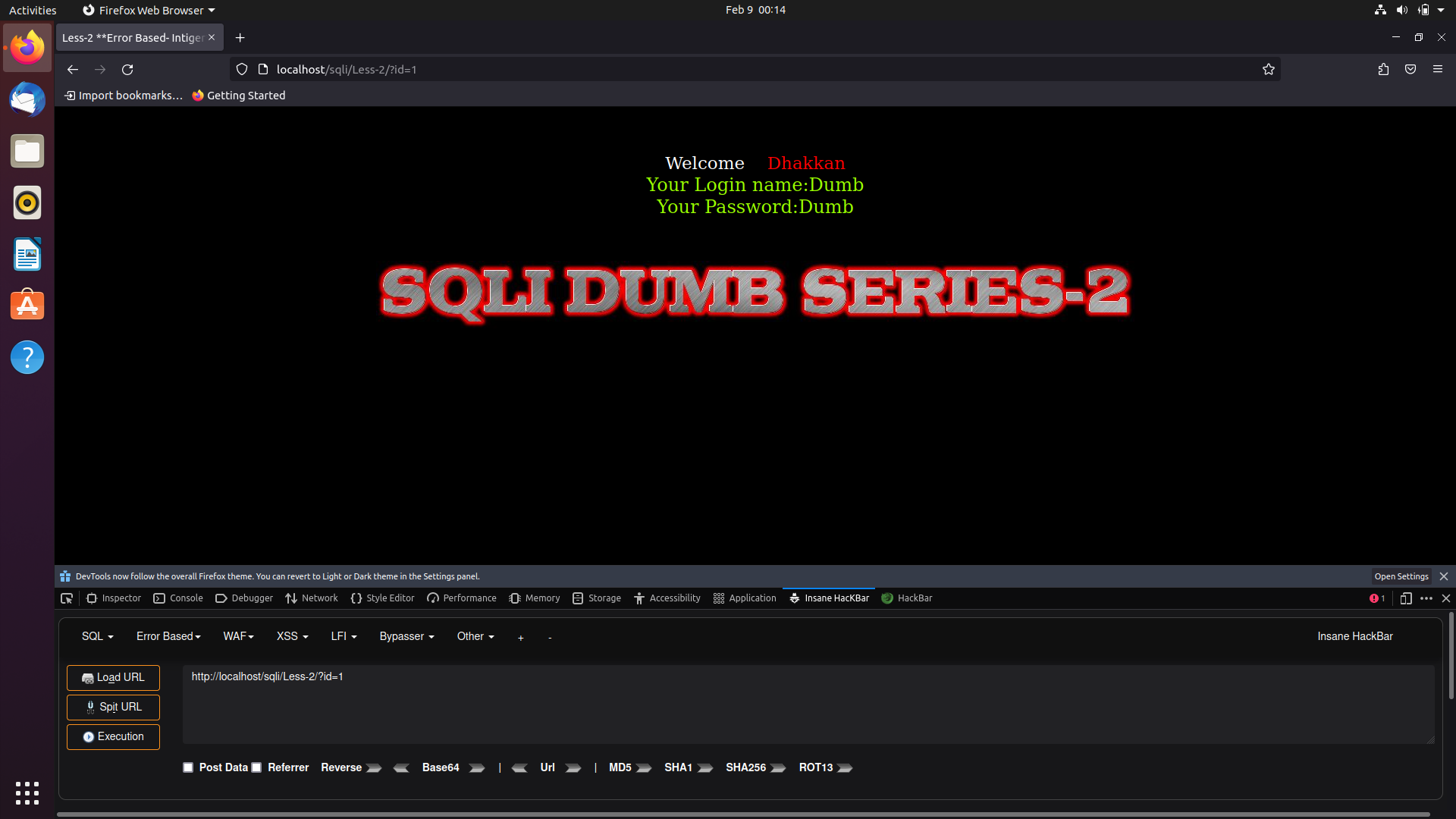
**SQLI LABS** - *LESS2*

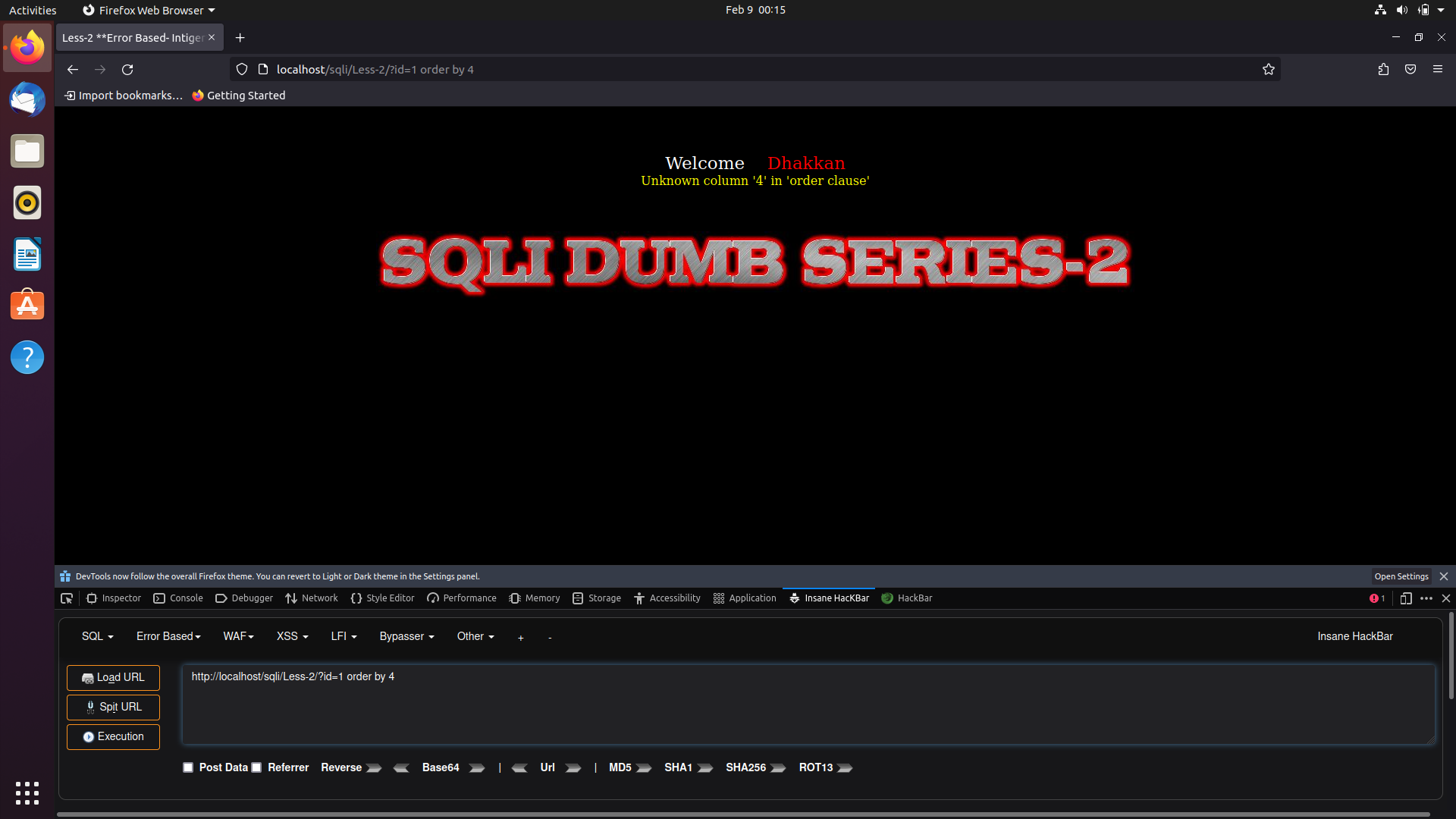
We start by testing the ID parameter in with a numeric value, thereby we add **?id=1**

Now when we run or execute the URL again we get a login name and password.

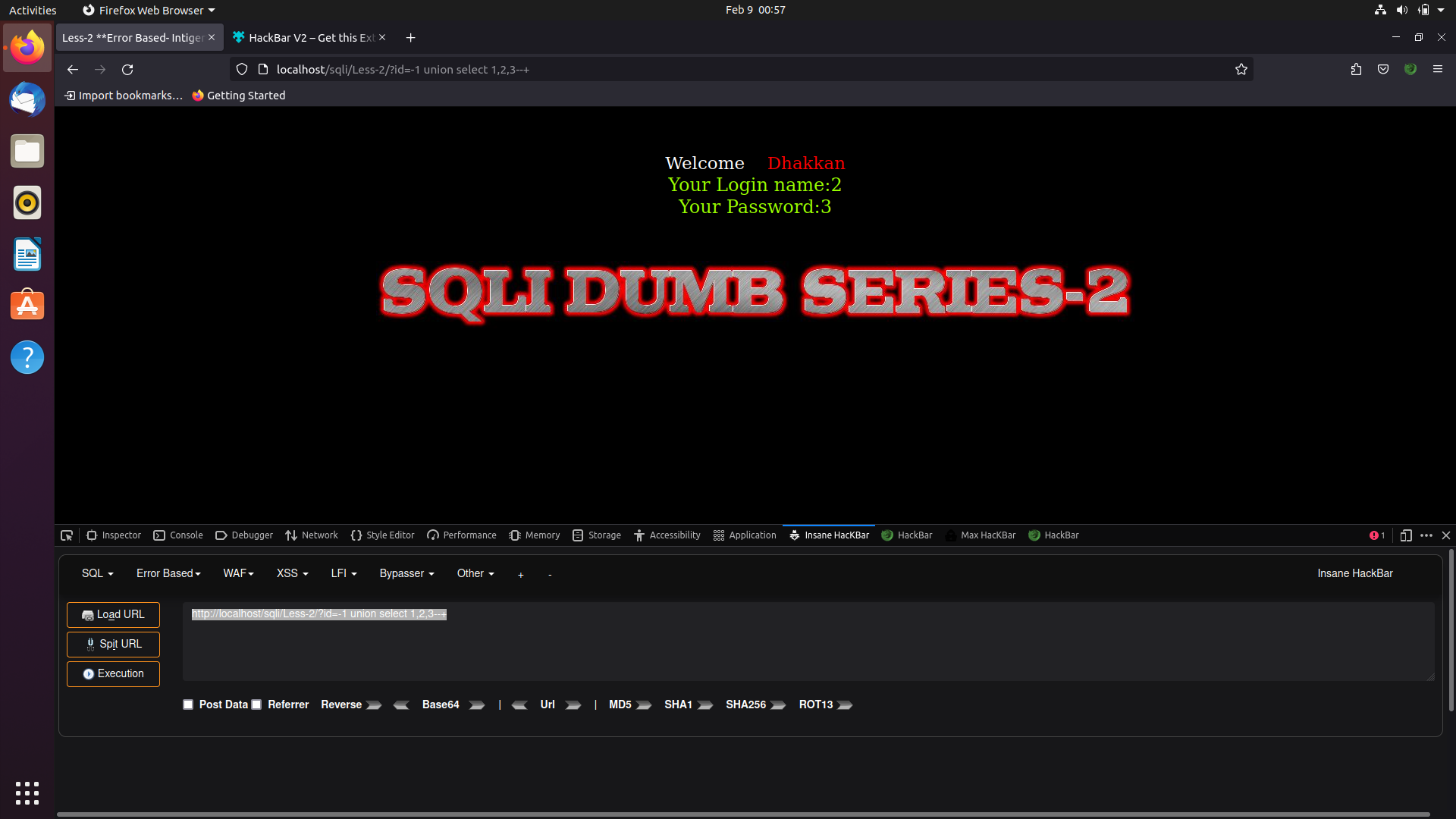
Similar to the last lesson this also has only a certain set of cases that ranges from 1-14.



By using the order functionality we will be able too see the number of tables that are committed to the database, in this case it is 3.



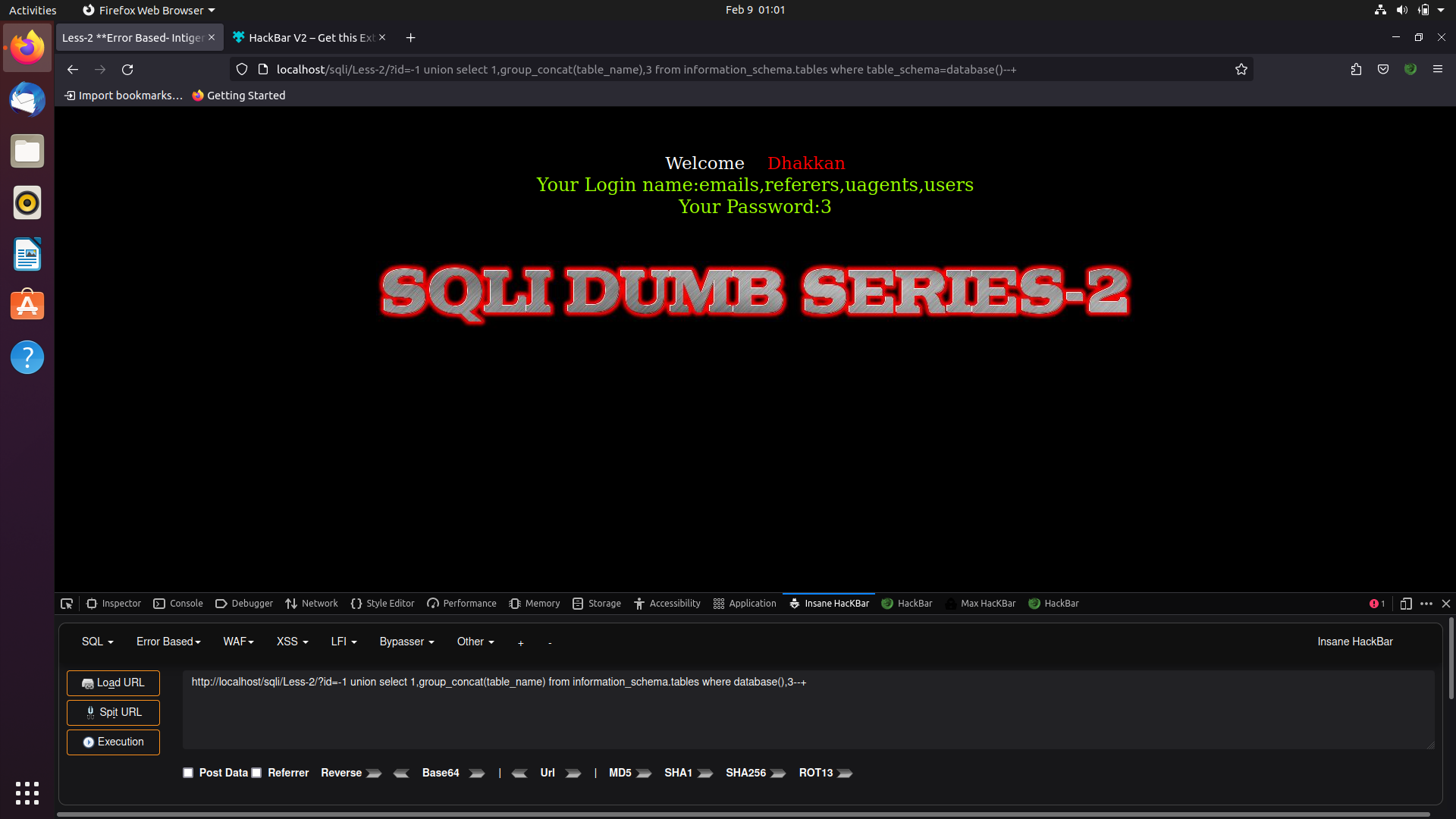
Now we perform aunion attack on the URL and we find that 2 and 3 are vulnerable and can be injected to retrieve data.



Now we can use the union attack functionality as padding and get the SQL query injected directly into the Database.

We will get the names of the tales that are present in the database using the following query

And list them



Now we will replace the tables by columns and collect the data from the user by group concat functionality in the URL.

On executing this it will give us a list of usernames and passcodes as follows:

