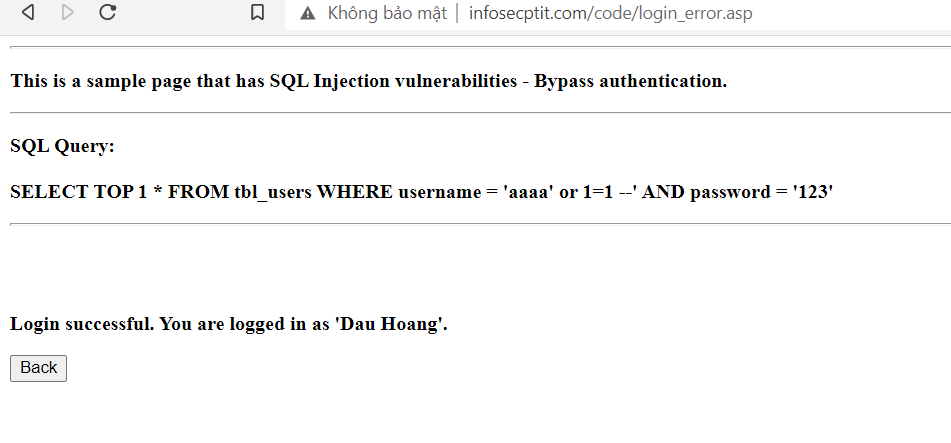
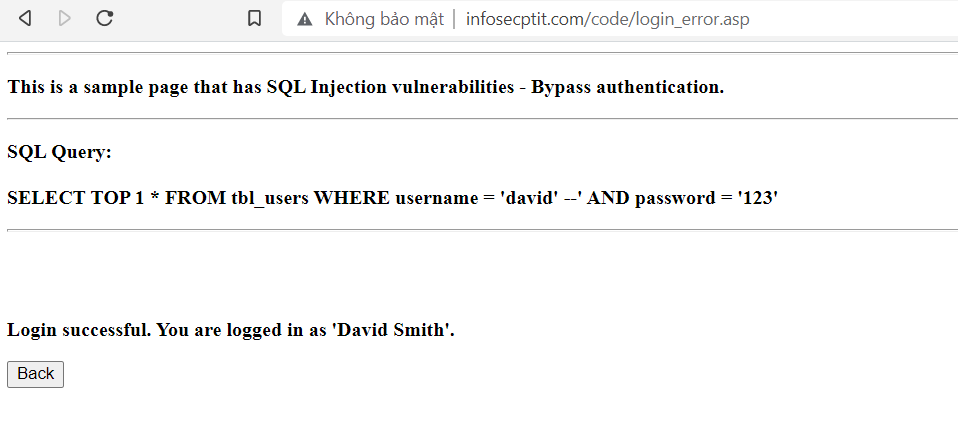
**Đinh Quang Hiếu – B19DCAT065**

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

* Đăng nhập với username : aaaa' or 1=1 -- và password : bất kì

****

* Đăng nhập với username : david' -- và password : bất kì

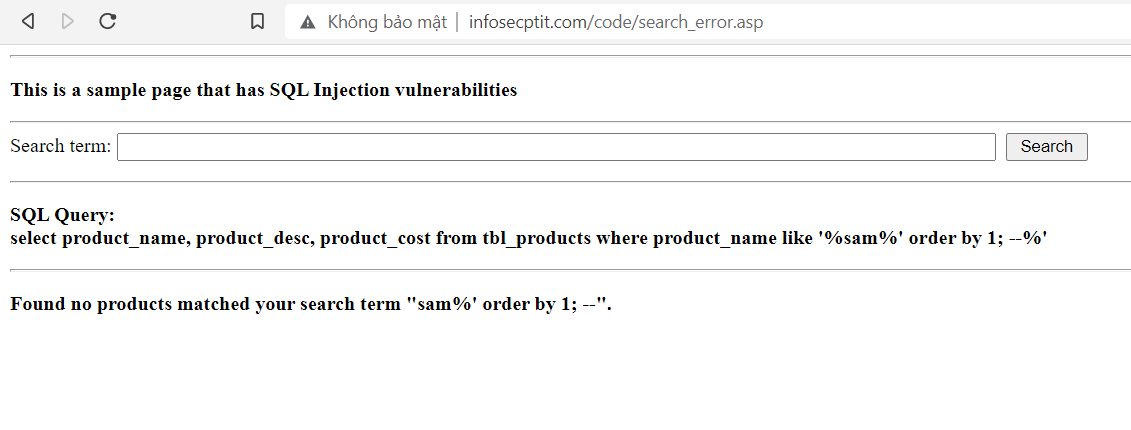
****

* **Giải thích câu lệnh SELECT TOP 1 \* FROM tbl\_users WHERE username = 'david' --' AND password = ‘123’**

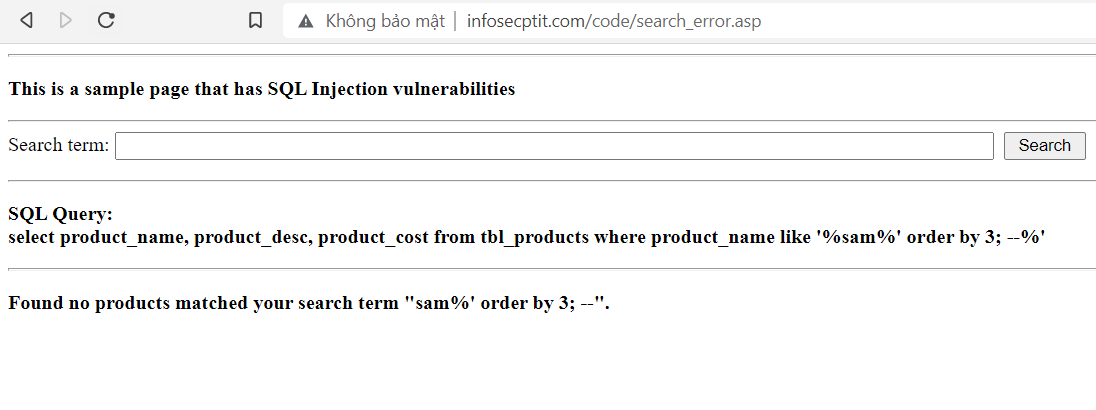
Trả về 1 giá trị đầu tiên dùng trong bảng tbl\_users thỏa mãn điều kiện sau WHERE đầu vào username là david’ – thì sau dấu ‘ dùng để ngắt lệnh , dấu – có tác dụng biến đoạn mã sau thành comment nên câu lệnh chỉ thực hiện so sánh điều kiện của username và bỏ qua password. Vì tài khoản người dùng david tồn tại nên sẽ login successful.

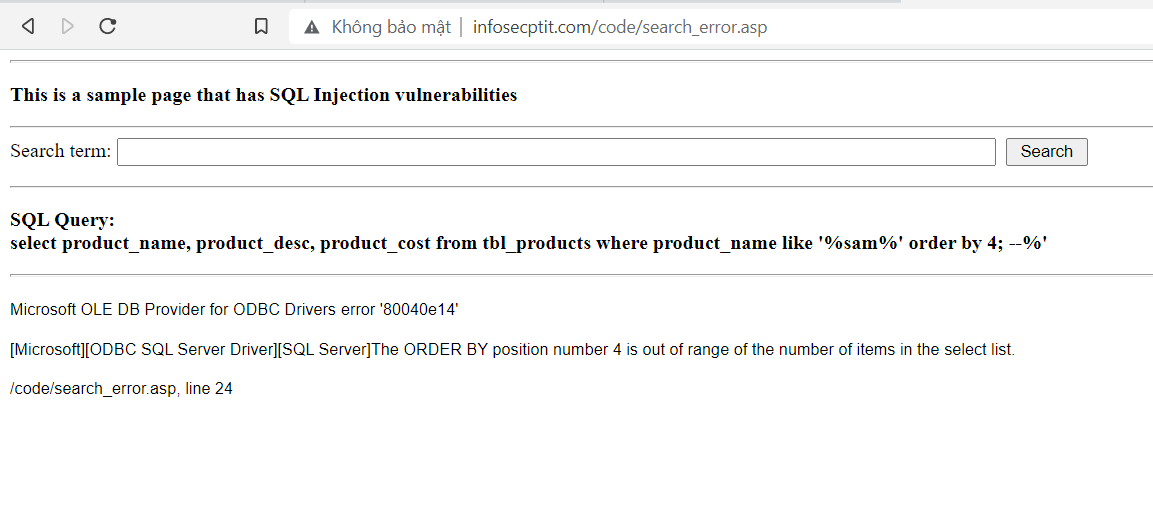
**2.Trích xuất dữ liệu từ CSQL**

* **Tìm số trường trong câu truy vấn**
* **Dùng câu lệnh sam%' order by <number>; --**

****

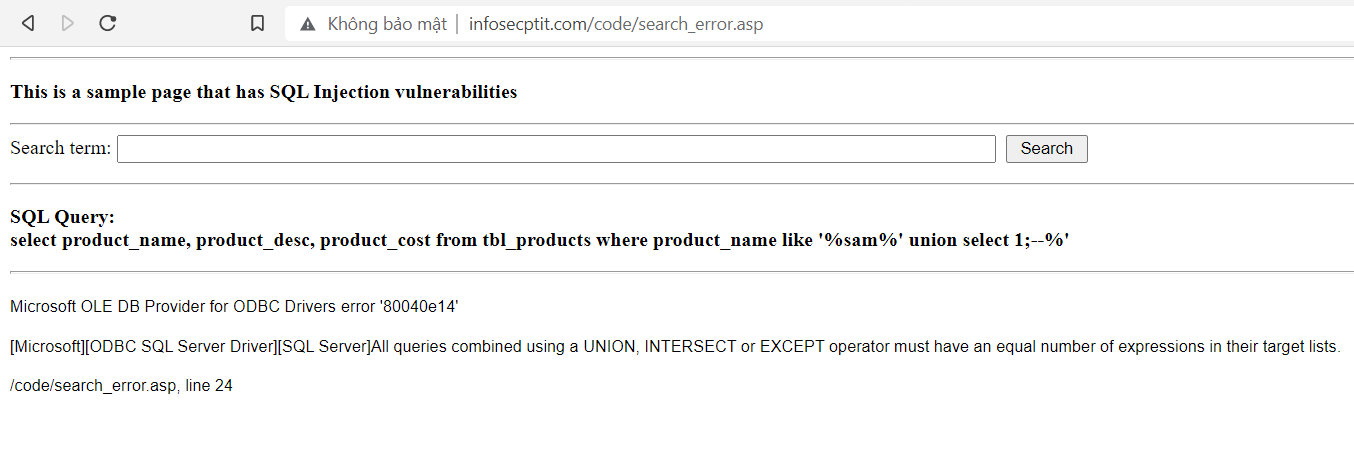
****

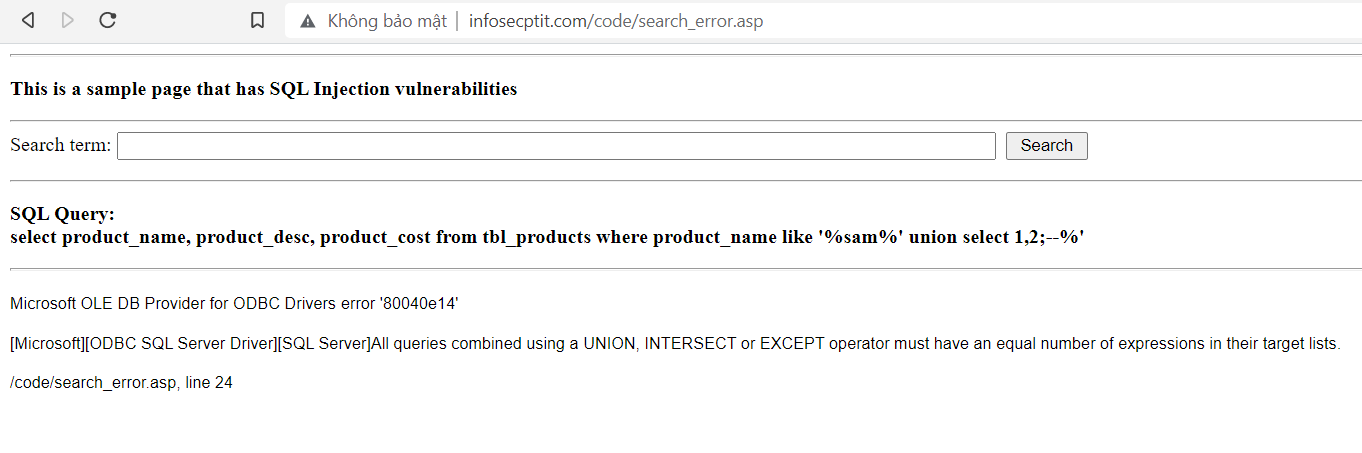
****

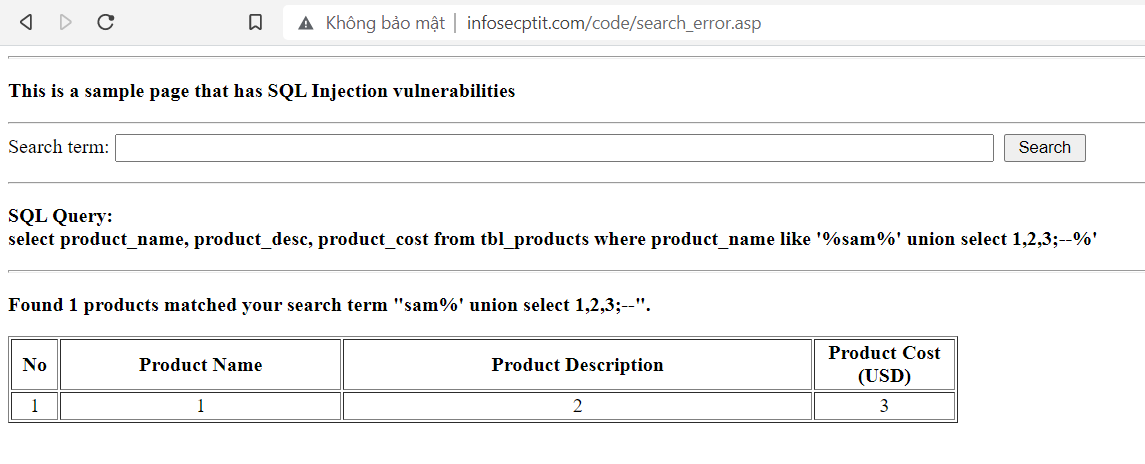
****

**→** Có 3

* **Dùng câu lệnh sam%' union select <danh sách trường thử>;--**

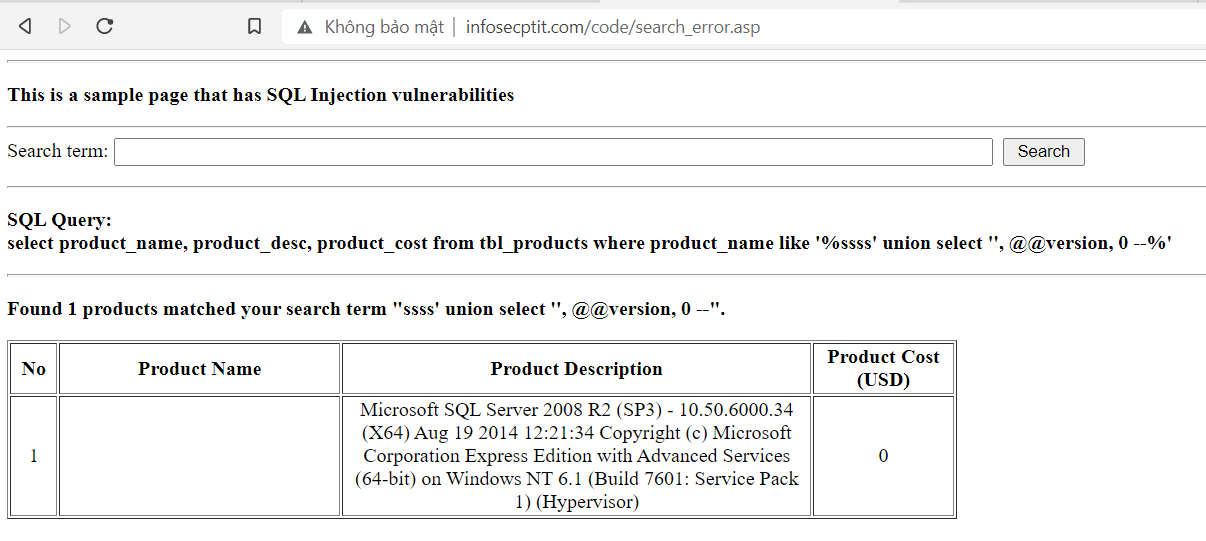
****

****

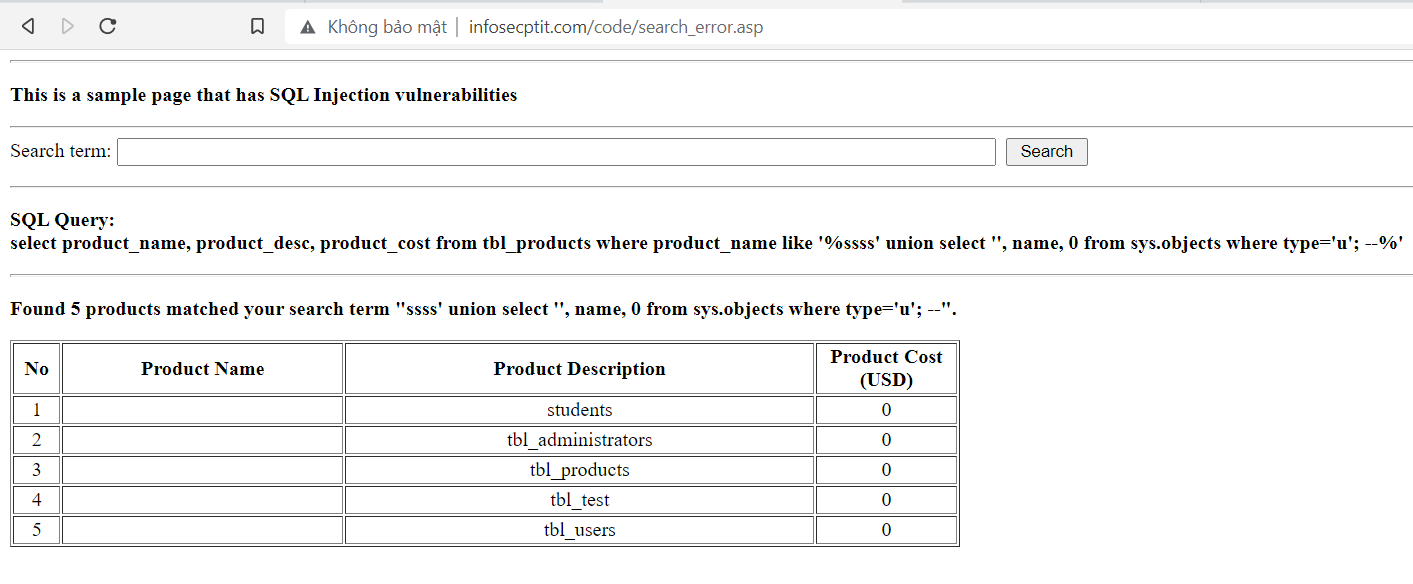
****

**→** Có 3

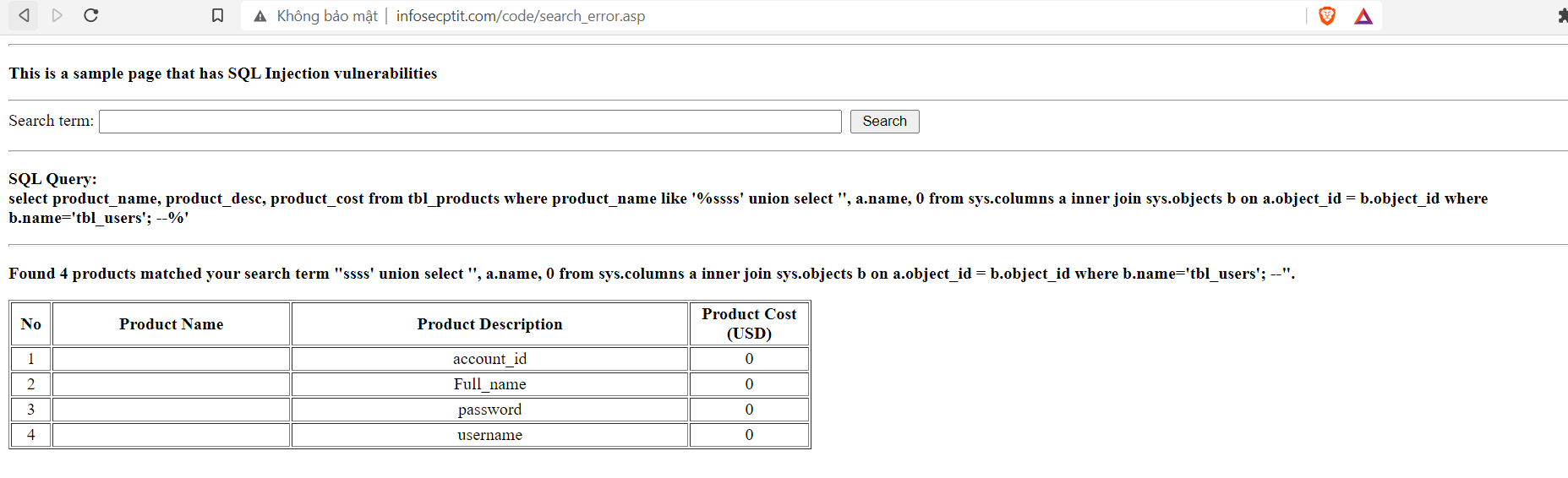
* **Hiển thị thông tin hệ quản trị CSDL và hệ điều hành:**

****

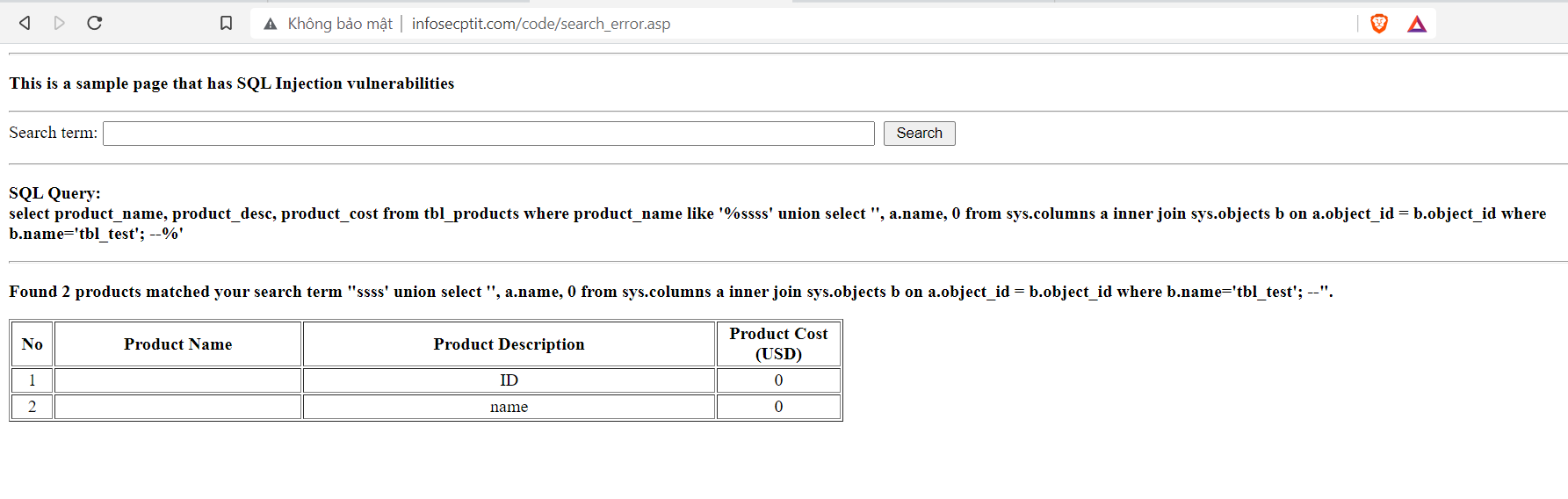
* **Trích xuất danh sách các bảng của CSDL:**

****

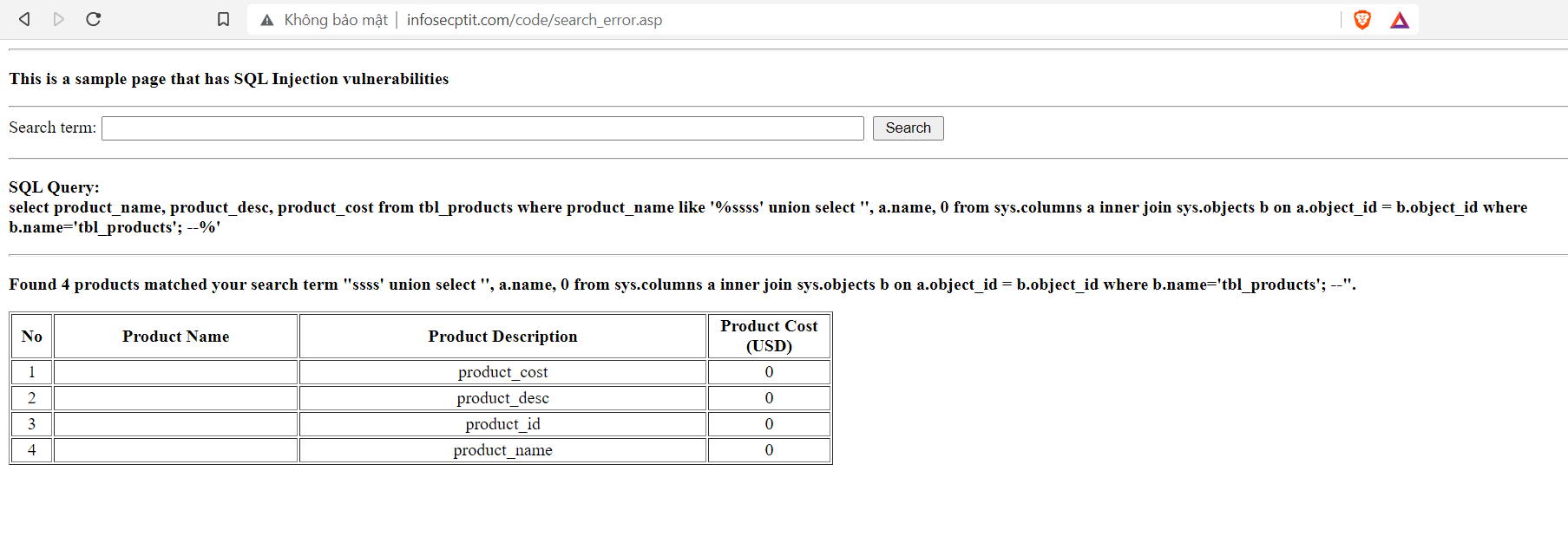
* **Trích xuất danh sách các trường của một bảng:**
* **tbl\_users**

****

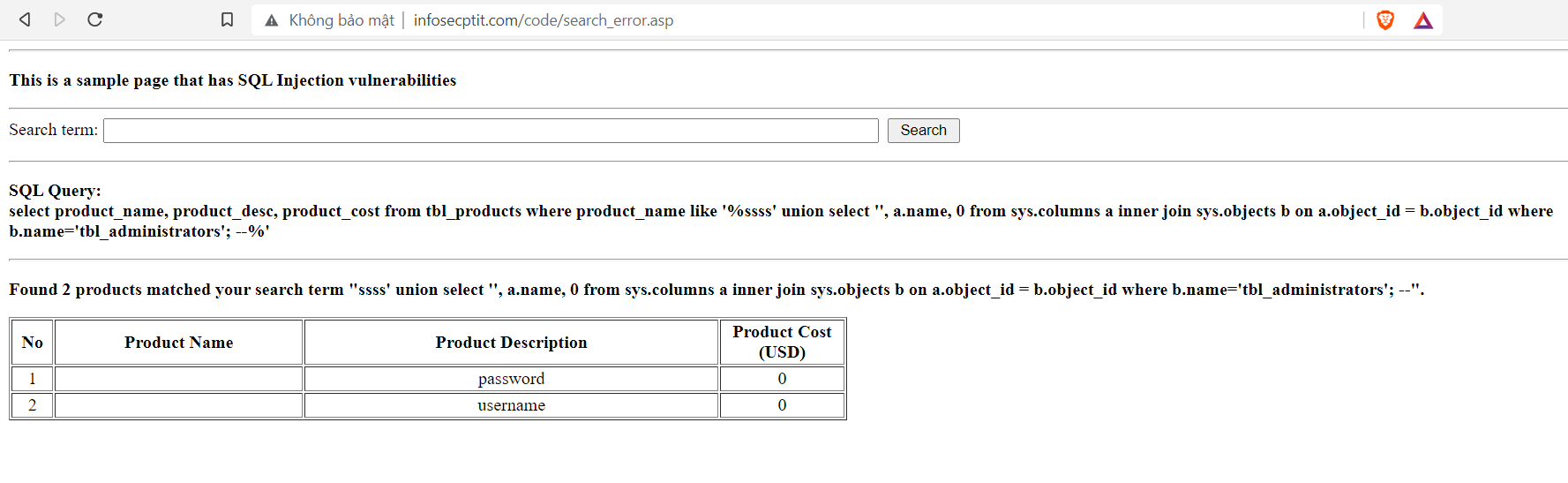
* **tbl.test**

****

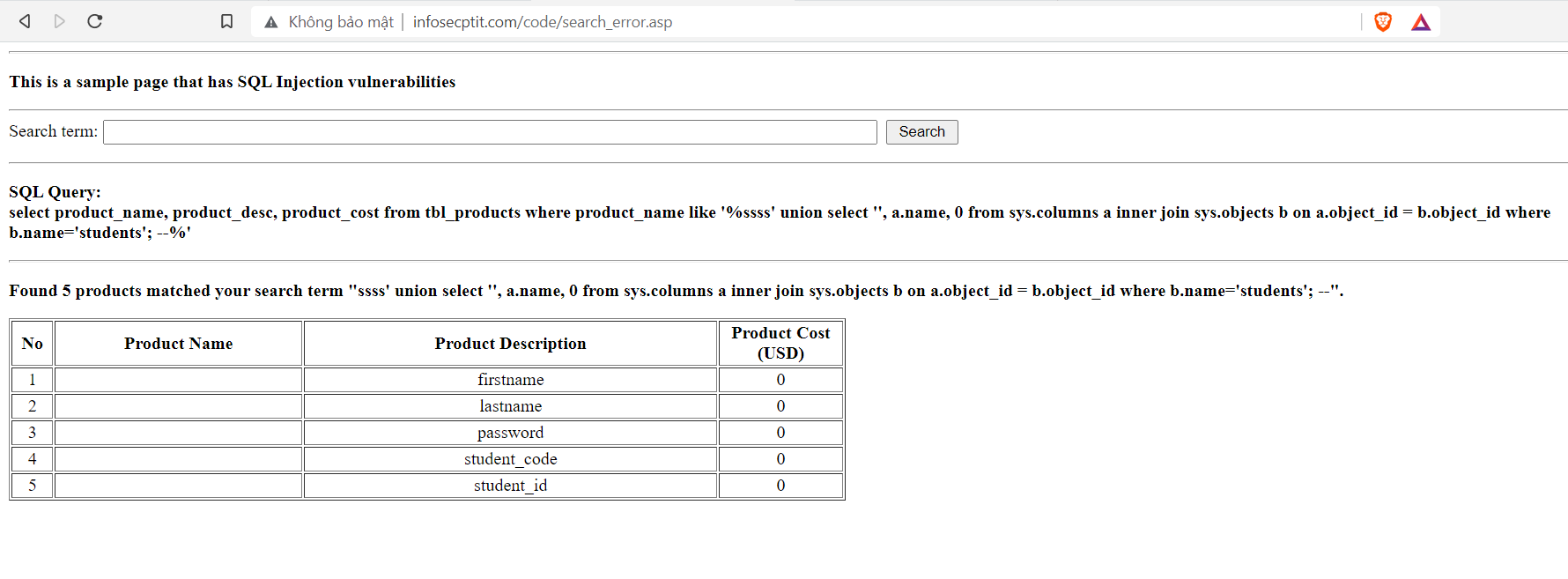
* **tbl\_products**

****

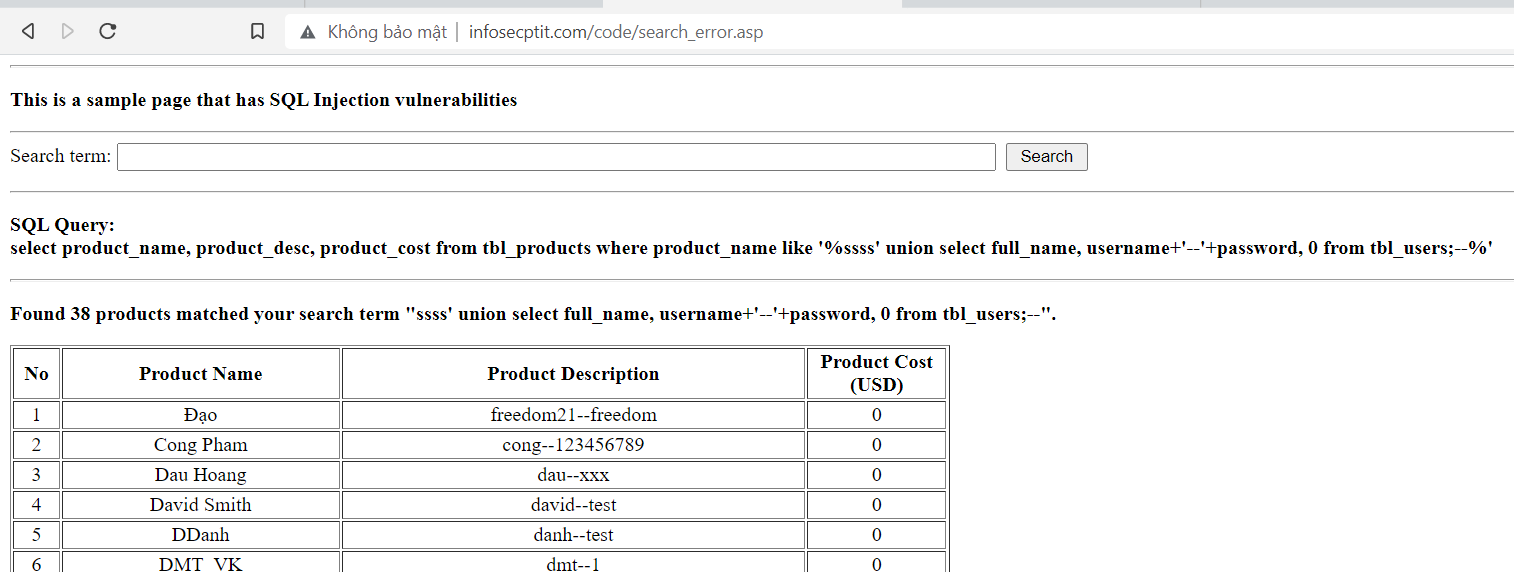
* **tbl\_administrators**

****

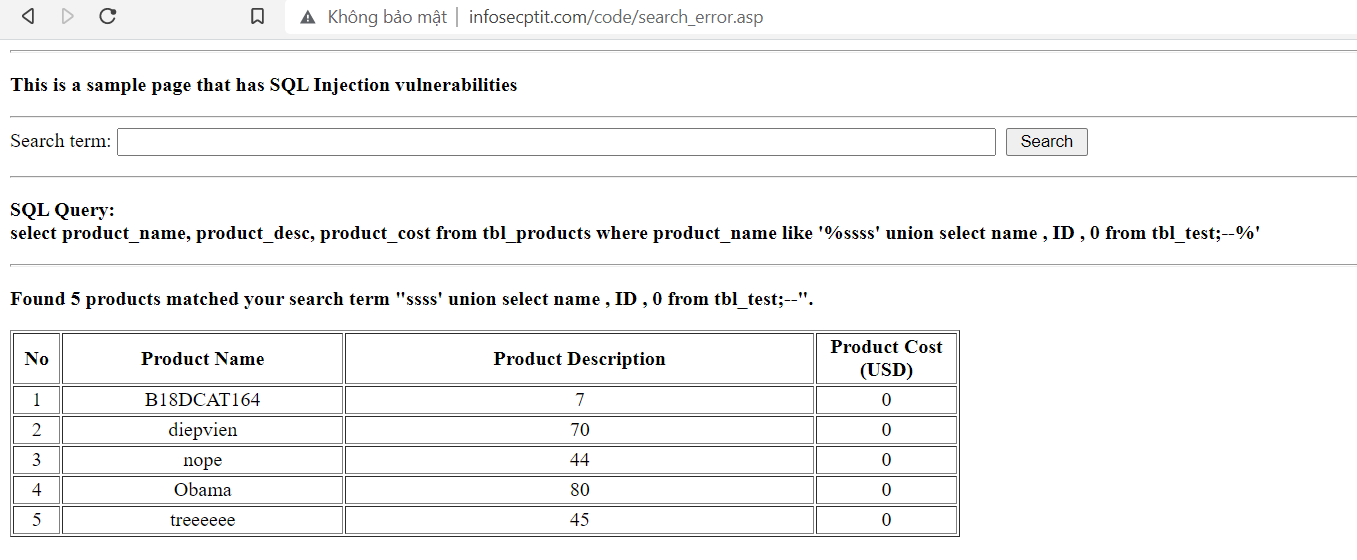
* **students**

****

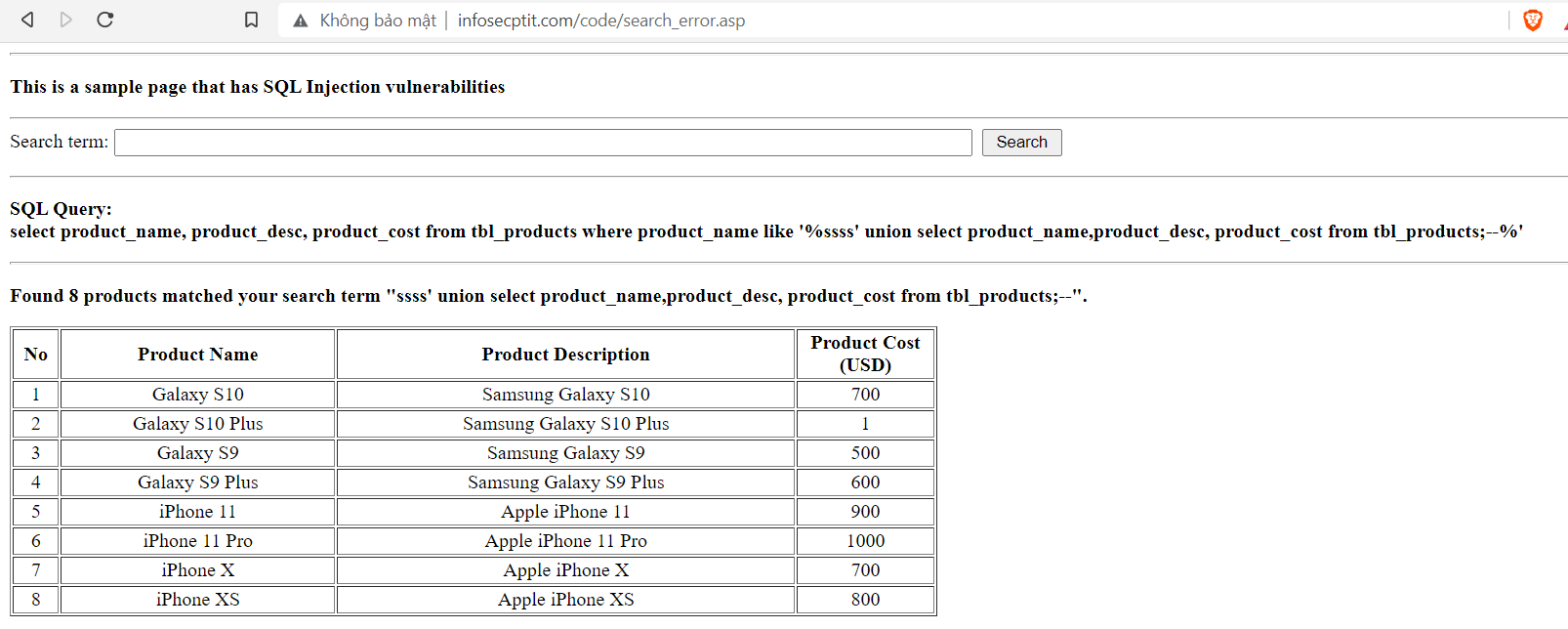
* **Trích xuất dữ liệu bảng:**
* **tbl\_users**

****

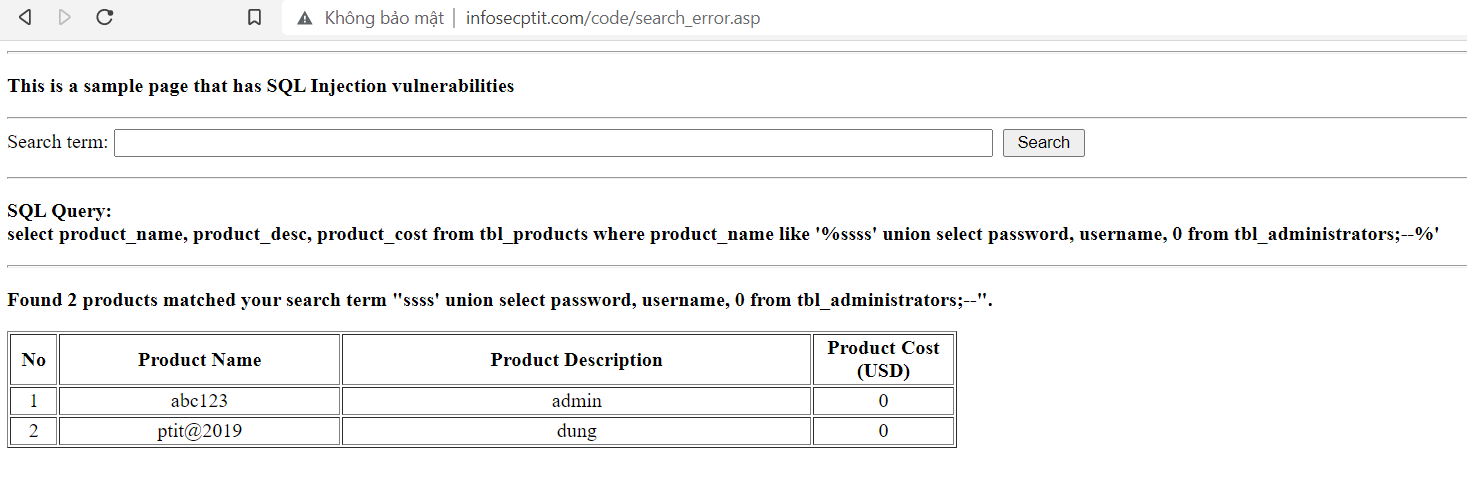
* **tbl\_test**

****

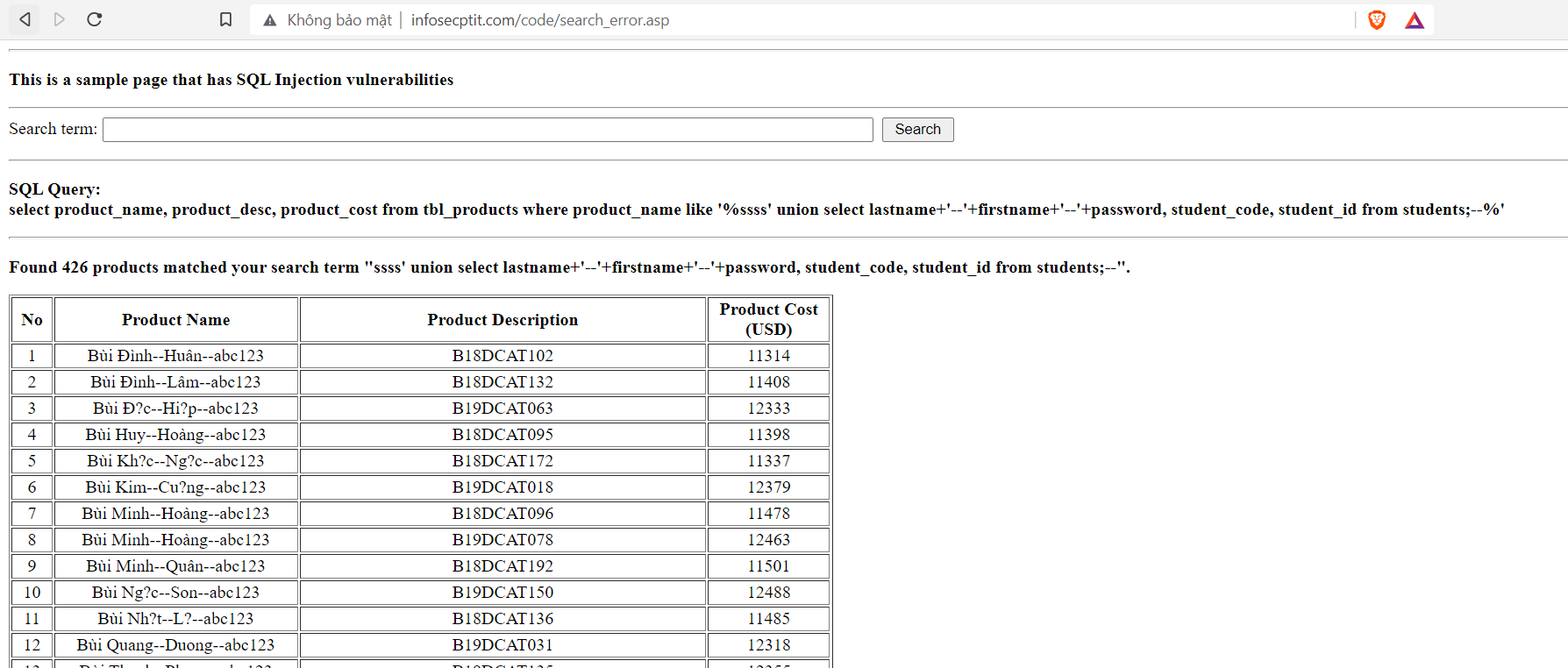
* **tbl\_products**

****

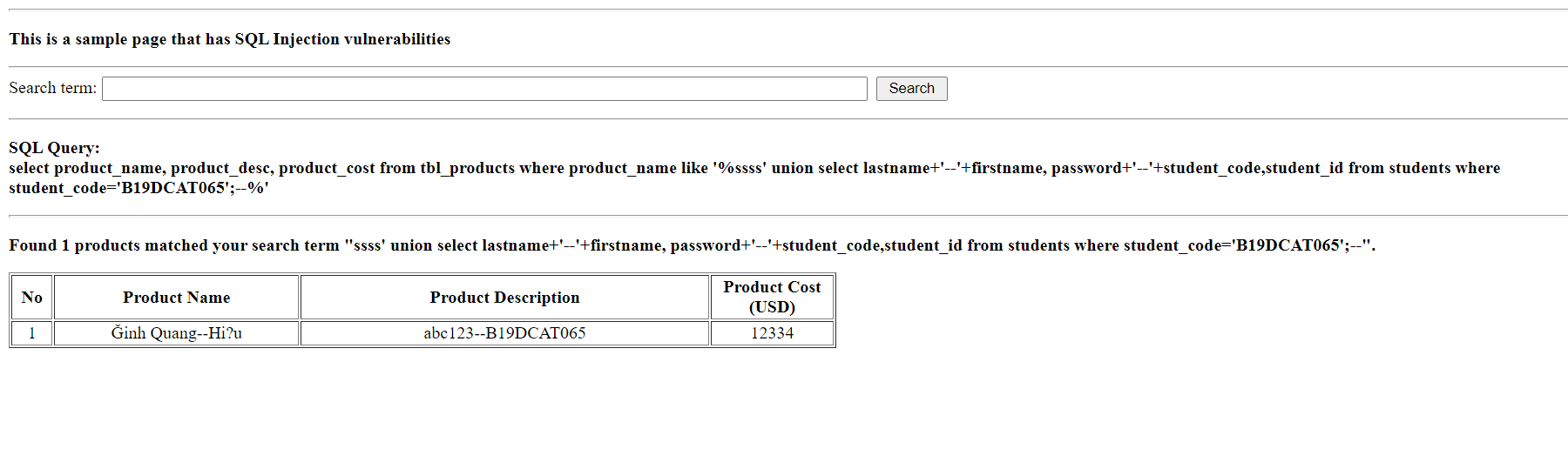
* **tbl\_administrators**

****

* **students**

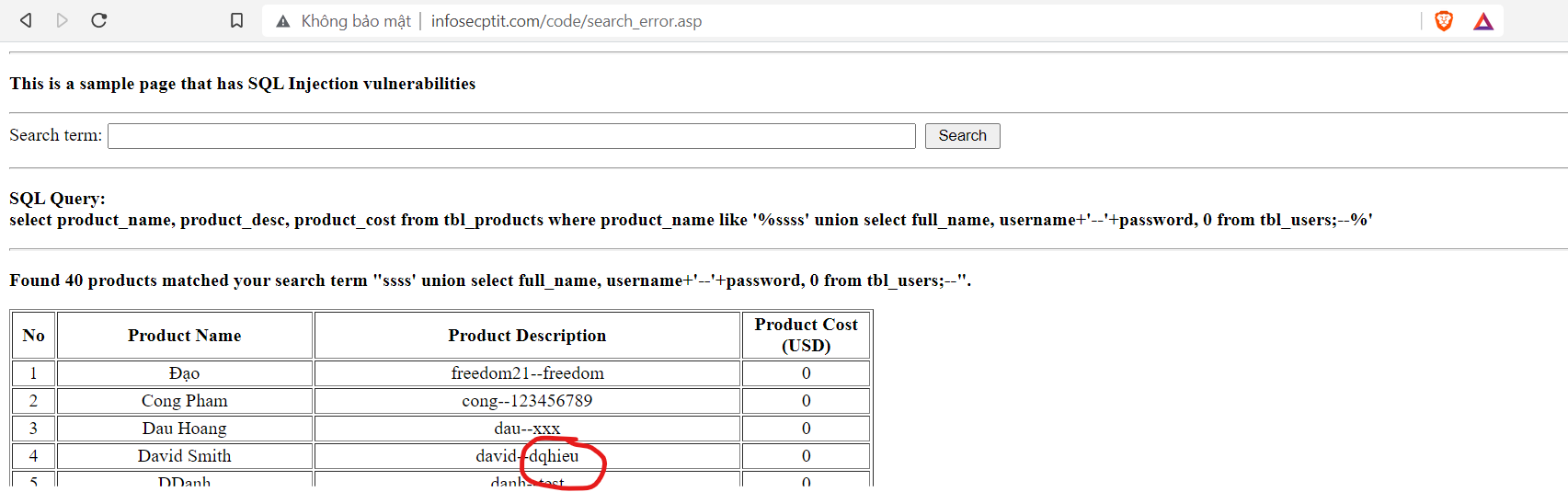
****

* **Hiển thị tên mình trong trường students**

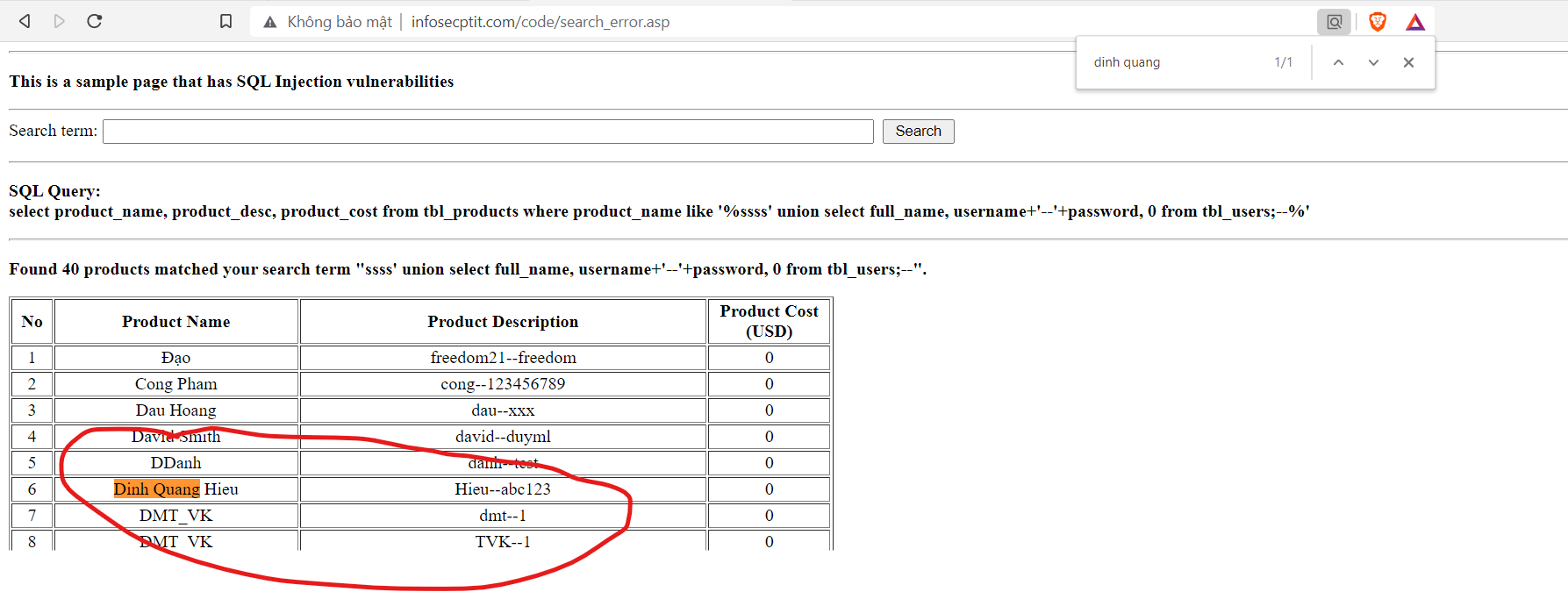
****

**3. Thêm, sửa, xóa dữ liệu**

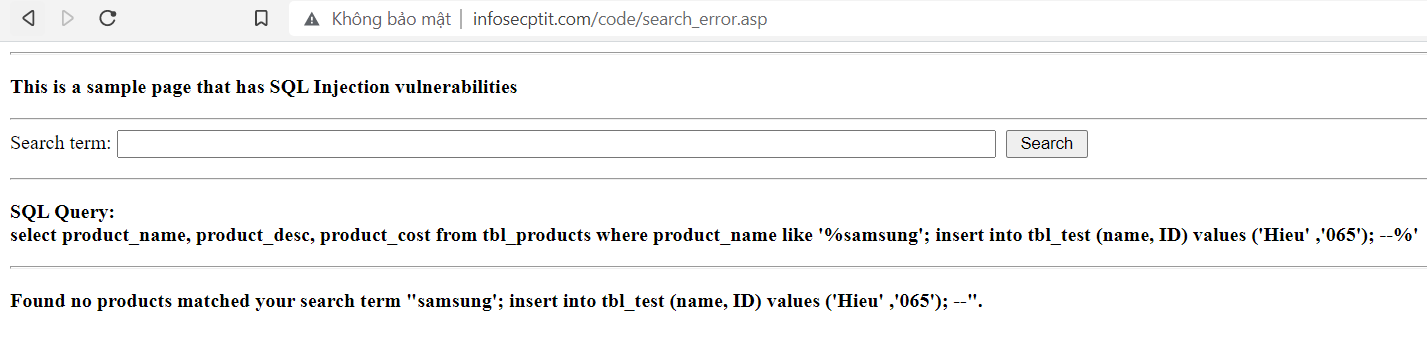
* **Sửa**

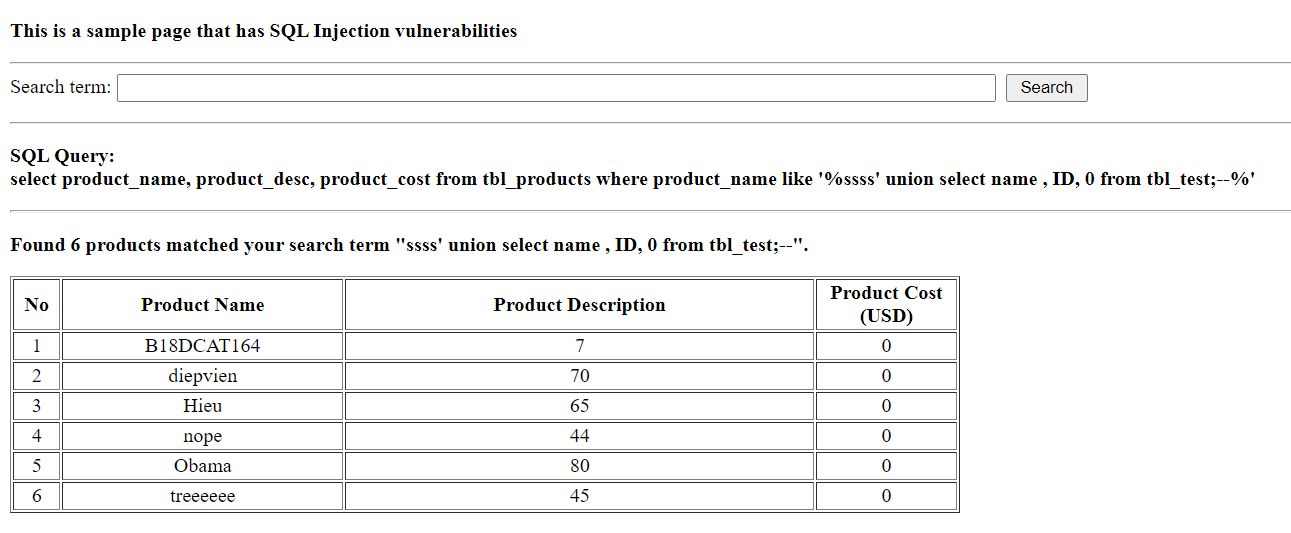
****

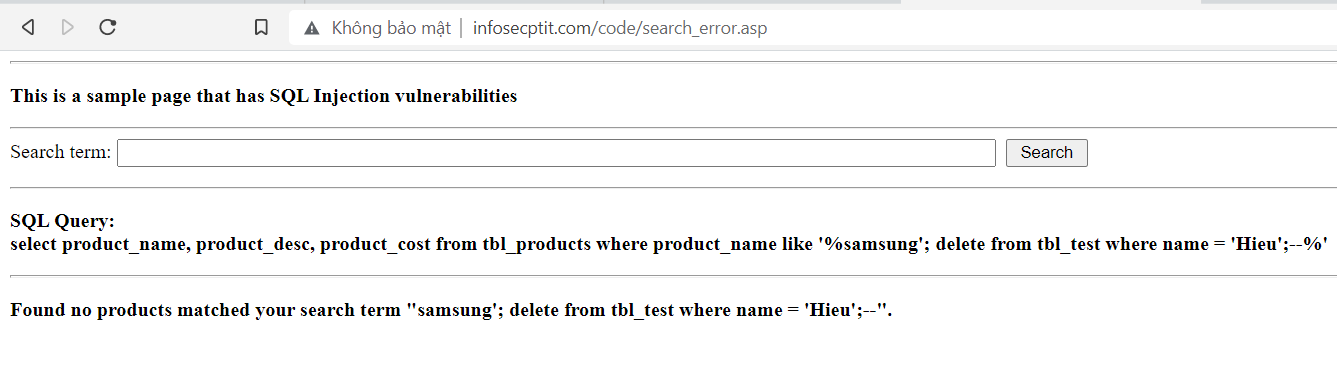
* **Thêm**

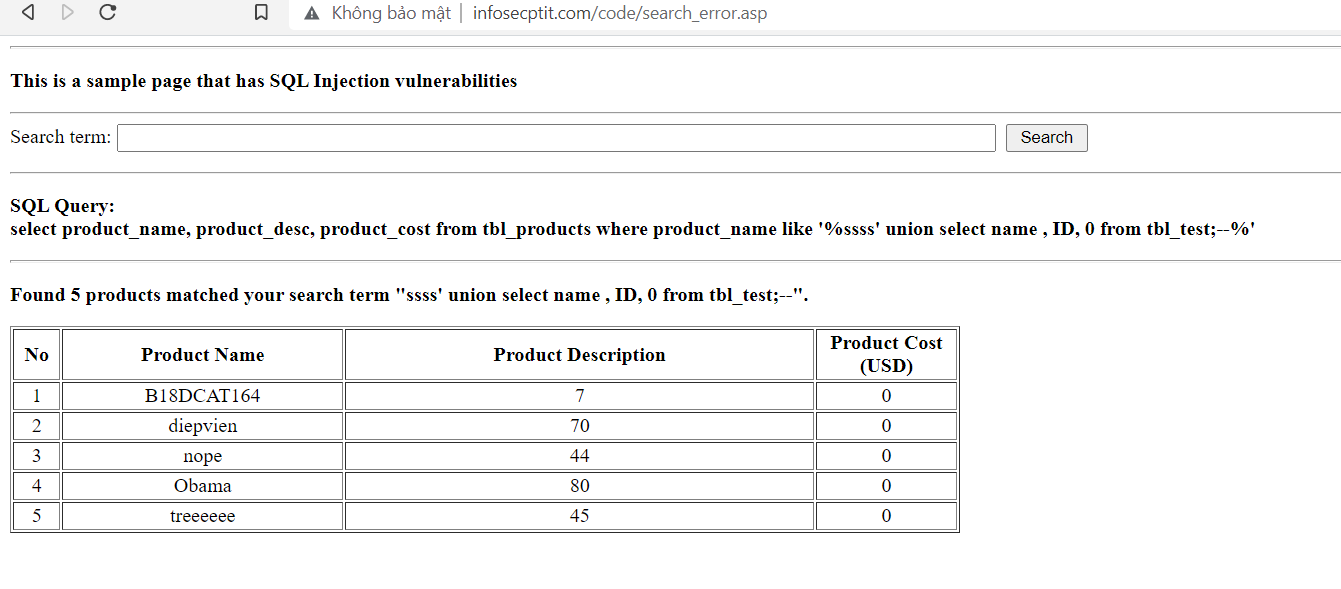
****

* **Xóa**

****

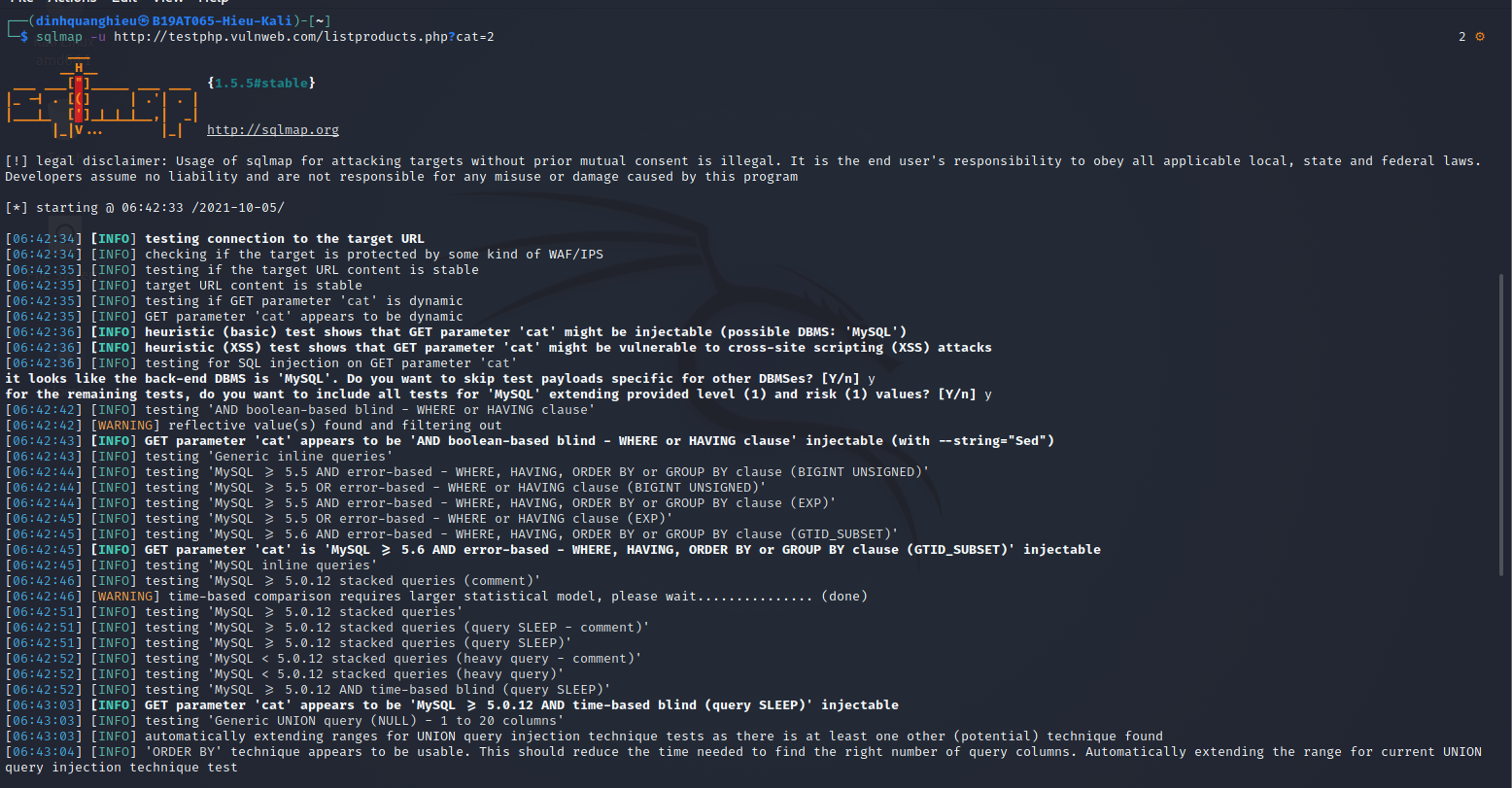
****

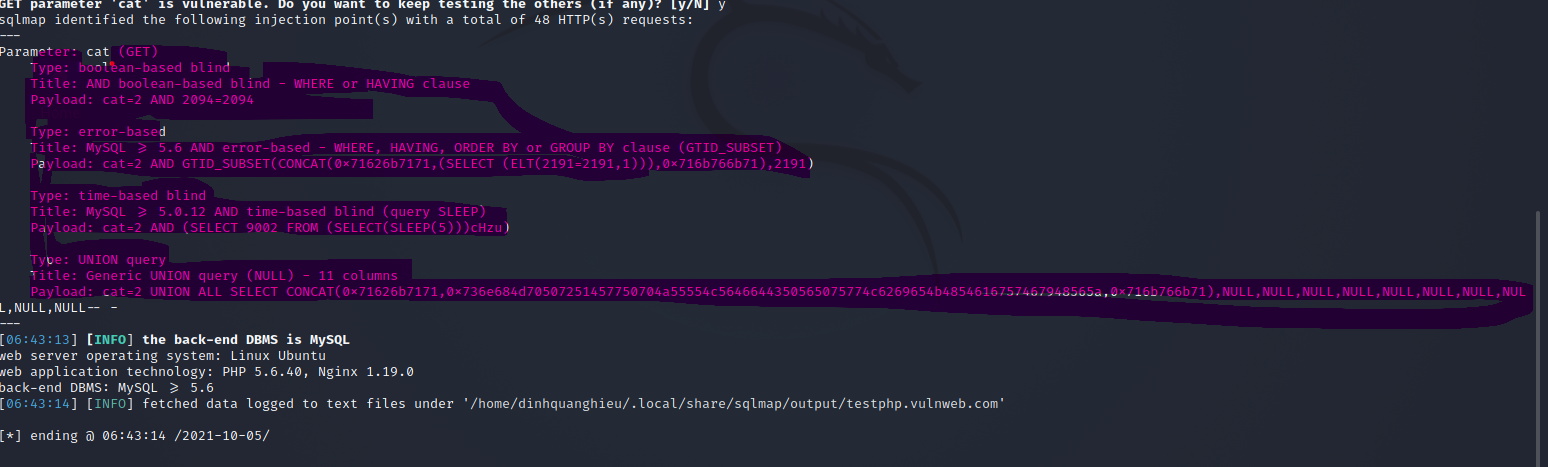
****

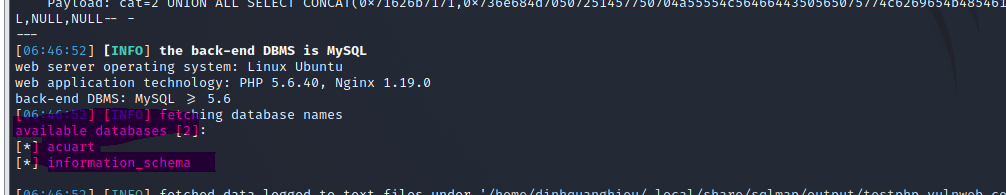
****

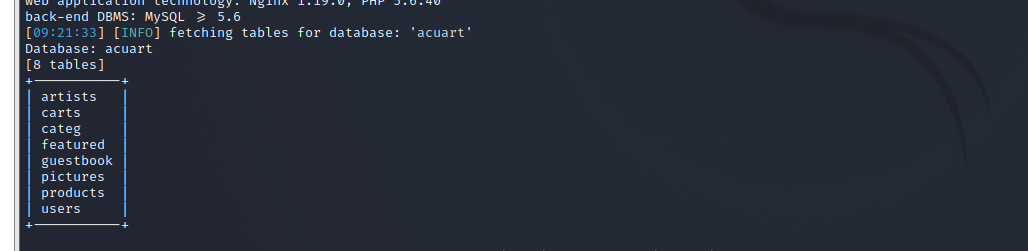
**Sử dụng công cụ rà quét lỗi và tấn công chèn mã SQL - SQLMap**

* **Trang testphp.vulnweb.com/listproducts.php?cat=2**

S



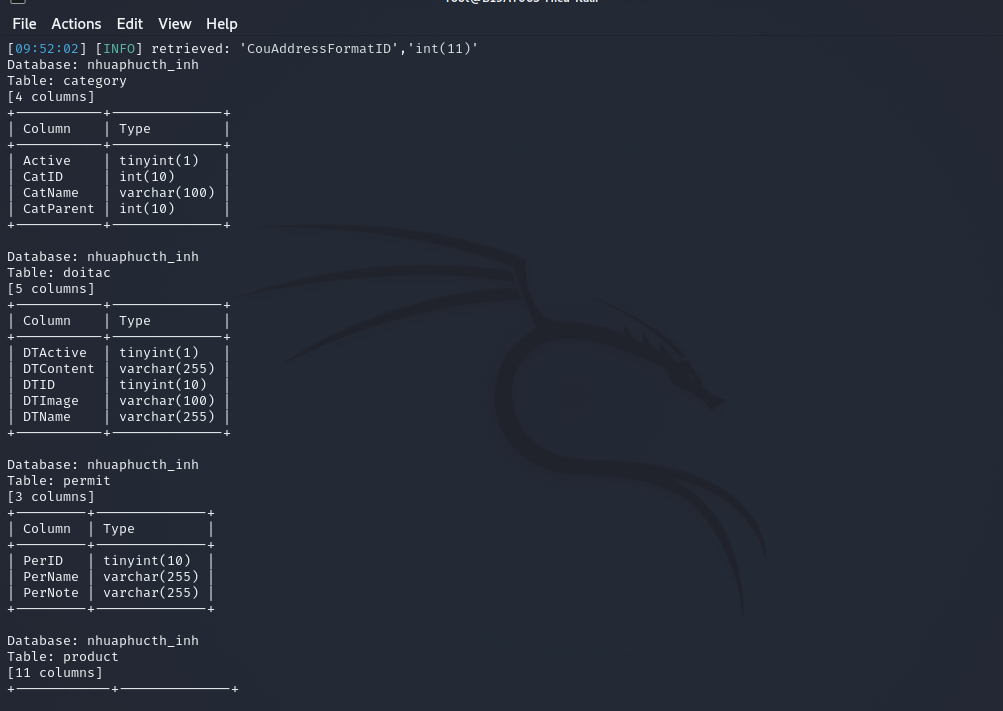




* **Trang** [**http://nhuaphucthinh.com.vn/product.php?id=35**](http://nhuaphucthinh.com.vn/product.php?id=35)

****

****

****