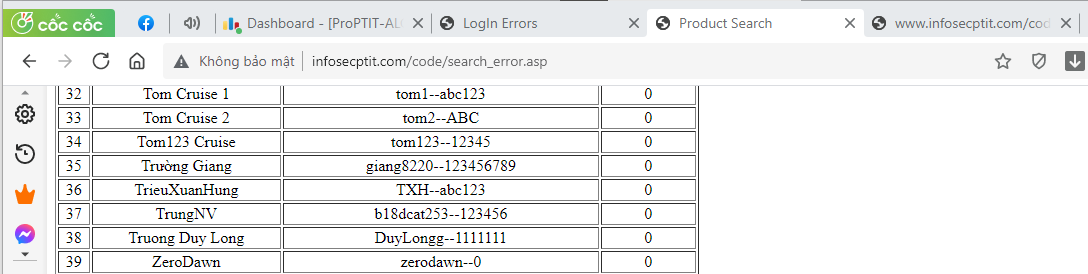
****

****

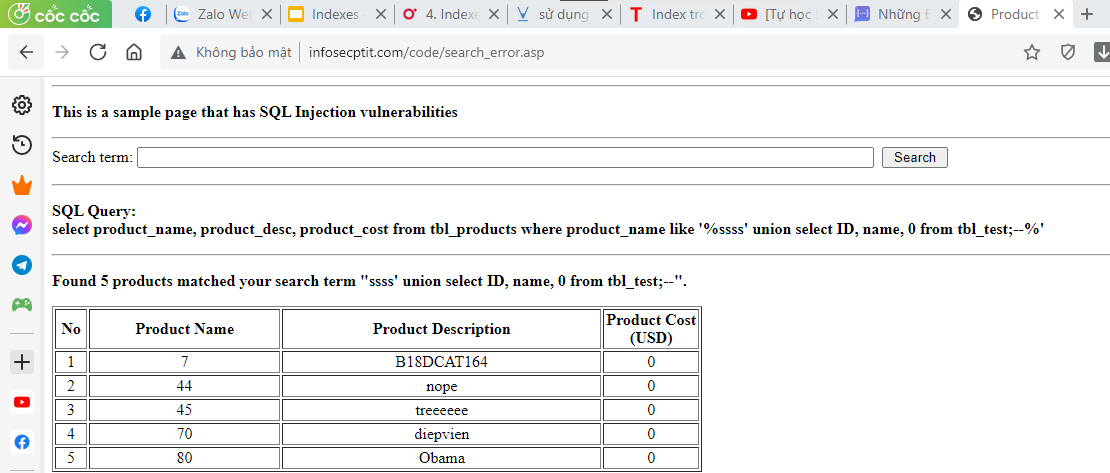
****

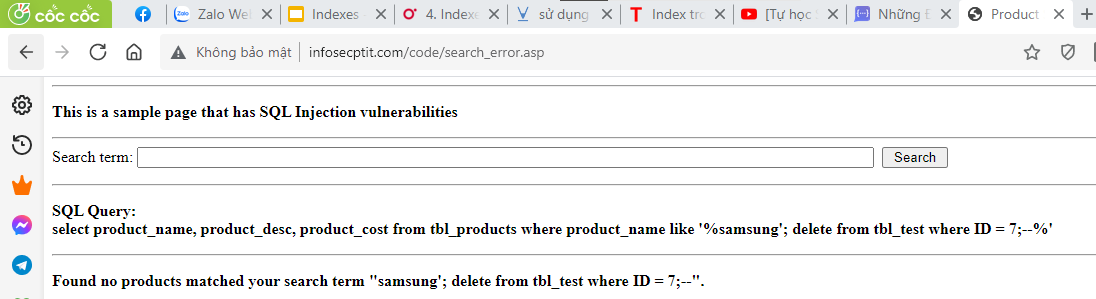
* Thêm dữ liệu:

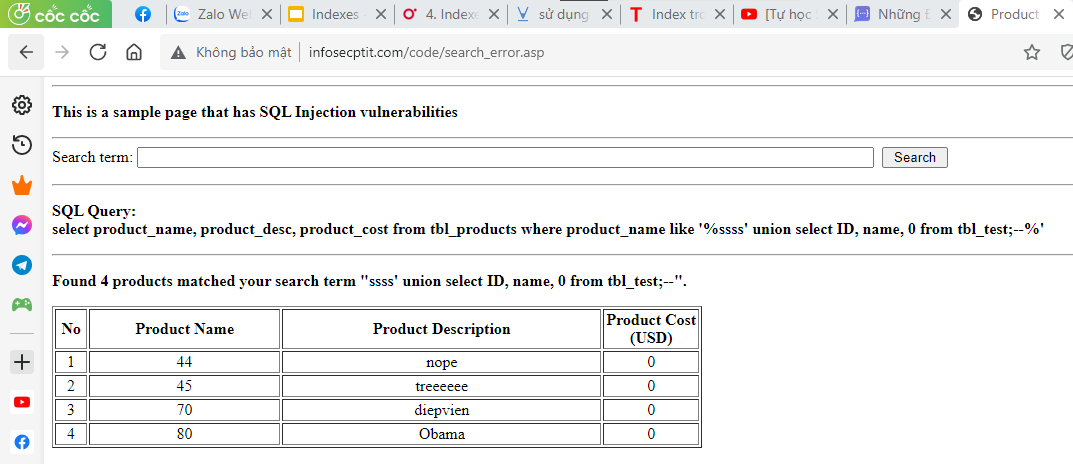
****

****

* Xóa dữ liệu:

****

****

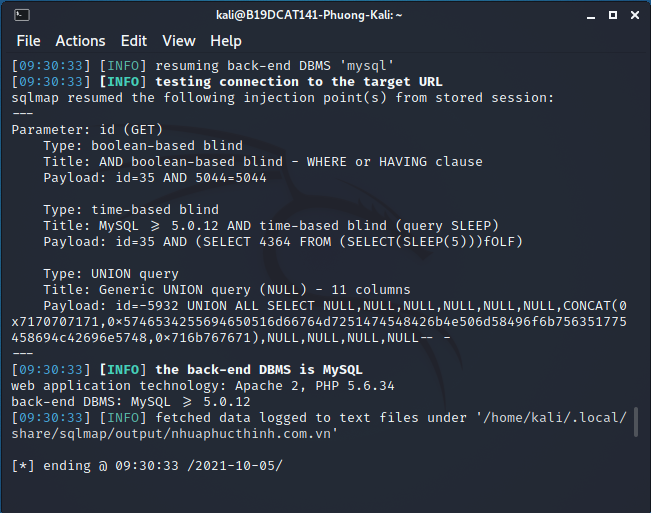
****

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

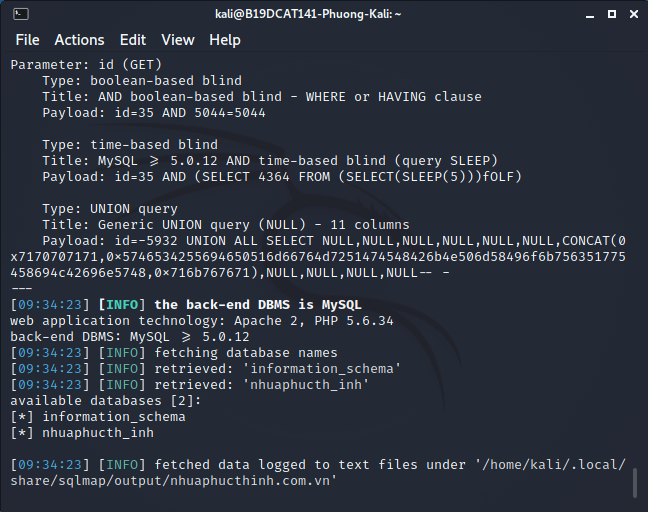
* <http://nhuaphucthinh.com.vn/product.php?id=35>

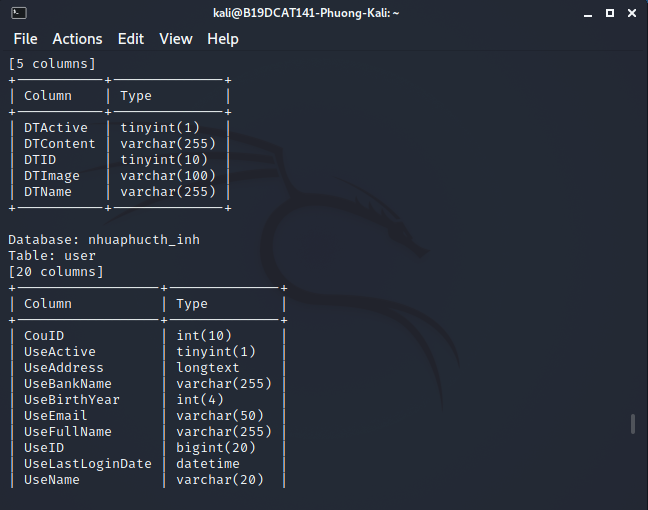
1. **Sử dụng công cụ rà quét lỗi và tấn công chèn mã SQL – SQLMap**

* **Rà quét lỗi** <http://nhuaphucthinh.com.vn/product.php?id=35>

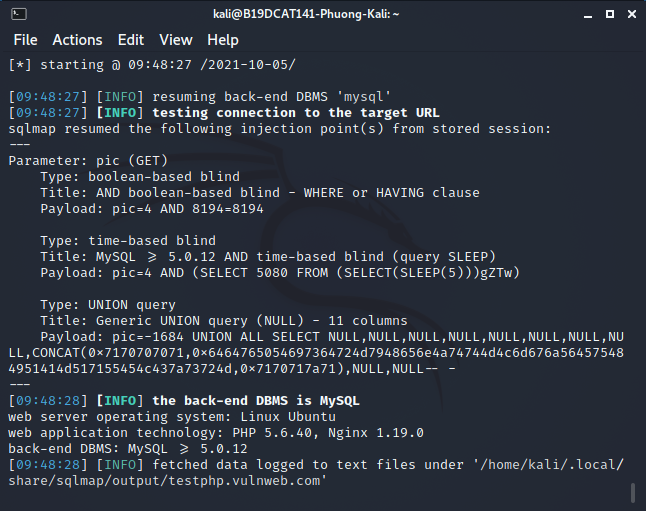


* **Tấn công chèn mã:** <http://nhuaphucthinh.com.vn/product.php?id=35>

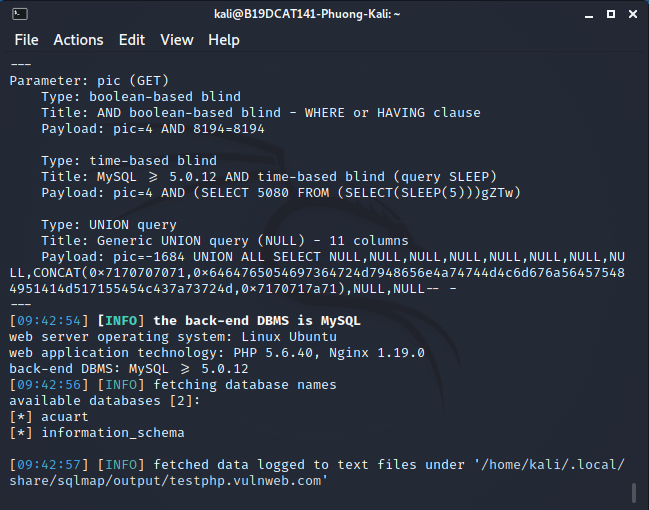
****

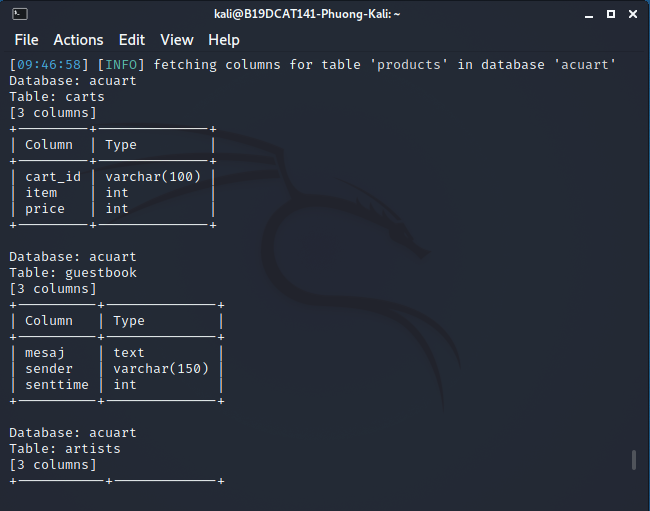


* **Rà quét lỗi:** <http://testphp.vulnweb.com/product.php?pic=4>

****

* **Tấn công chèn mã SQL**

****

****