RETO

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

PRACTITIONER

LAB | Not solved

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. To construct such an attack, you need to combine some of the techniques you learned in previous labs.

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.

ACCESS THE LAB

Ilustración 1. Reto seleccionado

1. Se ingresa al laboratorio y se activamos el FoxyProxy previamente configurado

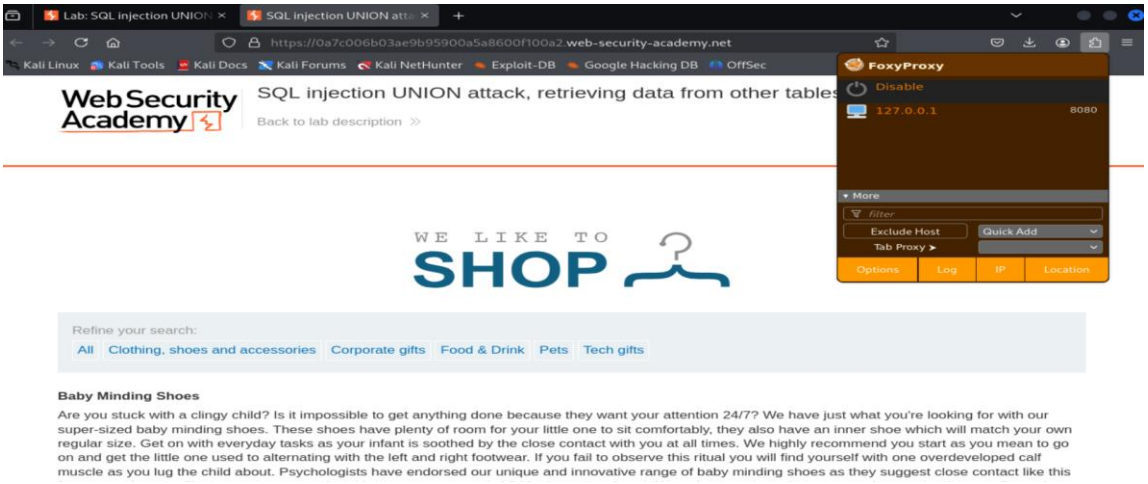

Ilustración 2. página del laboratorio seleccionado

2. Posterior a ello nos dirigimos al programa burnsuite y activamos la opcion **Intercep on** como se nuestra en la ilustración 3 **,** volvemos a recarar la pagina para que intercepte como se muestra en la ilustración 4

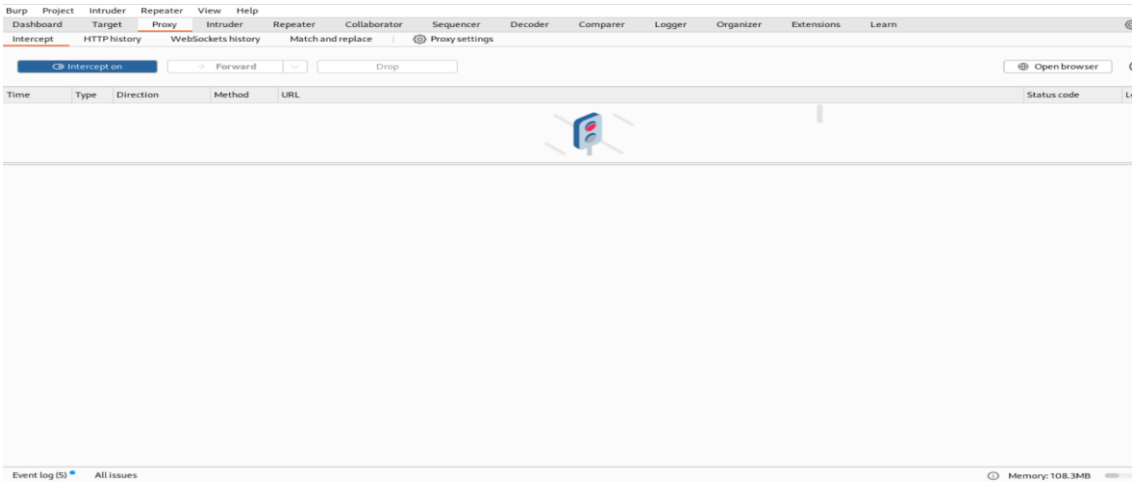

Ilustración 3. BurpSuite intercep ON

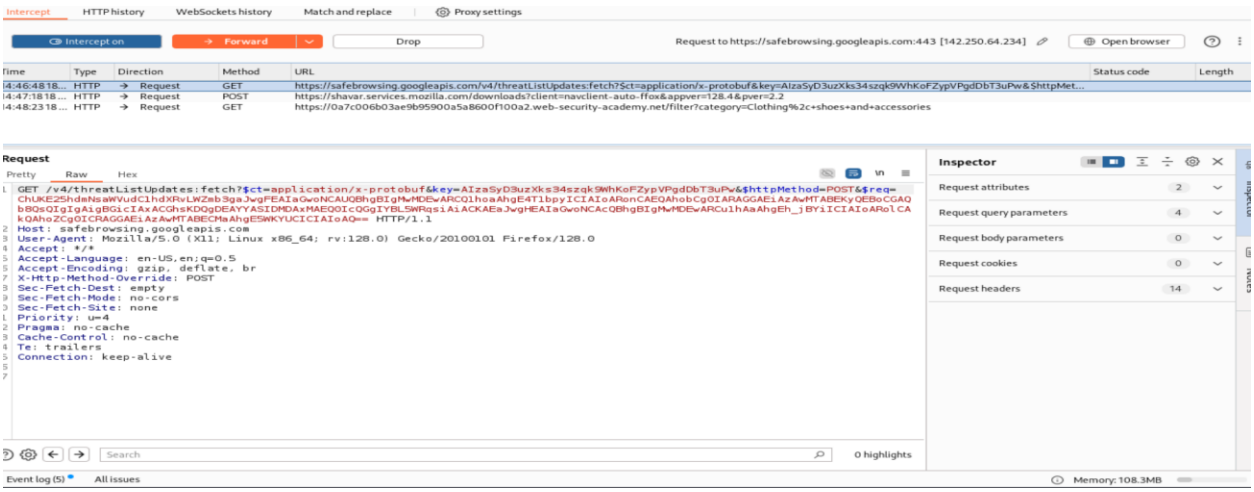

Ilustración 4. intersección de datos

3. Ahora damos clic derecho y seleccionamos la opción send to Repeater

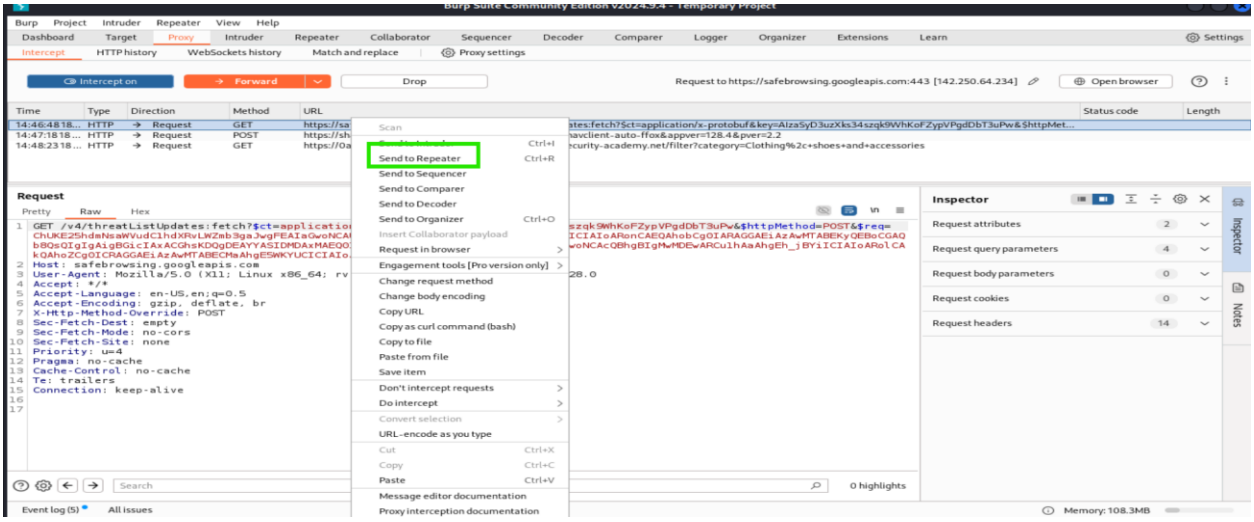

Ilustración 5. Sent to repeater

4. Luego nos dirigimos al recuadro Repeater y se nos muestra la siguiente interfaz

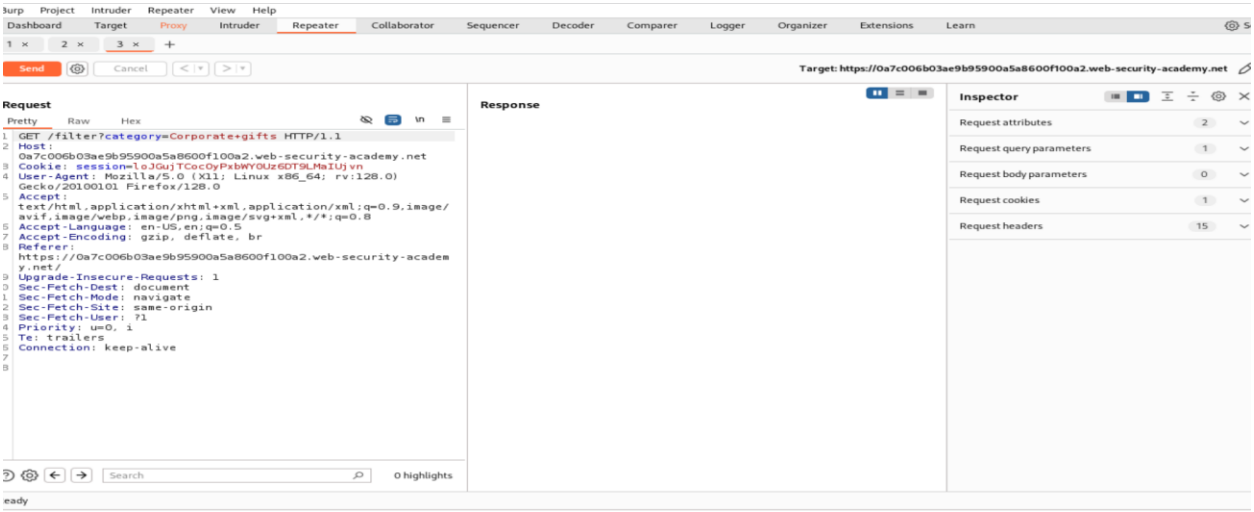

Ilustración 6. recuadro Repeater

5. Ahora para saber el numero de columnas modificados el código, en este caso quiero saber si tiene dos columnas.

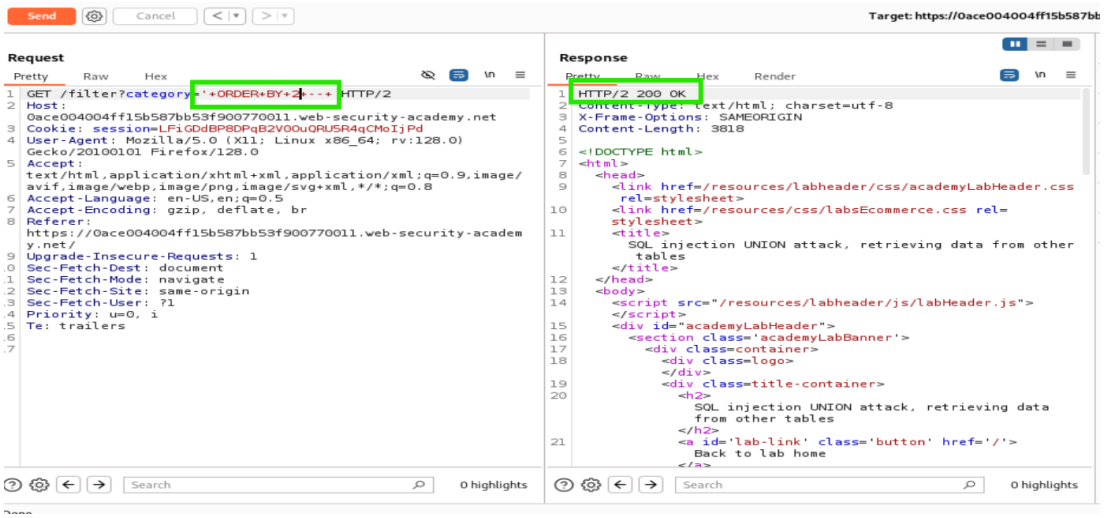

Ilustración 7. respuesta a consulta sobre el número de columnas

6. Ahora se procede con el ONION ATACK

```
'+UNION+SELECT+username,password+FROM+users+--+
```

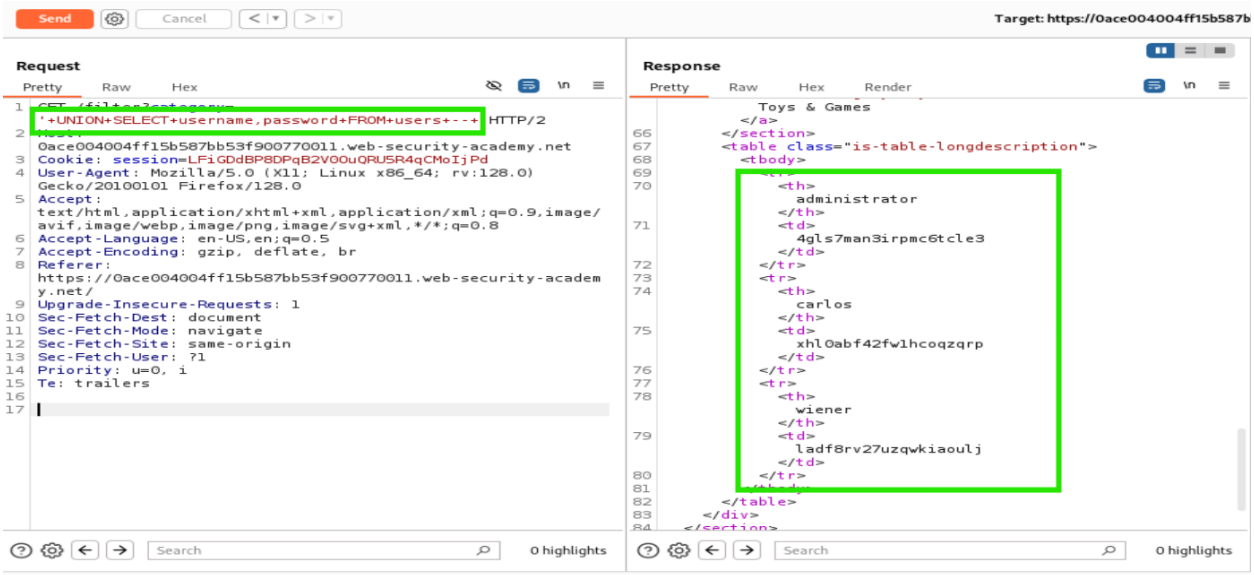

Ilustración 8. obtención de credenciales

Usuario: administrator

Contraseña: 4gls7man3irpmc6tcle3

7. Con el usuario y contraseña obtenido ingresamos

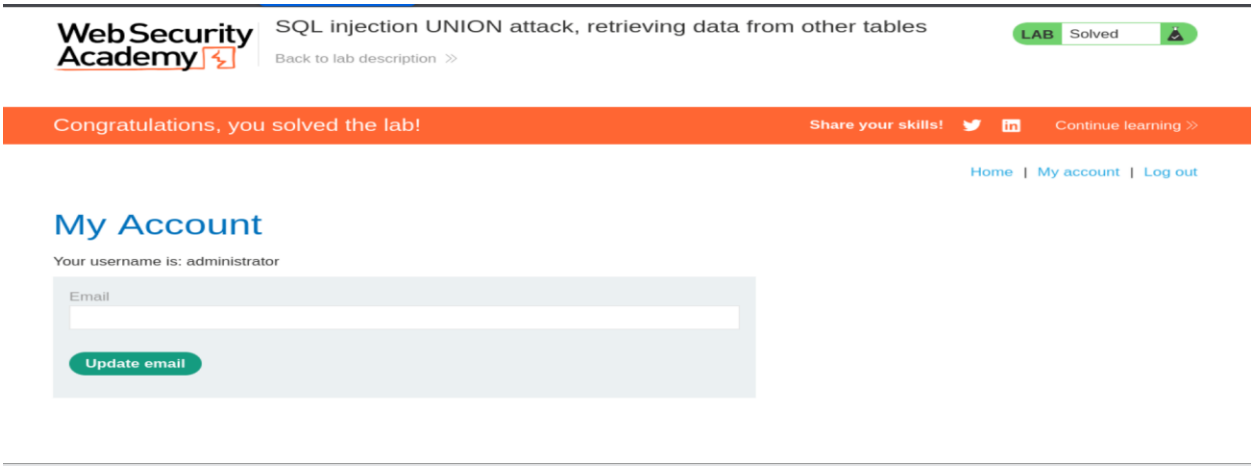

Ilustración 9. ingreso como administrador, reto cumplido