Report on Portswigger Lab

Submitted by:

Uttam Kumar Rajbanshi

Submitted to:

Director of SB Computer

**Date: 2023-01-05**

**Time: 06:00 PM**

Contents

# Lab 1: SQL injection vulnerability in WHERE clause allowing retrieval of hidden data

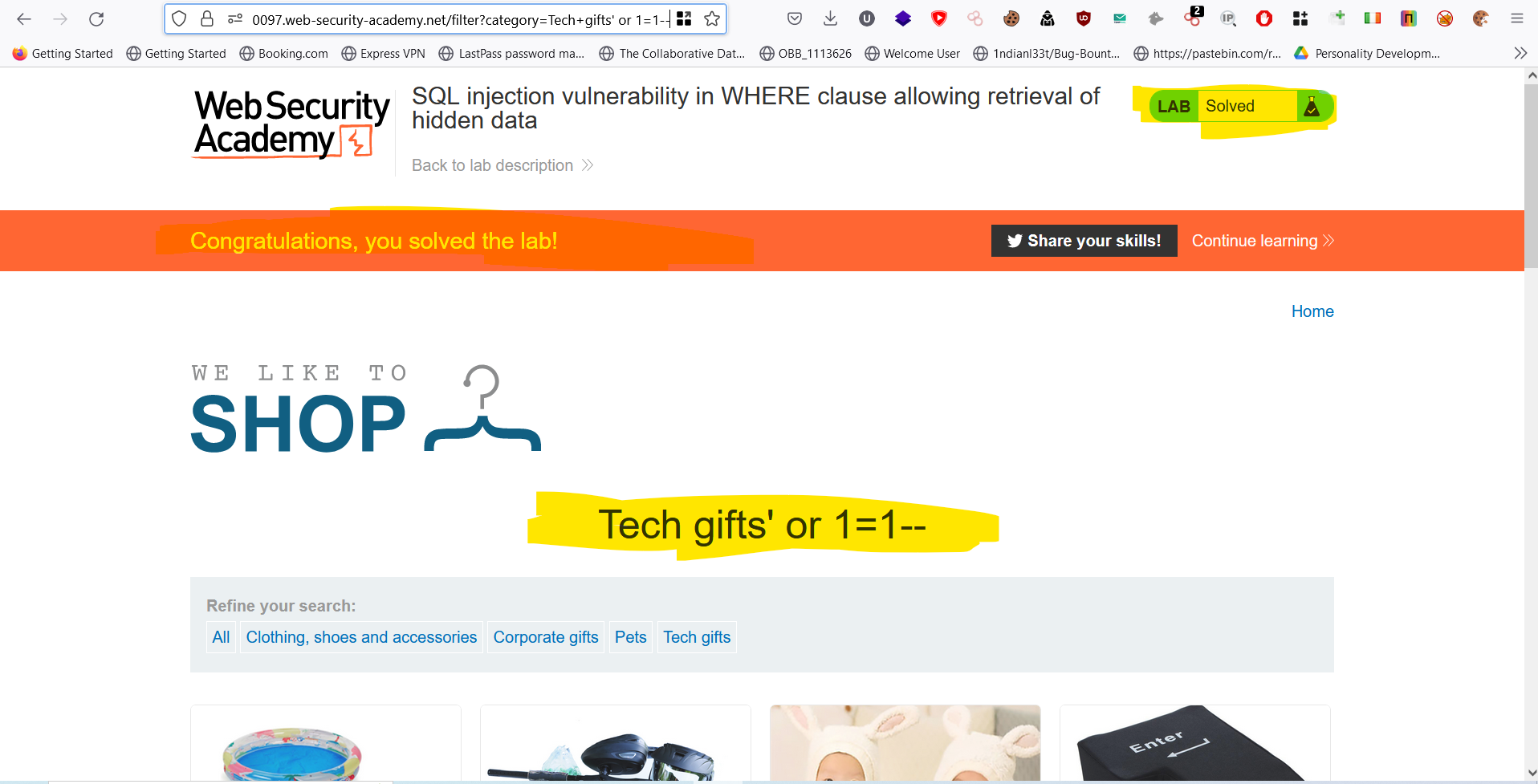
Graphical user interface, text, application, chat or text message, website

Description automatically generated

I found Categories sections like gifts, accessories, Clothes etc. It uses a get parameter as we can see in the above highlighted area in above screenshot. After that I tried ‘ in the parameter and it gave me internal server error as below picture. Graphical user interface, text, application, Word

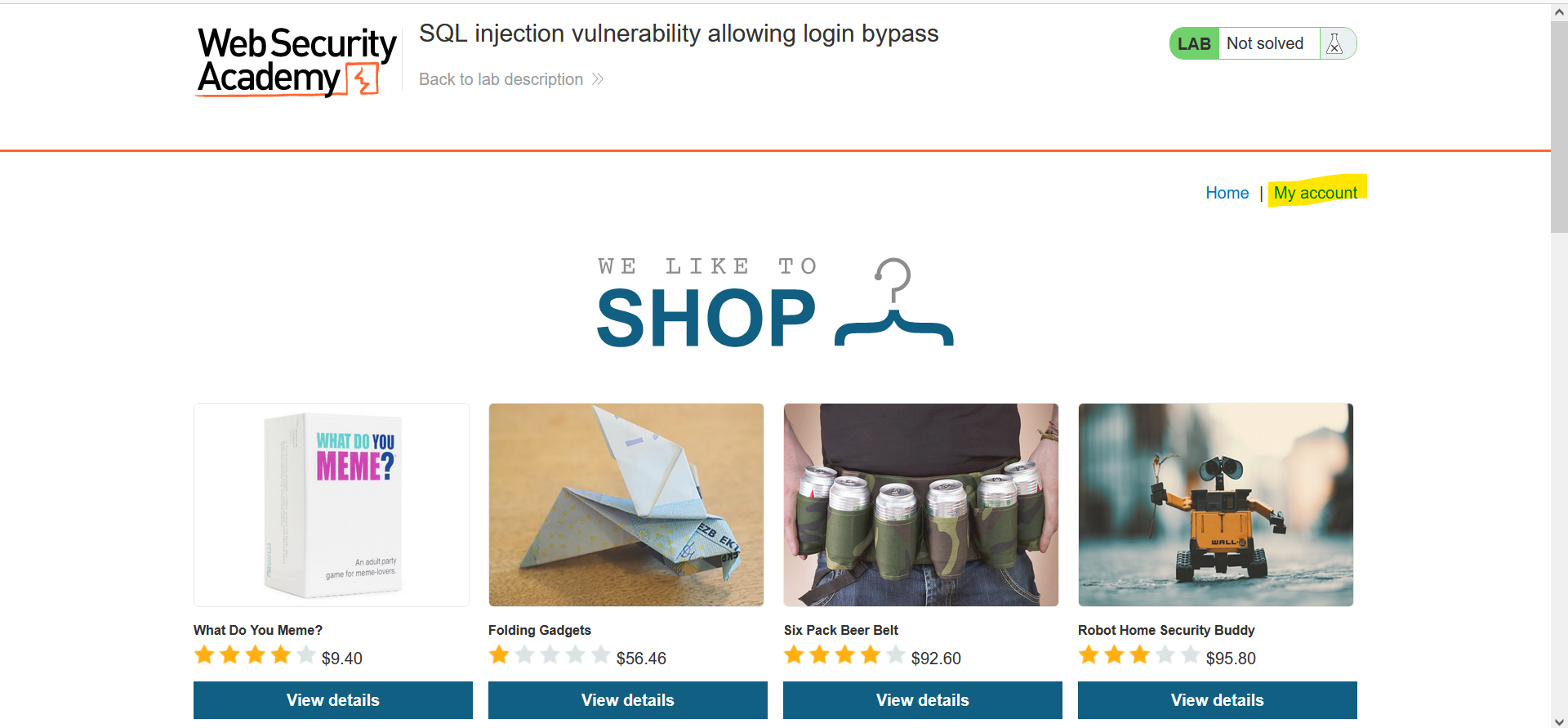
Description automatically generated

After that I used Gifts’ or 1=1-- for exploitation, it gave me administrator login.

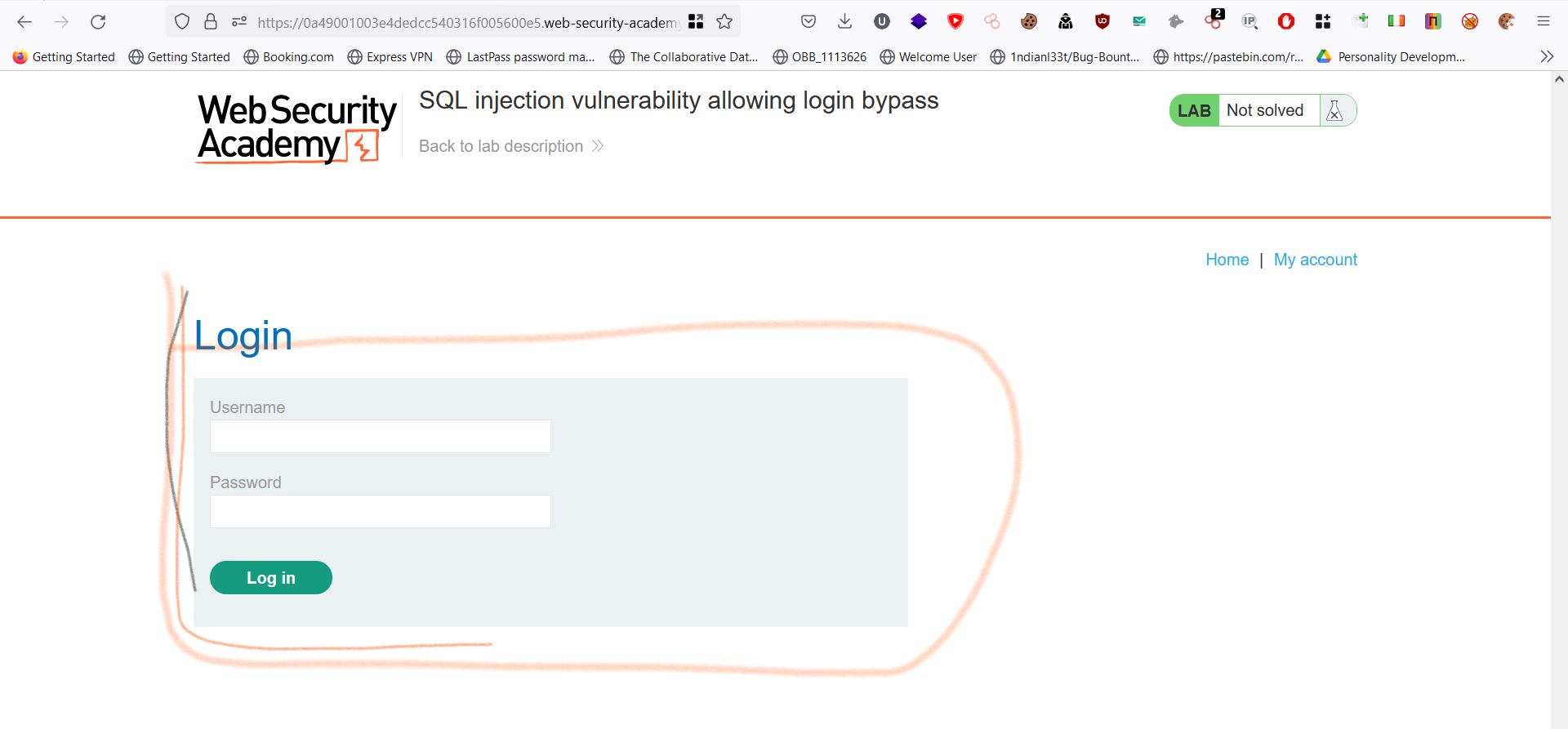


We can see I got congratulation message that means our lab has been solved.

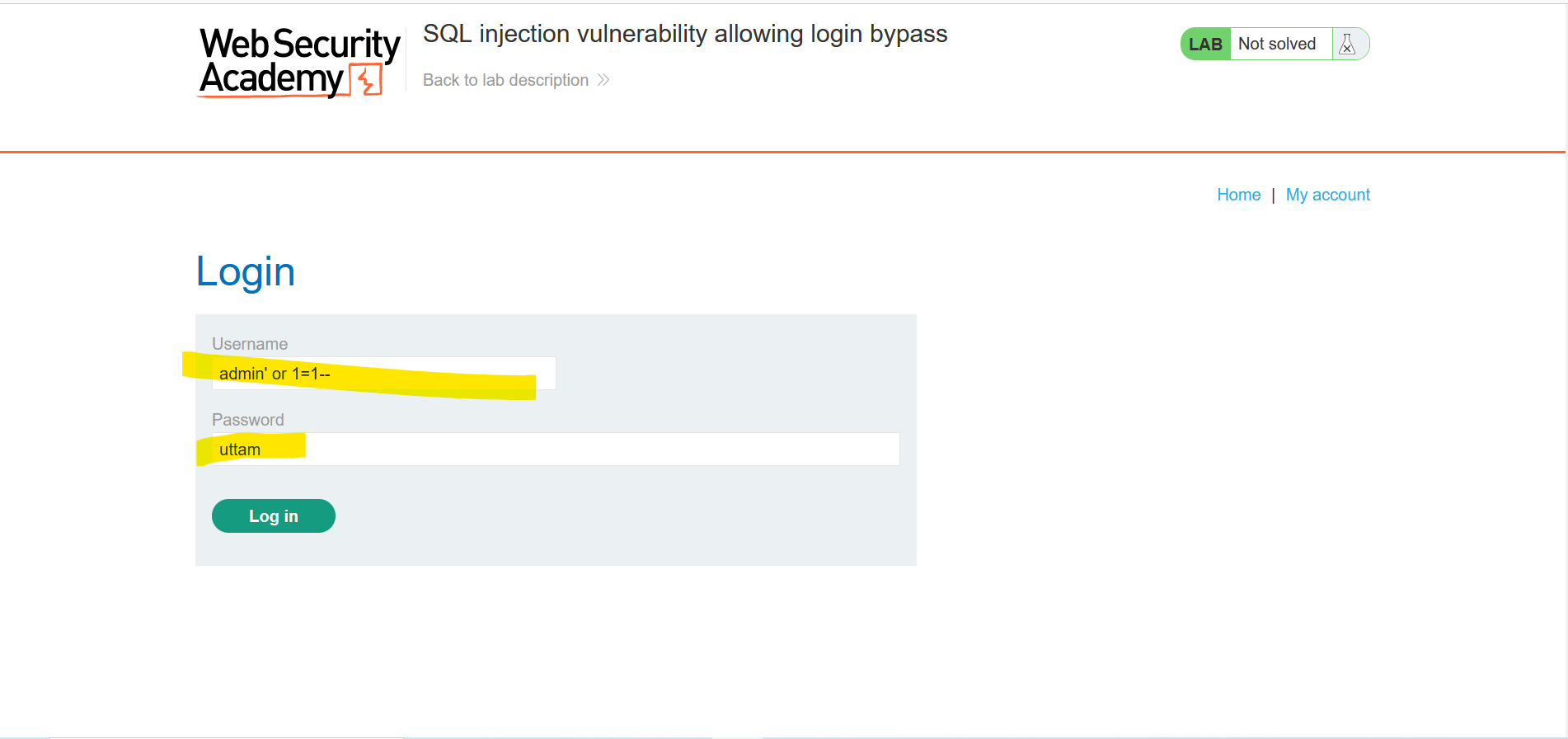
# Lab 2: SQL injection vulnerability allowing login bypass

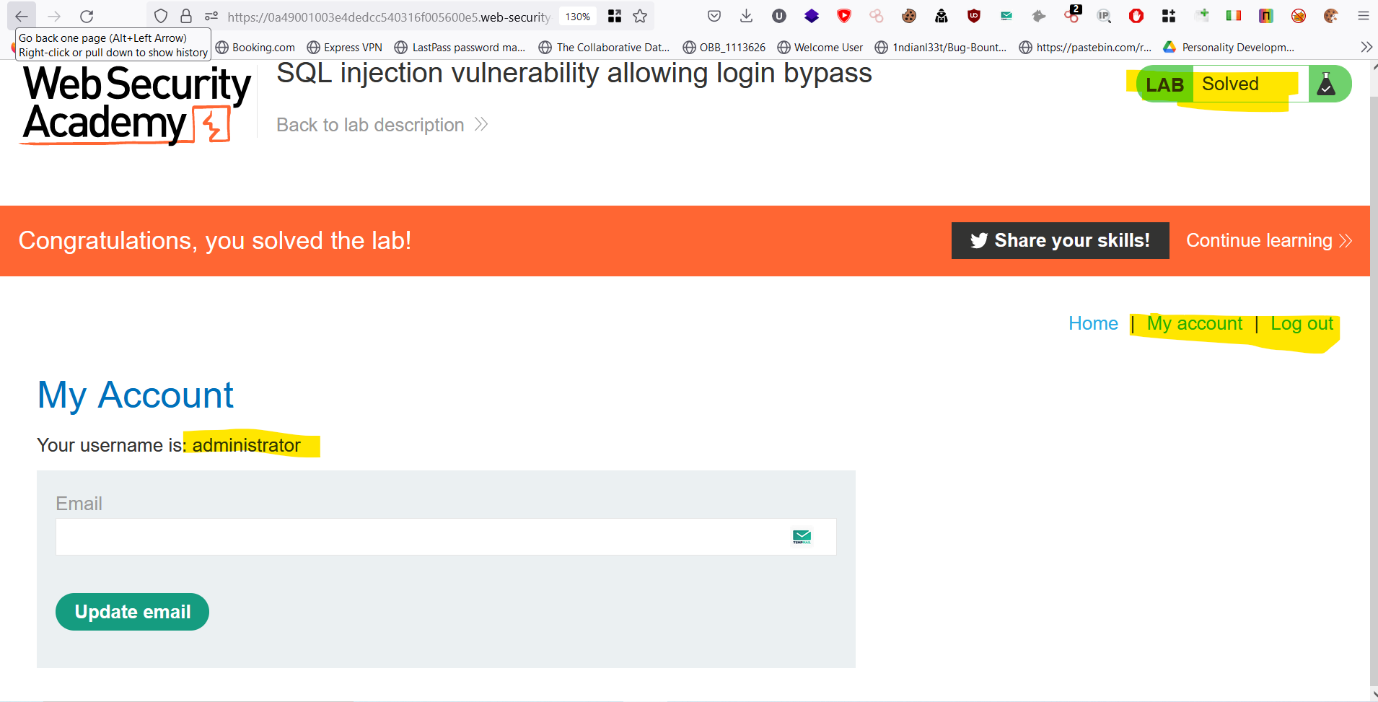


In this lab we don’t have categories parameter, instead of that we have my account we can see in the above picture. In there we have login page, we users can login using credentials.



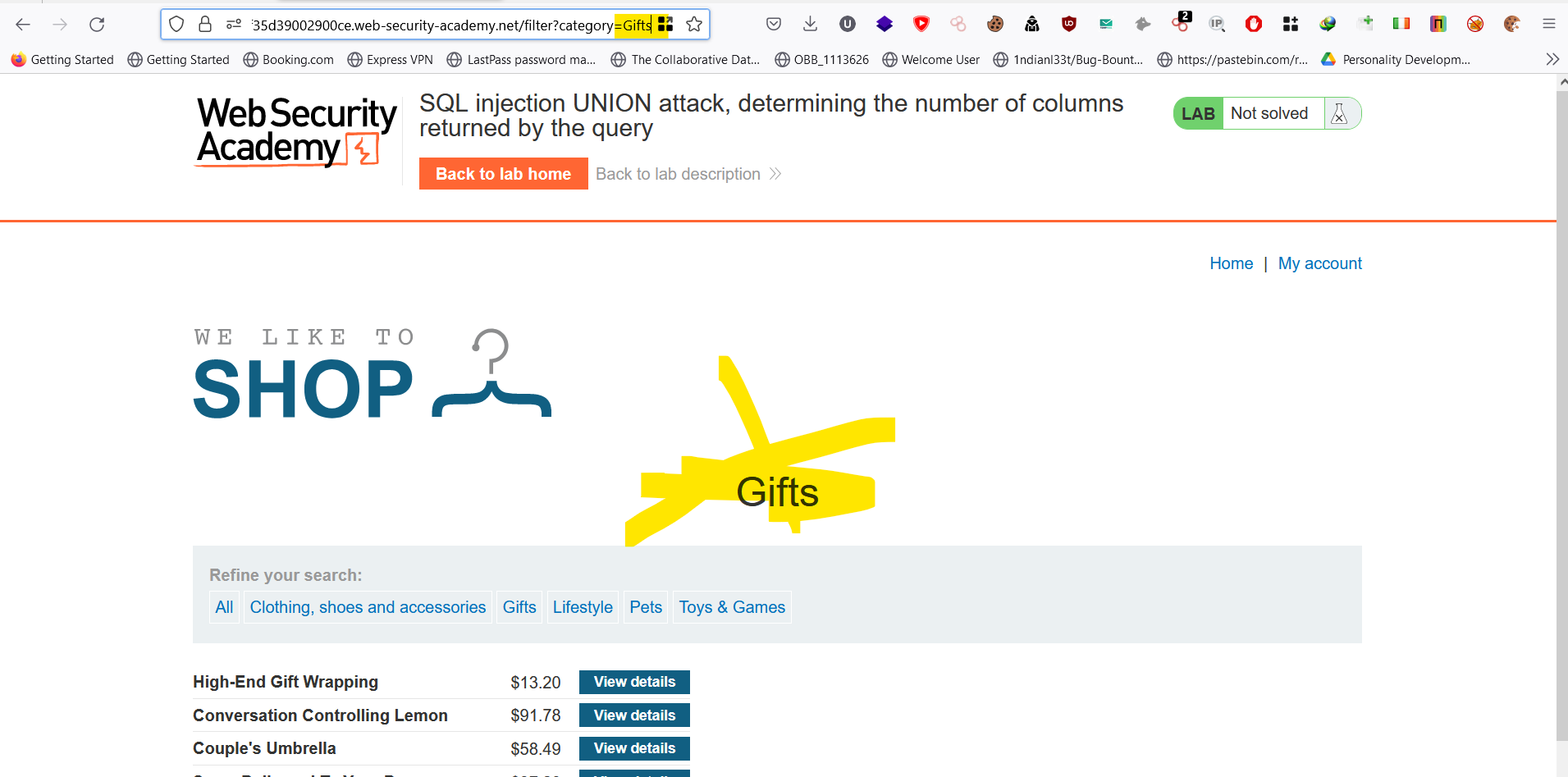
I tried sql injections in the input parameter. Like in the below picture.



In the username I used OR Boolean syntax as shown in the above picture and in the password I used any random character.

Using the above techniques I was able to logged in as an administrator.

# Lab 3: SQL injection UNION attack, determining the number of columns returned by the query

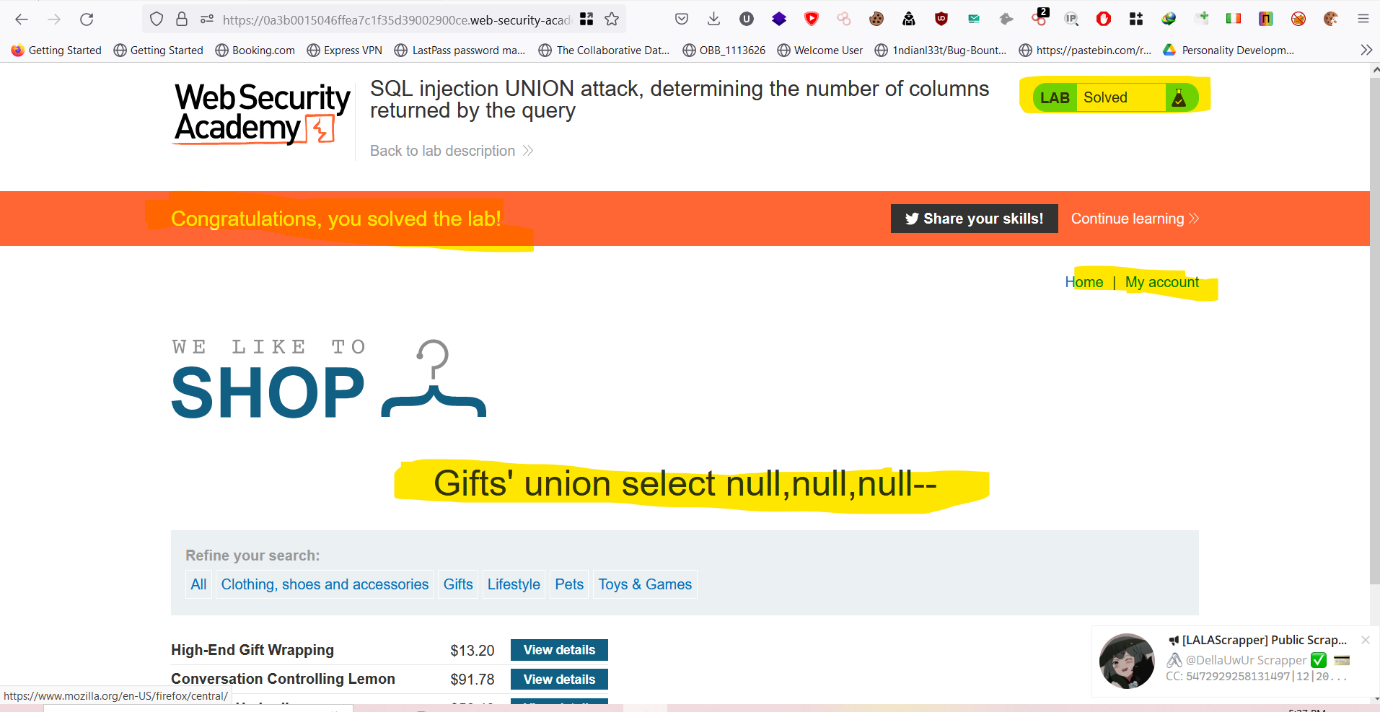


Here I got parameter in the categories section.

Graphical user interface, text, application, email

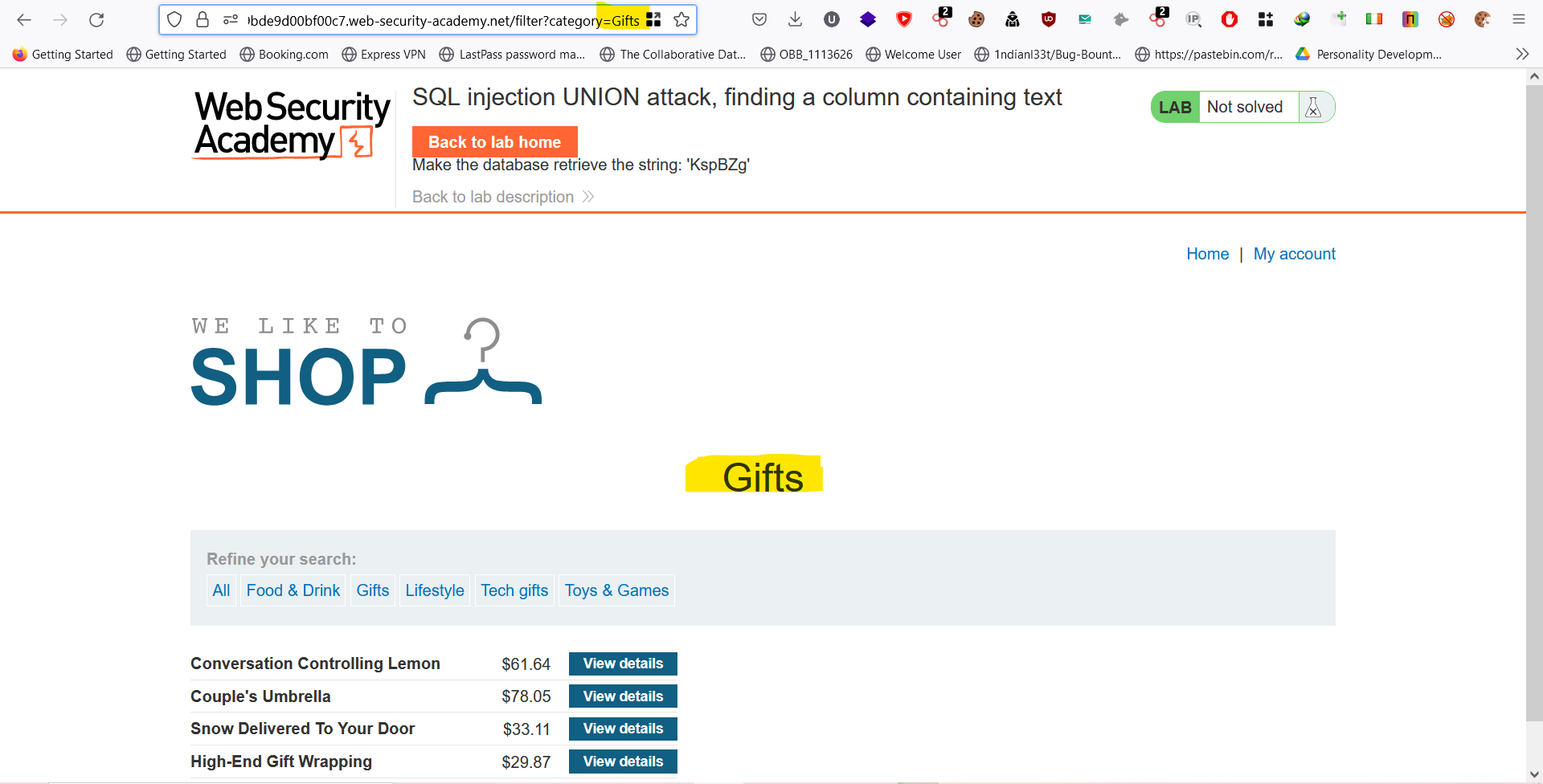
Description automatically generated

After that I used ‘ in the parameter to check either error is generated or not, but I got an error as seen in the above picture.



After that I used SQL command ‘ union select null,null,null -- and got to know that there are three column in the data base because we are able to get only three null statement. And here we solved the lab.

# Lab 4: SQL injection UNION attack, finding a column containing text



Got parameter in the categories section.

Graphical user interface, text, application, Word

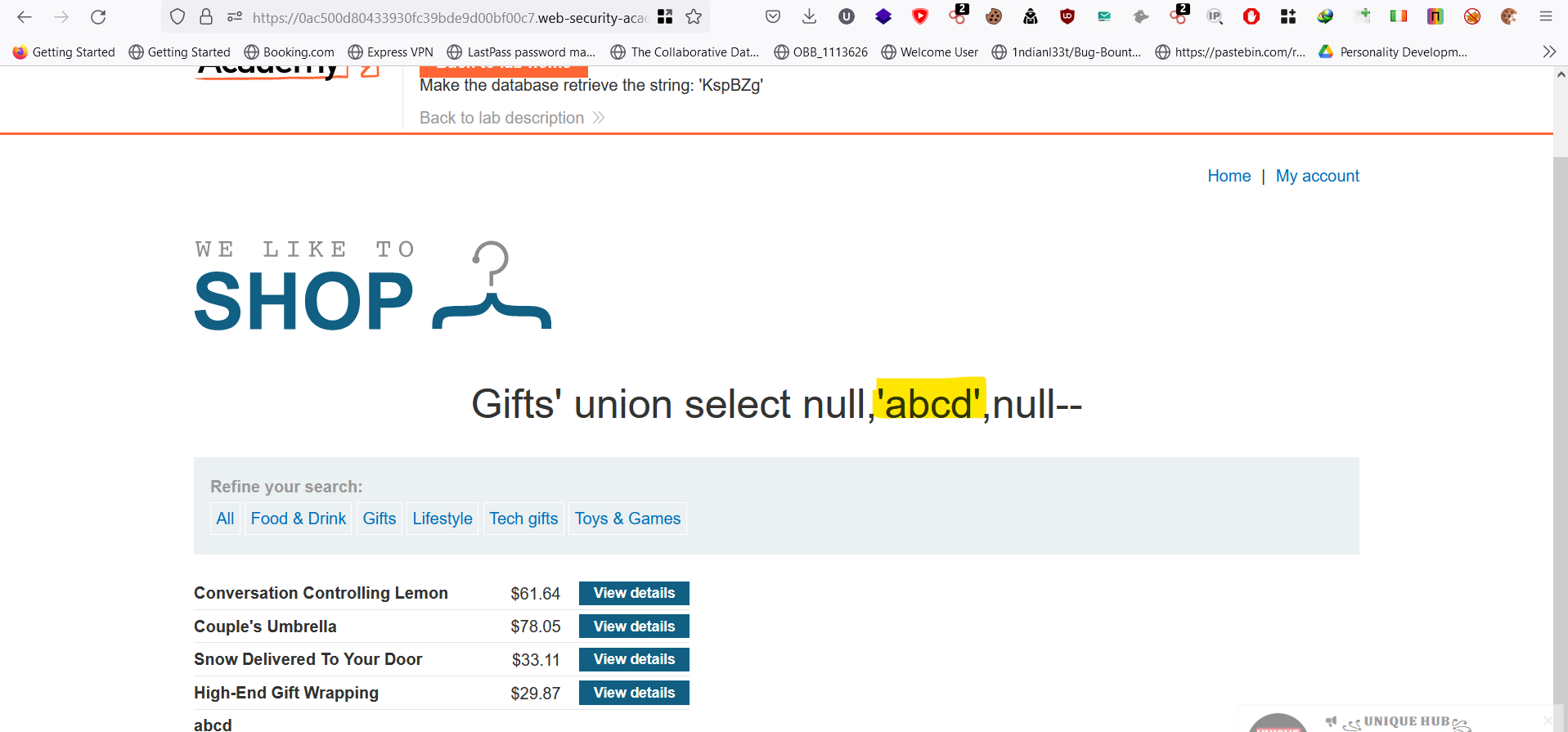
Description automatically generated

I used ‘ for generating error

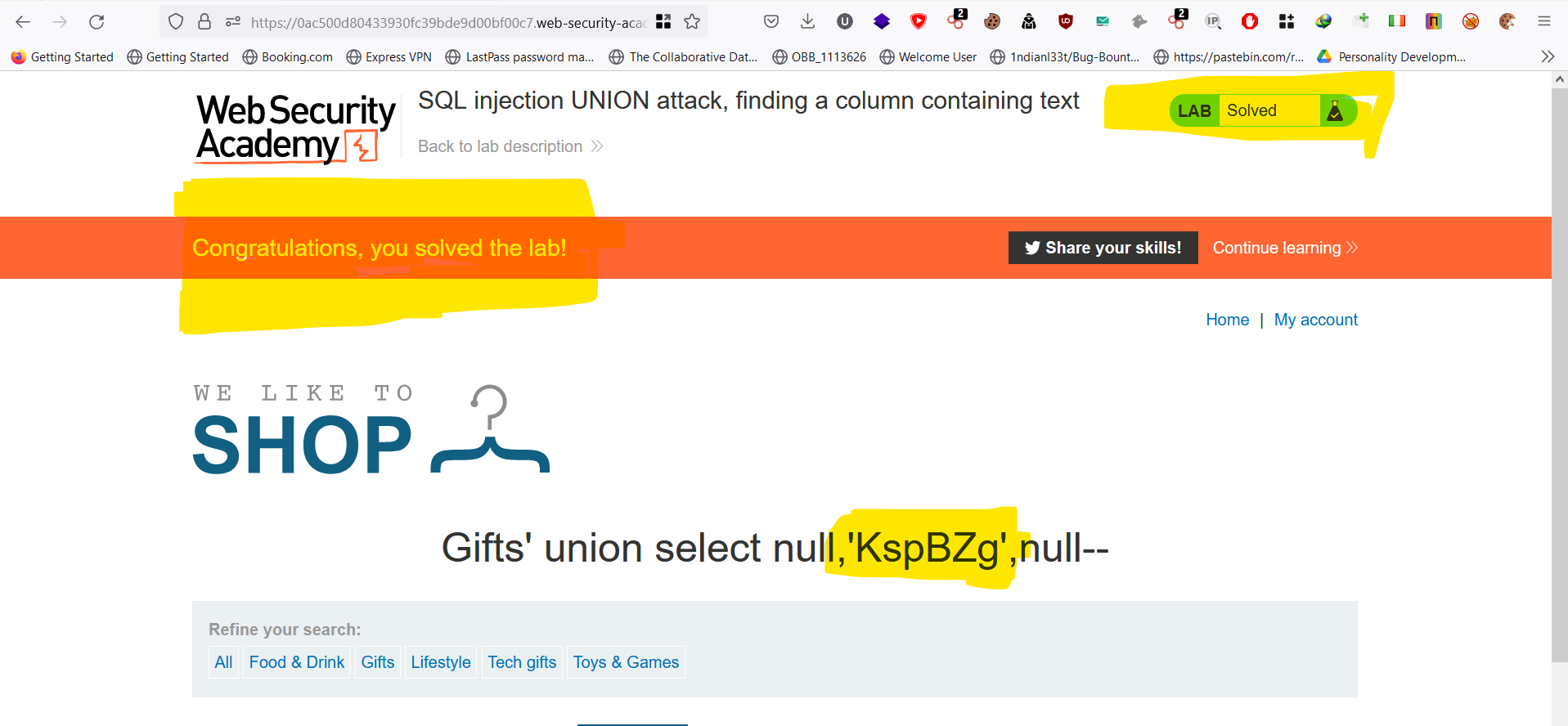
Graphical user interface, text, application

Description automatically generated

Here we got three column using highlighted command above on the image.

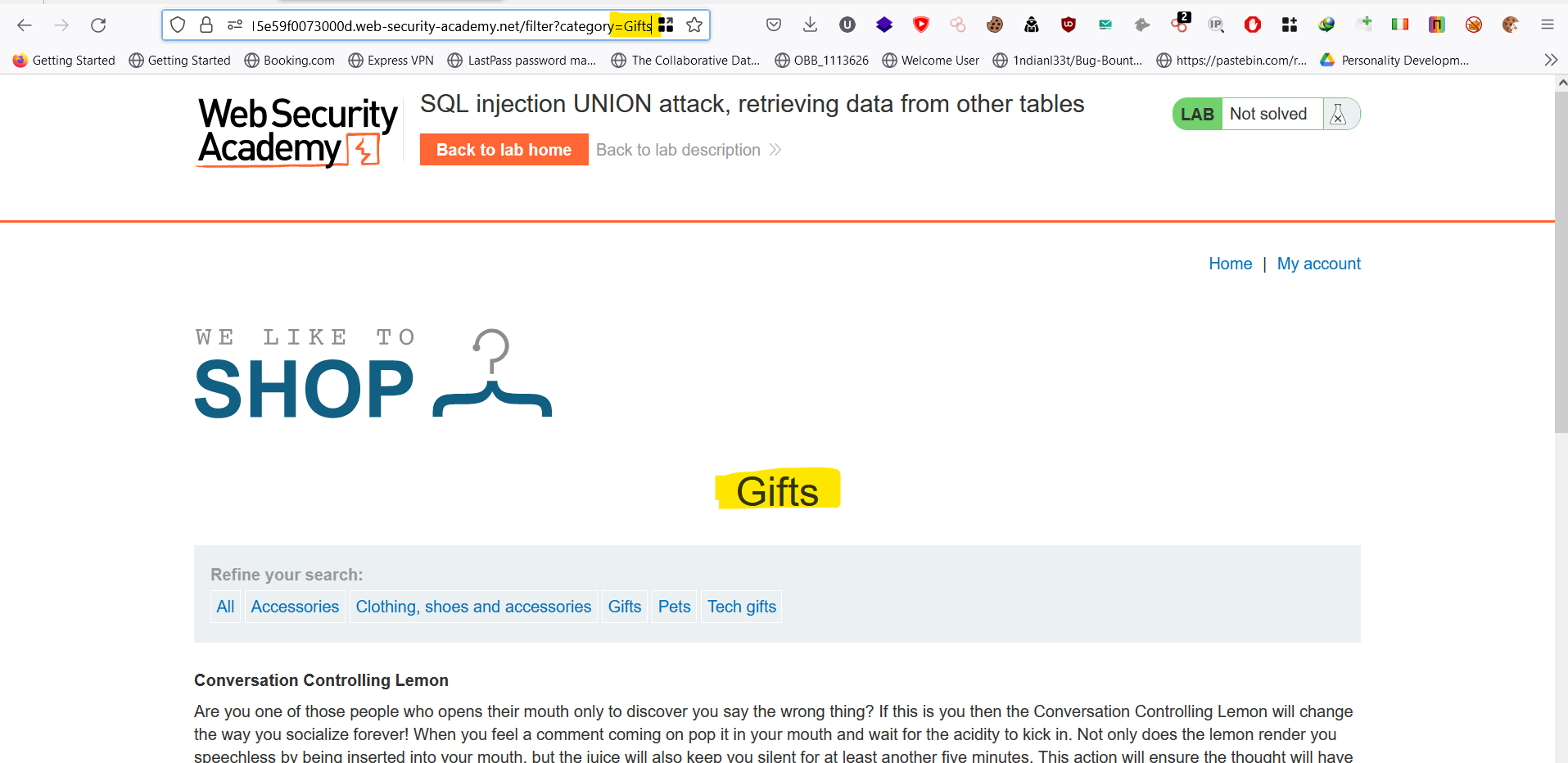


We found one column having character accepting column i.e second column.



In the place of text accepting column I used the name that is given in the above in the task section and I solved the lab.

# Lab 5: SQL injection UNION attack, retrieving data from other tables

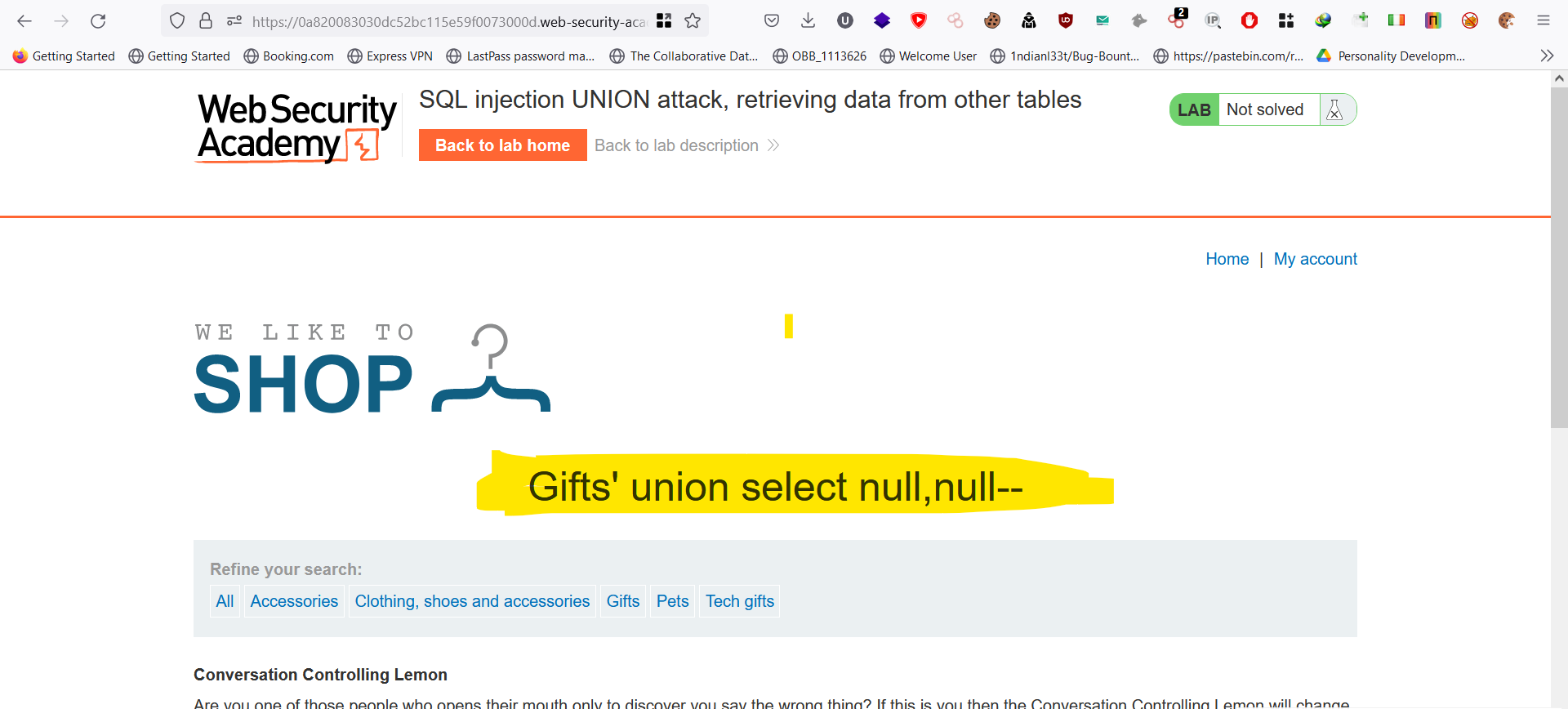


I got parameter in the categories section.

And used quotation marks ‘ in that parameter to produce and error as shown below.

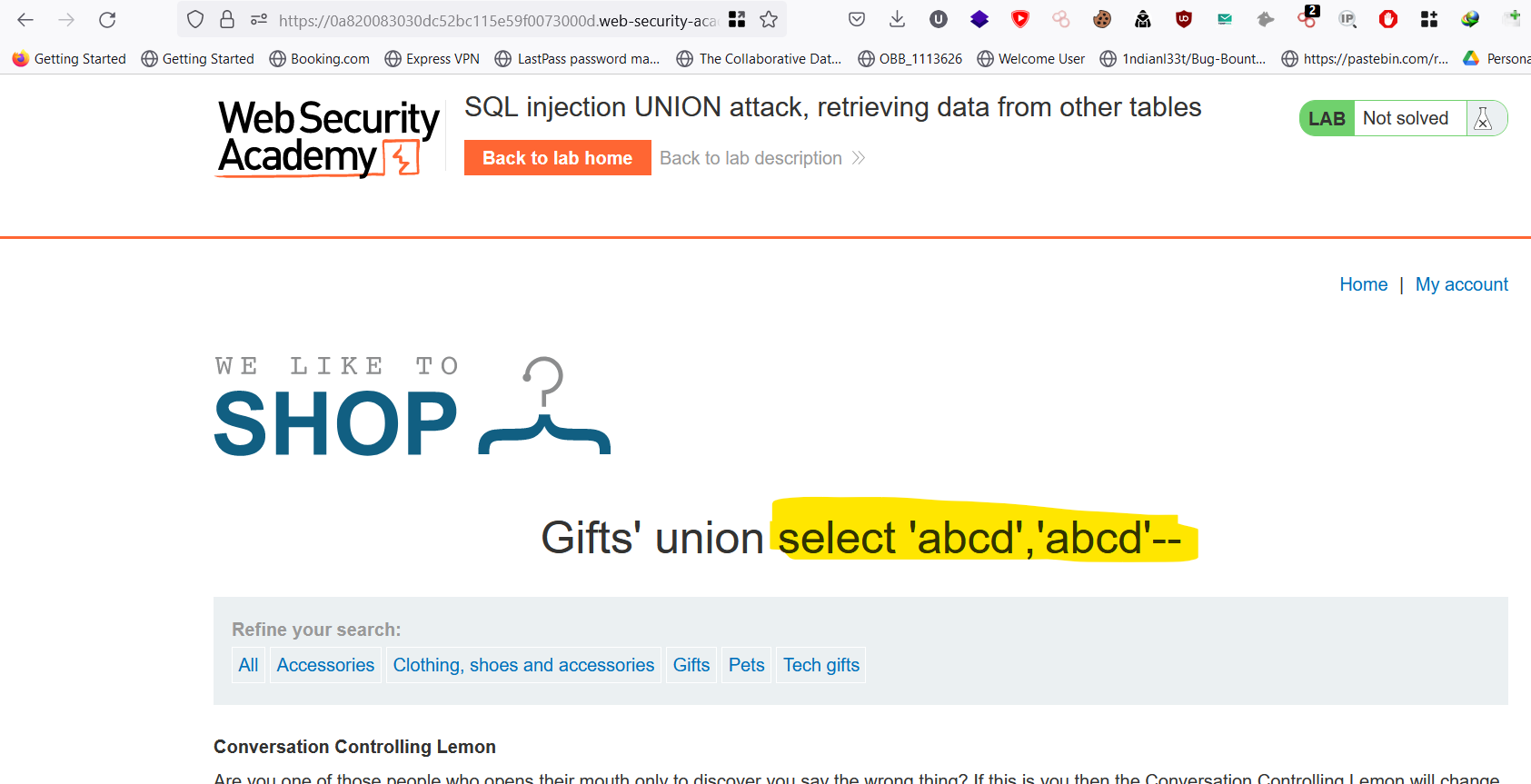
Graphical user interface, text, application, email

Description automatically generated



After that I search for number of columns in the database using above highlighted command in the picture. I was able to know that there were two column in the database.

And I search for text based column as shown in the image below

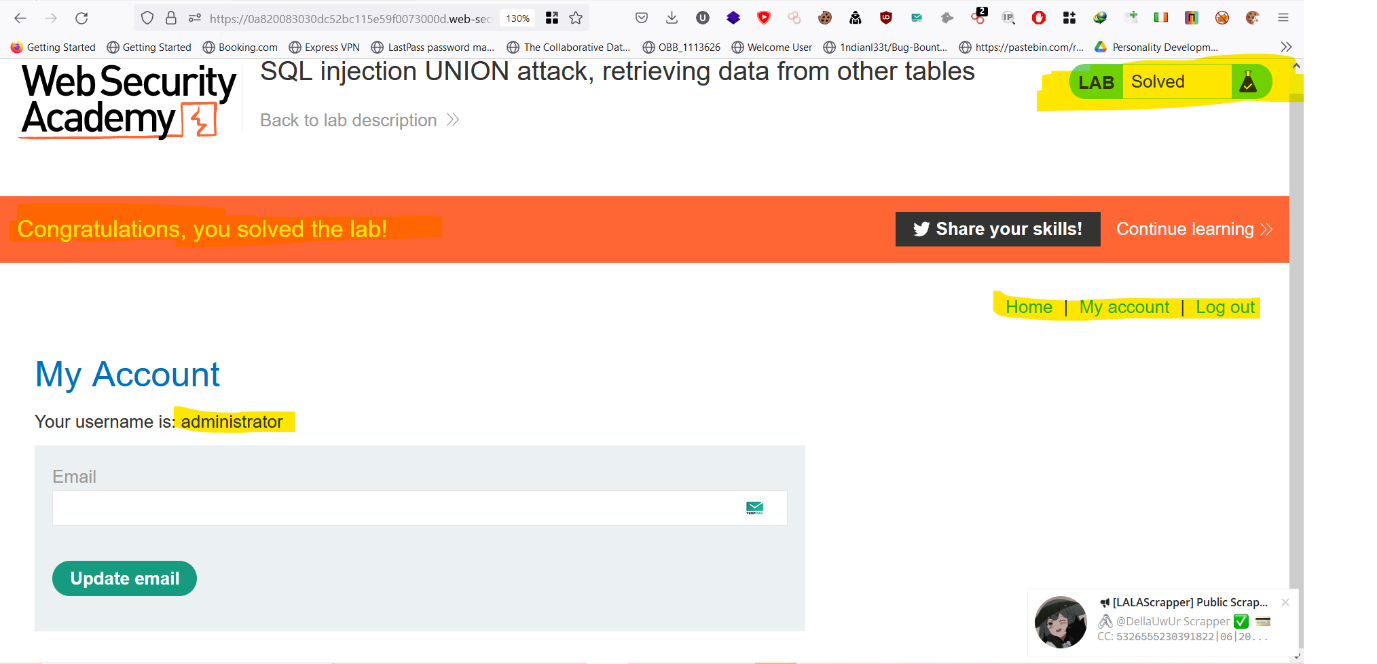


Here I was able to know that the column are text based.

Graphical user interface, text, application, email

Description automatically generated

Using username and password in the SQL command I was able to get username and password



Here in the above picture, I was able to login using the above credentials as administrator. And the lab was solved.