***BÁO CÁO BÀI THỰC HÀNH SỐ 5***

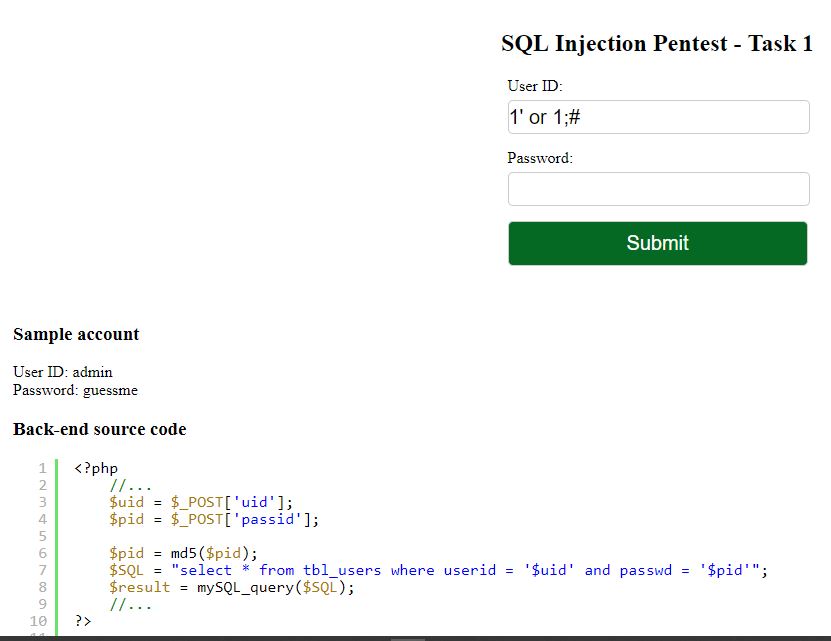
***KIỂM THỬ LỖ HỔNG SQL INJECTION***

***Họ và tên: Nguyễn Đăng Tới MSSV: 20153860***

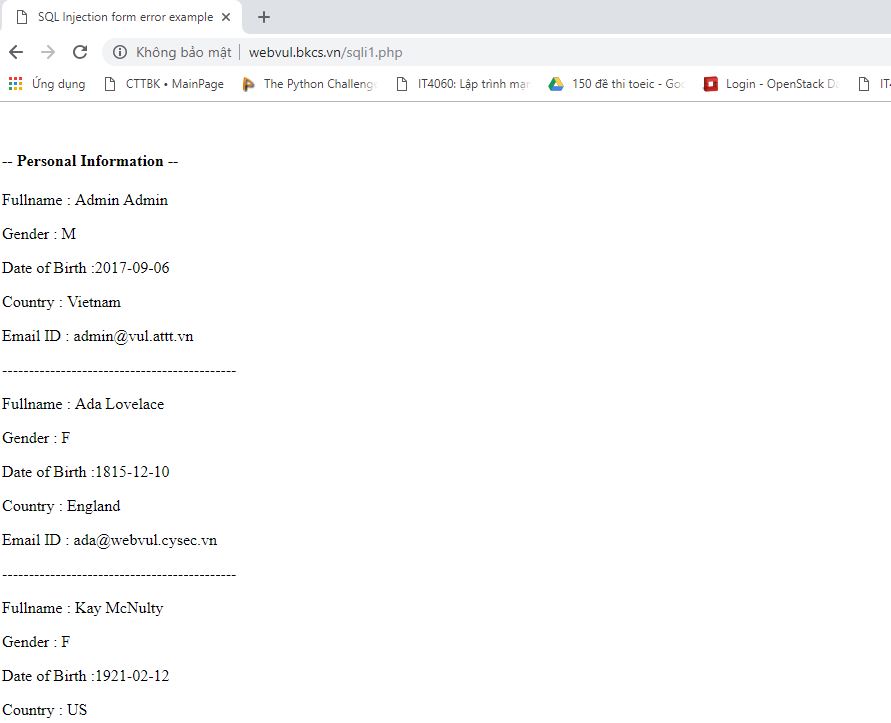
**Câu 1:**

* Cách thức xử lý tại back-end

Server lưu kết quả User ID và Password mà người dùng gửi lên vào lần lượt vào 2 biến uid và pid. Giá trị băm MD5 của pid sẽ được tính và lưu lại vào pid. Cuối cùng server thực hiện truy vấn bảng tbl\_users với giá trị userid là User ID và passwd là giá trị băm MD5 của Password.



* Giá trị kiểm thử



* Giải thích kết quả kiểm thử

Ta sẽ nhập chuỗi ***1’ or 1 = 1;#*** vào User ID. Khi đó câu truy vấn của server sẽ trở thành:

**select \* from tbl\_users where userid = *‘1’ or 1 = 1;#* and passwd = ‘$pid’;**

Lúc này kết quả trả về toàn bộ bảng tbl\_users vì điều kiện ***userid = ‘1’ or 1 = 1*** luôn cho kết quả là True. Dấu **;** sẽ kết thúc câu truy vấn và dấu **#** sẽ đánh dấu phần còn lại là chú thích, nên phần **passwd = ‘$pid’** sẽ không được truy vấn nữa.

**Câu 2:**

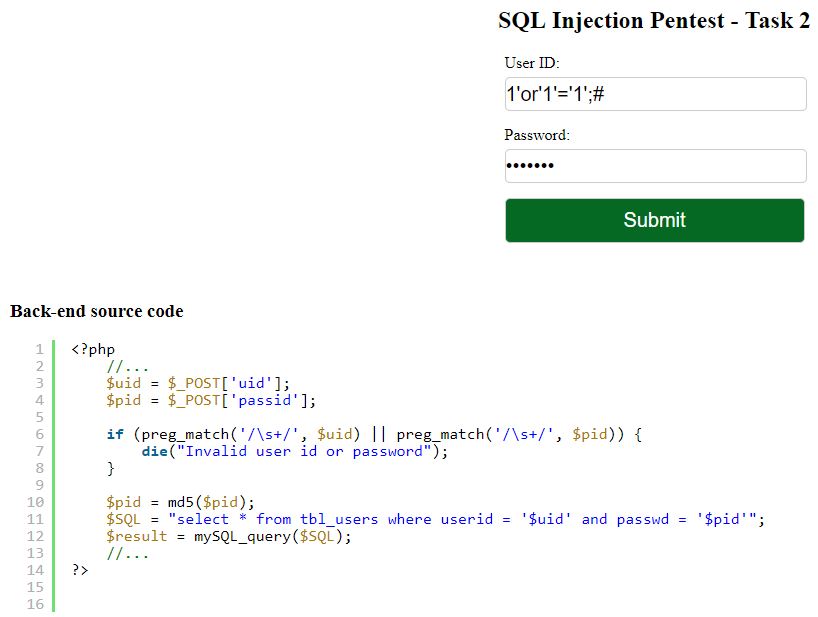
* Phân tích cách thức xử lý tại back-end

Server sẽ lưu giá trị User ID và Password người dùng gửi lên vào 2 biến uid và pid, sau đó tính giá trị băm MD5 của pid. Tiếp theo server thực hiện kiểm tra xem có dấu cách trong User ID và Password hay không, nếu có thì User ID hoặc Password sẽ được coi là không hợp lệ, nên không thể khai thác được theo cách 1 nữa.

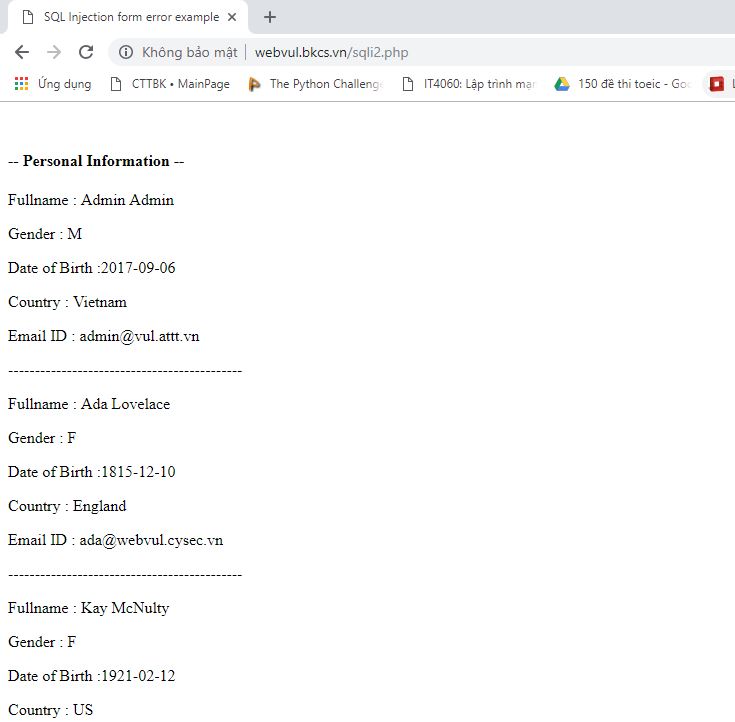
***if (preg\_match('/\s+/', $uid) || preg\_match('/\s+/', $pid)) {***

***die("Invalid user id or password");***

**}**



* Giá trị kiểm thử



* Giải thích kết quả kiểm thử :

Ta sẽ nhập chuỗi ***1’or’1’=’1’;#*** vào UserID. Không thể sử dụng dấu cách nữa nên chúng ta sẽ sử dụng dấu nháy đơn ‘ để ngăn cách các ký tự. Bây h câu truy vấn sẽ tương tự như câu 1.

**select \* from tbl\_users where userid = ‘1’or’1’=’1’;# and passwd = ‘$pid’;**

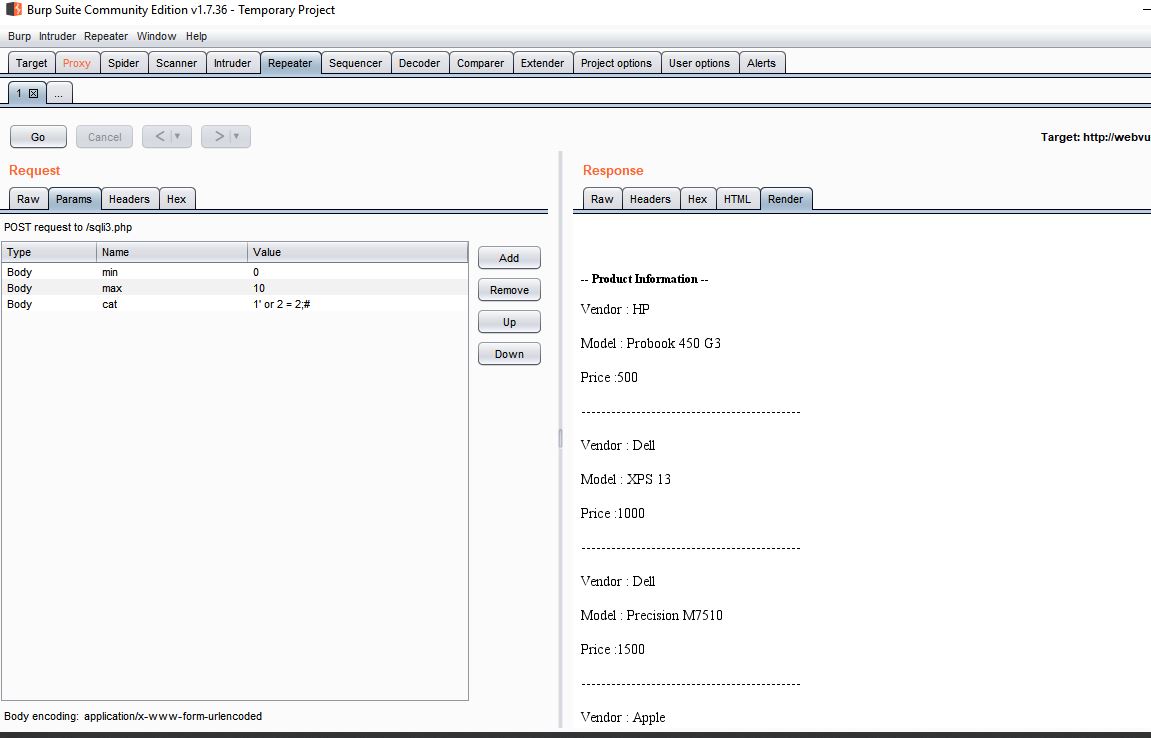
**Câu 3:**

* Cách thức xử lý tại back-end

Server thực hiện lưu các giá trị Min. price và Max.price mà người dùng gửi lên trong phương thức POST vào 2 biến min và max. Sau đó Server kiểm tra xem giá trị của min và max có phải là số hay không, nếu không sẽ thông báo giá trị không hợp lệ. Biến min sẽ được gán giá trị 0 nếu min < 0 và max sẽ được gán giá trị 1000000 nếu max > 1000000. Cuối cùng server thực hiện truy vấn trong bảng tbl\_product với category là giá trị category trong phương thức POST , và price nằm trong khoảng min và max.



* Giá trị kiểm thử



* Giải thích kết quả kiểm thử

Dùng BurpSuite để gửi HTTP Request lên server với giá trị cat trong phương thức POST là ***1’ or 2 = 2;#*** và khi đó câu truy vấn sẽ trở thành:

**select \* from tbl\_product where category = '1' or 2 = 2;# and price <= $max and price >= $min**

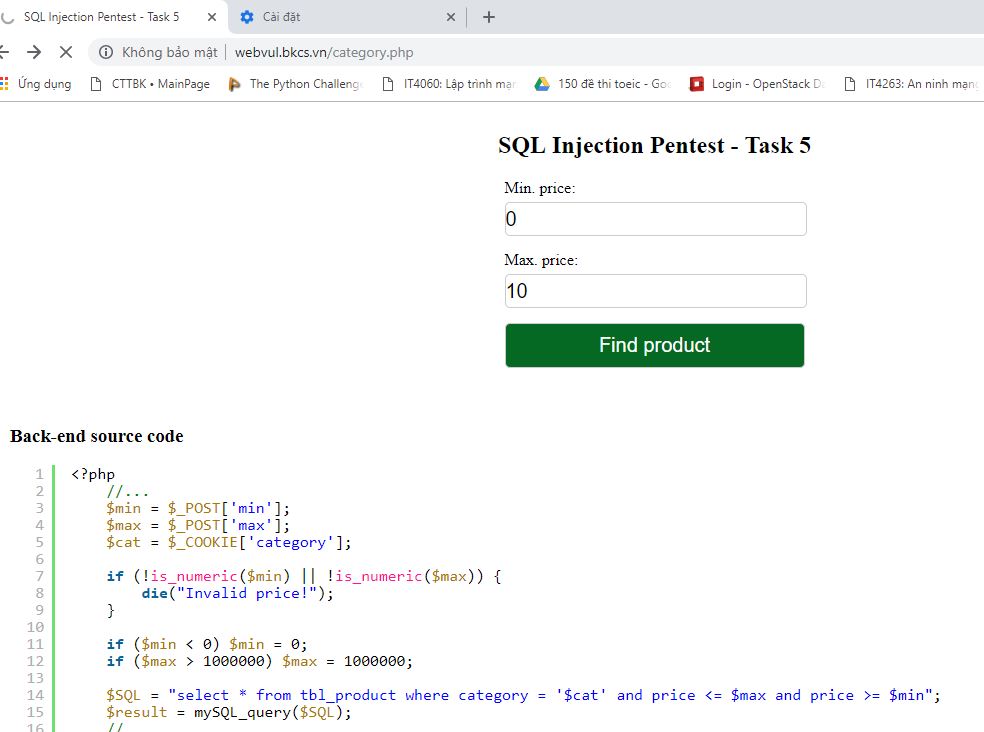
Bây h câu truy vấn sẽ trả lại cho chúng ta toàn bộ bản ghi trong bảng tbl\_product vì điều kiện **category = '1' or 2 = 2** luôn đúng, và toàn bộ phần truy vấn price sau đó sẽ không được thực hiện.

**Câu 4:**

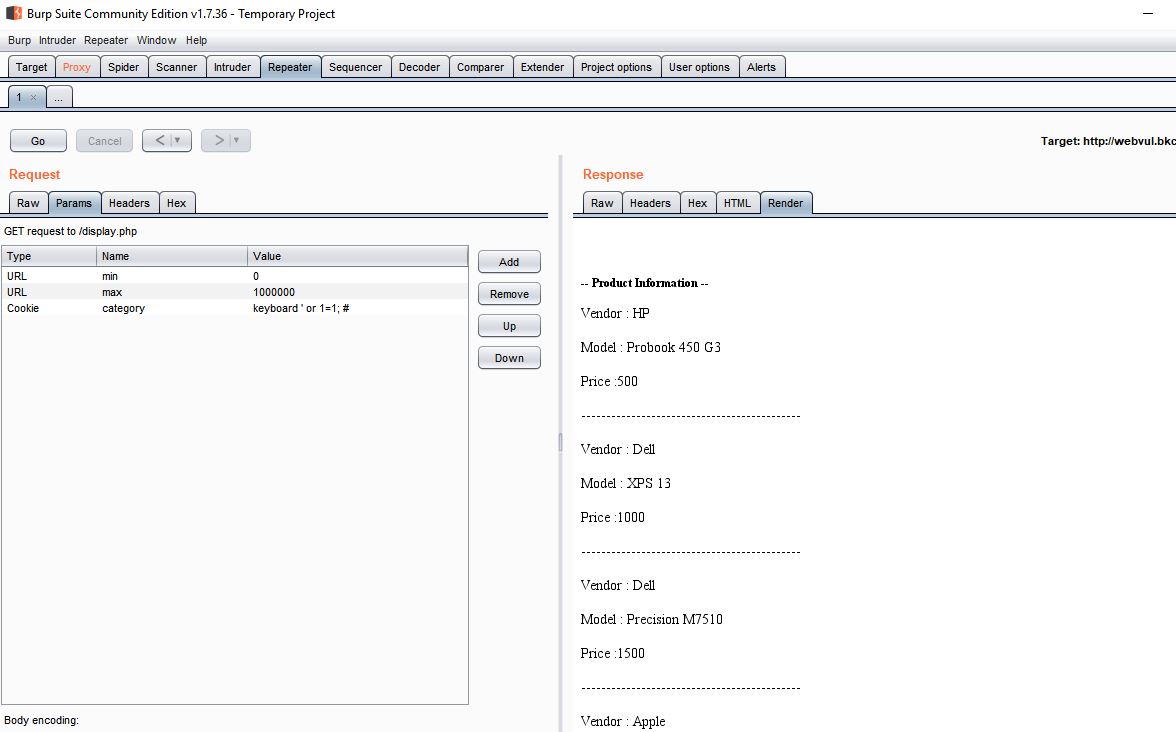
**Câu 5:**

* Cách thức xử lý tại back-end

Server sẽ lưu các giá trị Min. price và Max.price mà người dùng gửi lên vào 2 biến min và max. Khi người dùng chọn product category, thì giá trị của category sẽ được lưu vào cookie “category”. Sau đó Server kiểm tra xem giá trị của min và max có phải là số hay không, nếu không sẽ thông báo giá trị không hợp lệ. Biến min sẽ được gán giá trị 0 nếu min < 0 và max sẽ được gán giá trị 1000000 nếu max > 1000000. Cuối cùng server thực hiện truy vấn trong bảng tbl\_product với category là giá trị của cookie “category”, và price nằm giữa 2 giá trị min và max.



* Giá trị kiểm thử



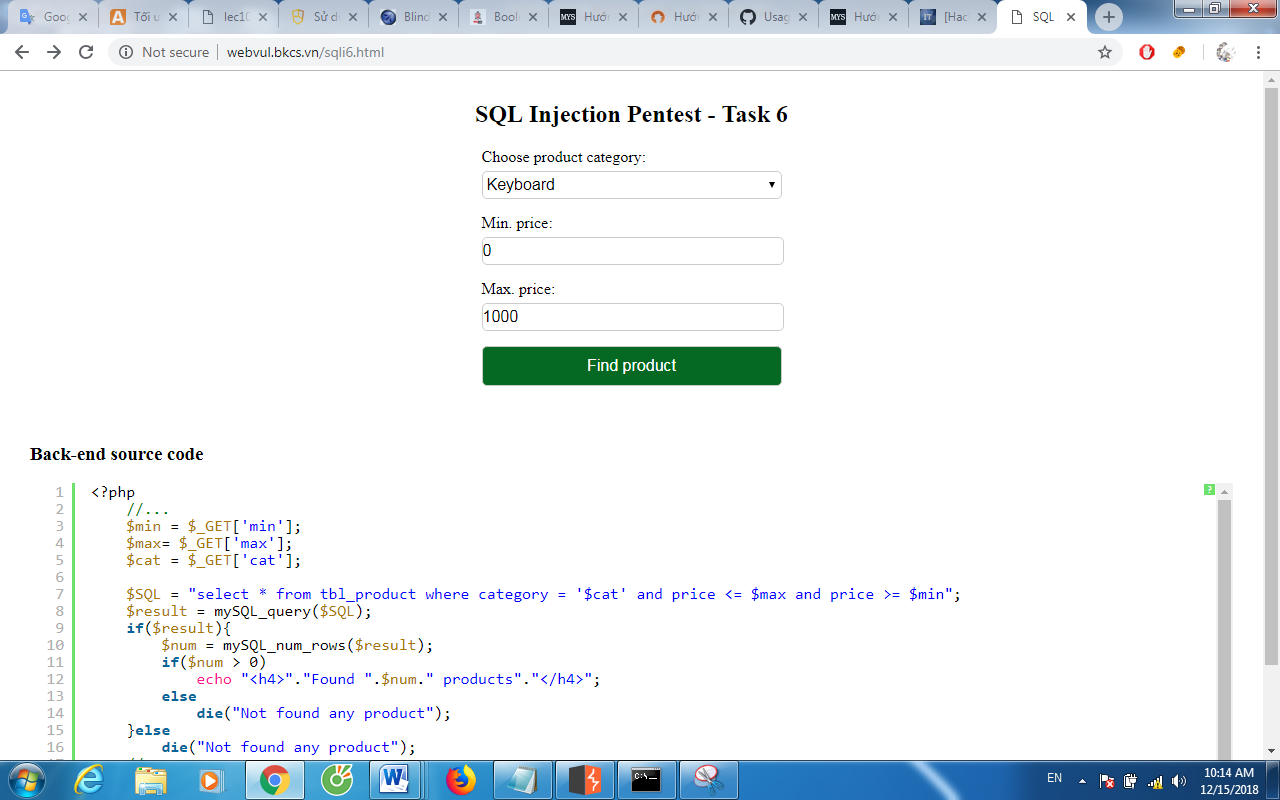
* Giải thích kết quả kiểm thử (cần phân tích rõ tại sao với giá trị kiểm thử đã sử dụng cho kết quả kiểm thử như vậy)

Ta sẽ dùng Burp Suite để gửi HTTP Request lên server với giá trị cookie “category” là **1’ or 1 = 1;#** và khi đó câu truy vấn sẽ trở thành:

**select \* from tbl\_product where category = 'keyboard' or 1 = 1;# and price <= $max and price >= $min**

Bây h câu truy vấn sẽ trả lại cho chúng ta toàn bộ bản ghi trong bảng tbl\_product vì điều kiện **category = 'keyboard' or 1 = 1** luôn đúng, và toàn bộ phần truy vấn price sau đó sẽ không được thực hiện.

**Câu 6:**



* Cách làm và kiểm thử:

Bước 1: Chúng ta khởi động sqlmap : trong windows đến thư mục Python27 -> sql



Bước 2: Tiếp theo chạy câu lệnh:

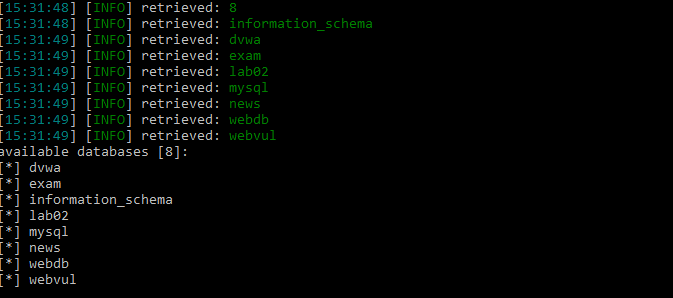
**Sqlmap.py –u “http://webvul.bkcs.vn/sqli6.php?cat=keyboard&min=0&max=1000” --dbs**

trong dó

–u kiểm tra câu truy vấn theo sau có lỗi sqli hay ko?

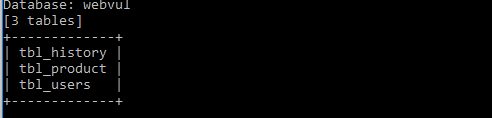
--dbs để xem tất cả các cơ sở dữ liệu khả dụng trong máy

Sau khi tìm đc dữ liệu cần tìm ta tiếp tục gõ lệnh:



**Sqlmap.py –u “http://webvul.bkcs.vn/sqli6.php?cat=keyboard&min=0&max=1000**” **–D webvul --tables**

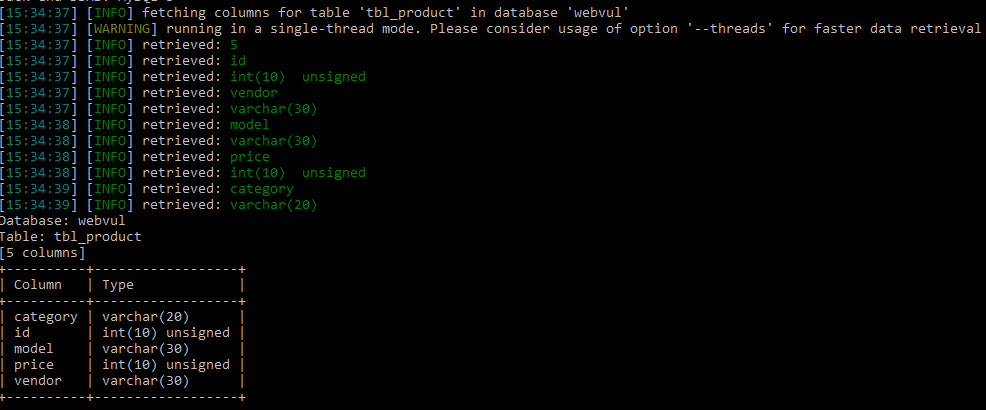
-D báo cho chương trình biết mình sẽ làm việc với database là webvul và - -tables để show ra bản của sơ sở dữ liệu ấy



Bước 3:

**Sqlmap.py –u “http://webvul.bkcs.vn/sqli6.php?cat=keyboard&min=0&max=1000**” **–D webvul –T tbl\_product - -columns**

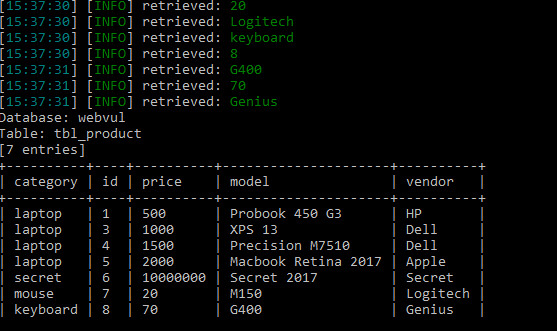
-T cho biết chương trình sẽ làm việc với bảng tcl\_product và --columns để show toàn bộ các cột trong bảng



Bước 4:

**Sqlmap.py –u “http://webvul.bkcs.vn/sqli6.php?cat=keyboard&min=0&max=1000**” **–D webvul –T tbl\_product –C category,id,price,model,vendor - - dump**

-C để làm việc với các cột của bảng - -dump để dump tất cả dữ liệu của cột



Một số cách thức kiểm thử để có thể xác định được tên và phiên bản của phần mềm quản trị CSDL

* Phân này em có tìm hiểu trên mạng

**Thử nghiệm 1: xác định cơ sở dữ liệu**

Cơ sở dữ liệu ở đây là MySQL, làm thế nào chắc chắn rằng đó là bằng cách thử một số truy vấn cơ bản mà MySQL, MsSQL, postgreSQL và Oracle sử dụng như là mặc định tương ứng. Nếu có thể chỉ ra một cái cung cấp cho bạn đầu ra Boolean mong muốn, bạn có thể tìm ra cơ sở dữ liệu, nhưng nó là một công việc sẽ phải lặp đi lặp lại nhiều lần

**MYSQL sử dụng nhận xét là – – [dấu gạch đôi đòi hỏi 1 không gian sau nó] và #**

**1 ’AND 1 = 1 – -> hoạt động**

**1 ’AND 1 = 1 #> hoạt động**

**MSSQL và Oracle sử dụng – [không có khoảng trống sau dấu gạch đôi] hoặc / \* \* / [nhiều dòng chú thích]**

**1 ’AND 1 = 1 -> không hoạt động**đã sử dụng dấu gạch ngang kép không có khoảng trống nhưng nó không hoạt động. Điều này loại bỏ khả năng cơ sở dữ liệu là của MSSQL hoặc Oracle hoàn toàn.

**Thử nghiệm 2: xác định version của cơ sở dữ liệu**

**MySQL sử dụng phiên bản @@ và phiên bản () để kiểm tra phiên bản.**  
**MSSQL sử dụng phiên bản @@ để kiểm tra phiên bản   
Oracle sử dụng SELECT banner FROM v $ version**

Cả hai phiên bản @@ và version () đều làm việc ở đây.   
Do đó cho câu trả lời rằng đó là cơ sở dữ liệu MySQL ở phần phụ trợ

Có rất nhiều cách khác để kiểm tra hành vi của ứng dụng và tìm ra cơ sở dữ liệu nào nó sử dụng nhưng cho ứng dụng này là đủ.

Em đã sử dụng các truy vấn sau đây, nhận được một số thông tin về cơ sở dữ liệu.

**1 ' and substring (@@ version, 1,1) = 4**

**#**

**Hàm substring bên trên sẽ lấy kí tự đầu tiên của version database so sánh với 4**

Nếu version là 4 thì trả về truy vấn là TRUE

Sử dụng công cụ sqlmap trả về tên database cũng như loại cơ sở dữ liệu

Truy vấn: ***sqlmap.py –u “—url—“ --dbs***