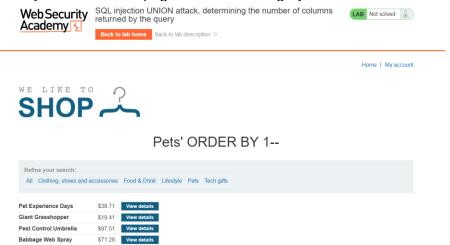
TASK 1

In this lab, we are required to find the number of fields in the table by performing a UNION SELECT injection.

There are two ways to do this:1. Using ORDER BY, where we will iterate over the values until we encounter a server error. That is:

Modify the URL of the page to .. /filter?category=Pets'+ORDER+BY+1-



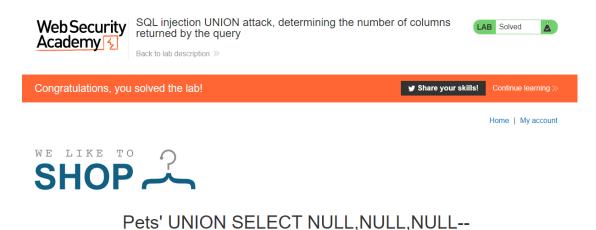
If the request is processed successfully, increase the last value by 2, 3, and so on.



This means that the table under study has 3 fields.

2. Using a UNION SELECT query of the form: '+UNION+SELECT+NULL--

In this case, we will observe the error until the number of selected items is equal to the number of fields in the table. Add NULL to the query separated by commas until the request is successfully processed:



Refine your search: All Clothing, shoes and accessories Food & Drink Lifestyle Pets Tech gifts Pet Experience Days \$38.71 View details Giant Grasshopper \$19.41 View details Pest Control Umbrella \$97.51 View details Babbage Web Spray \$71.28 View details

So, we have confirmed that there are 3 fields in the table.

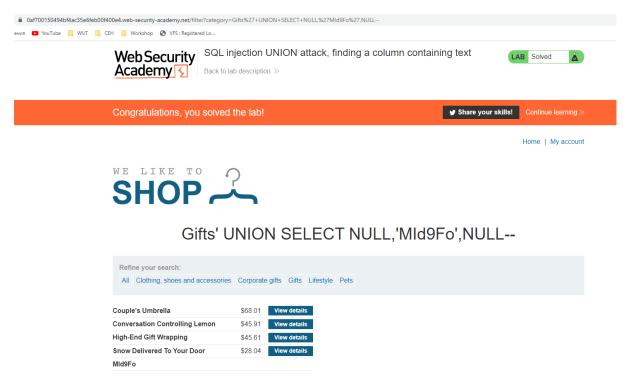
TASK 2

This time, you need to know in which of the fields the text type data is stored.

To do this, you need to modify the query from the previous job by replacing one of the null values with an arbitrary text string. Let's say 'MId9Fo', as suggested by the lab.



The attempt was unsuccessful: (This means that the first field contains something else. Most likely, this will be an integer numeric value-identifier of the item item.



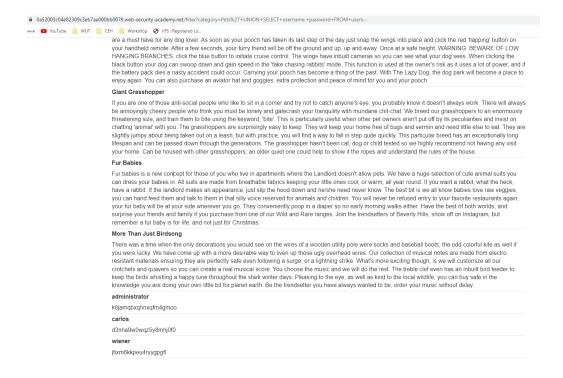
Everything worked out with the second field, and as you can see, our row was added to the very bottom of the existing table.

So, field No. 2 contains text data.

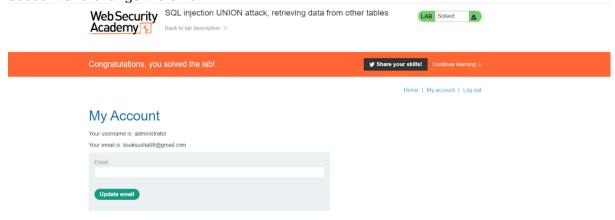
TASK 3

Based on the description of the task, we know that there is a users table in the database with username and password fields. Knowing this information, we can try to extract the data stored in it and try to access the administrator account. Let's use the same UNION SELECT:

'UNION SELECT username, password FROM users-:



We can see how records with existing users have been added at the bottom, including the administrator, who should have been fired for such carelessness. Now we can log in to his account and change the email:



In the course of this task, we learned how to get data from other tables.