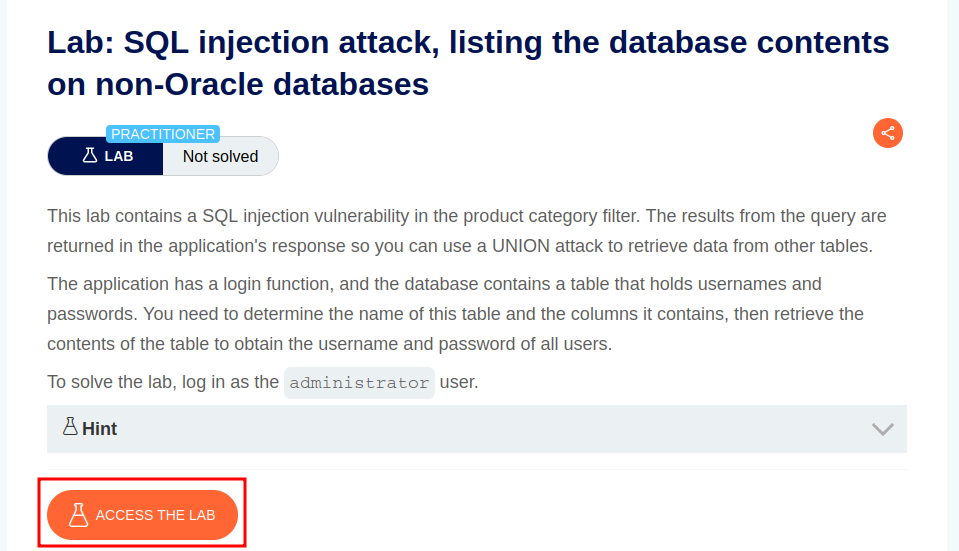
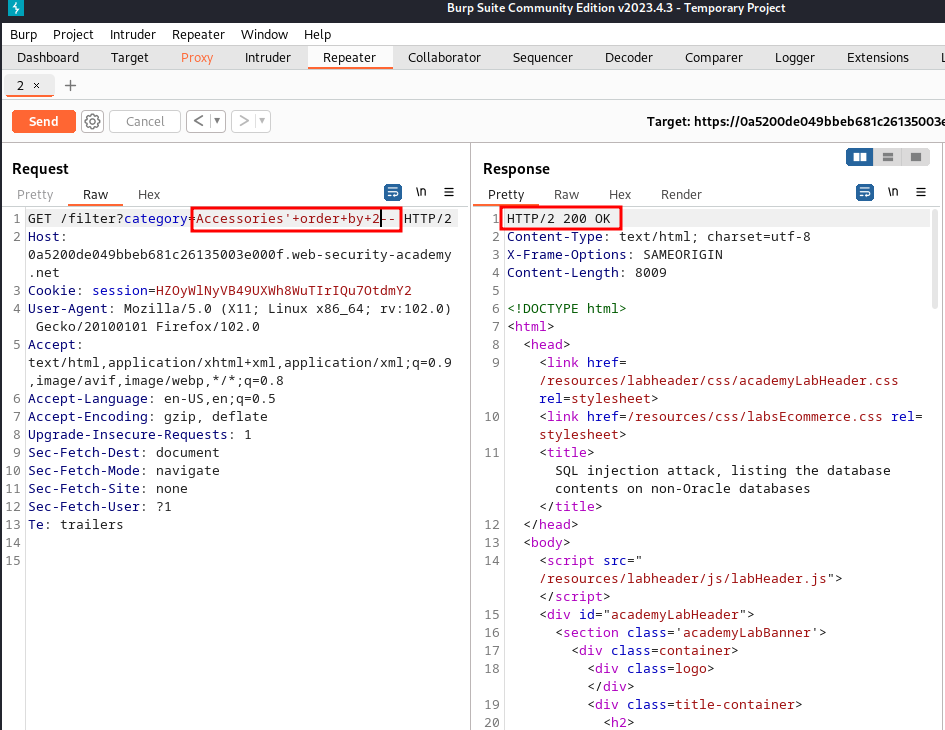
To Access the Lab –

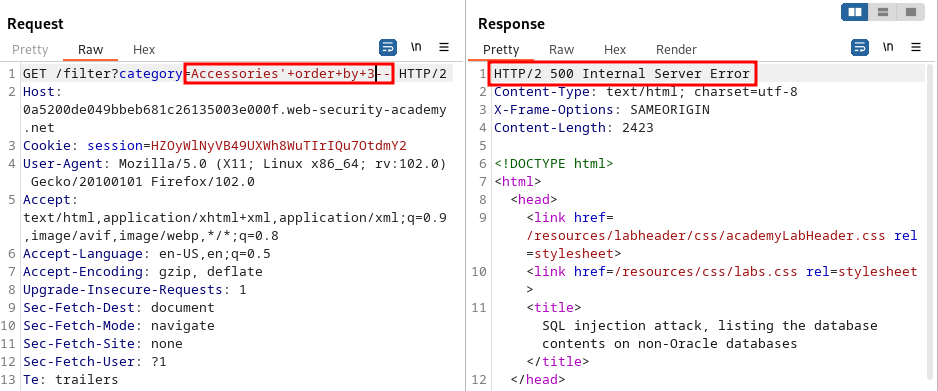


Intercept the request on Burp and send to repeater,

On repeater, URL – We can use the Union based SQLi cheatsheet to determine the number of columns that are being returned by the query and which columns contain text data.



Here we can see that for 2 columns, we are getting a 200 response

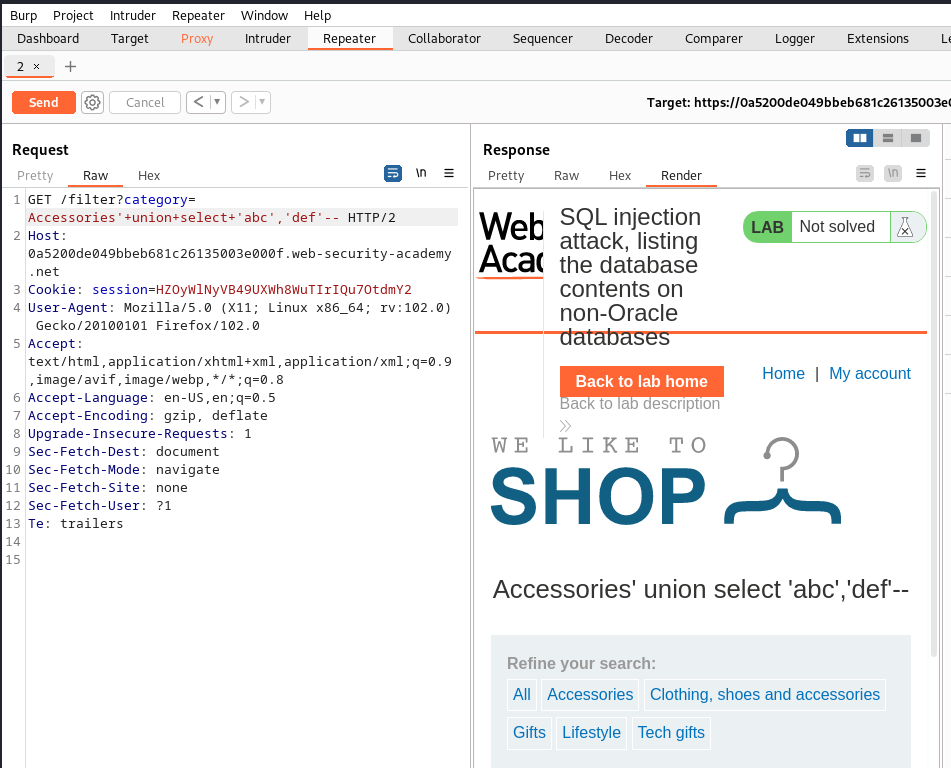


Here we can see that for 3 columns, we are getting a 500 ISE response.

This means that there are 2 columns.

Next, we can find out which columns print out data.

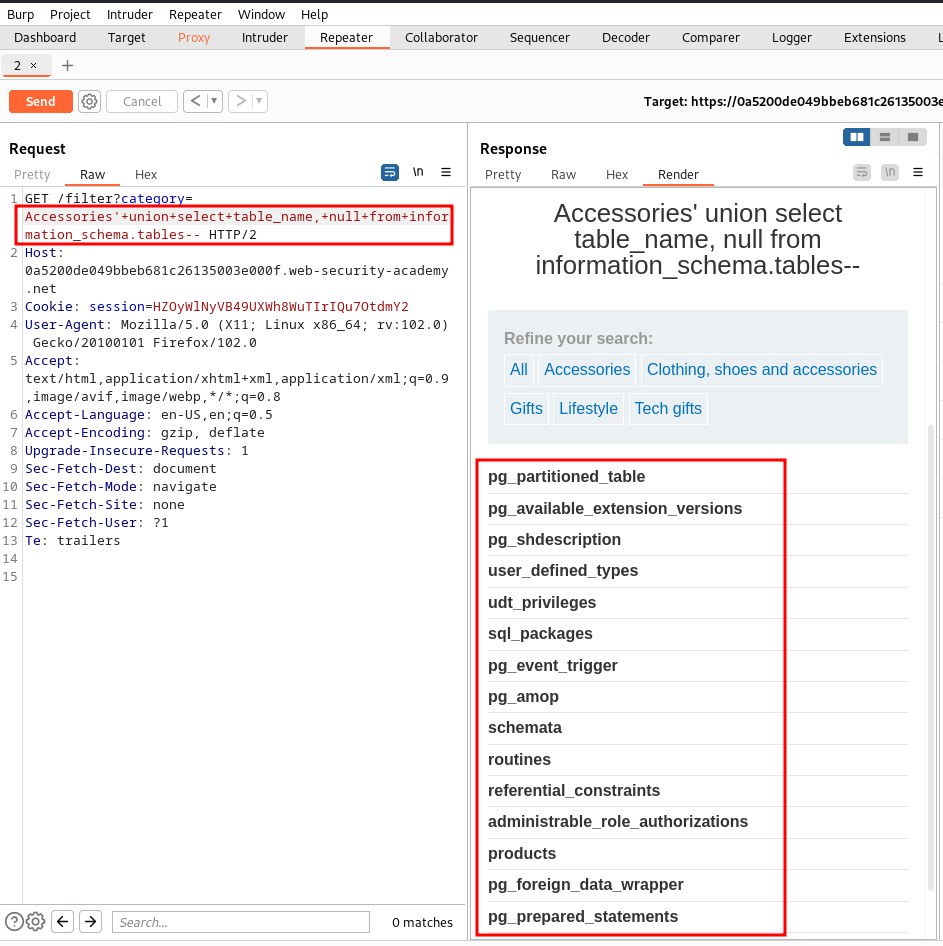
**Accessories’+union+select+’abc’.’def’--**



Here we can see that both columns print out data.

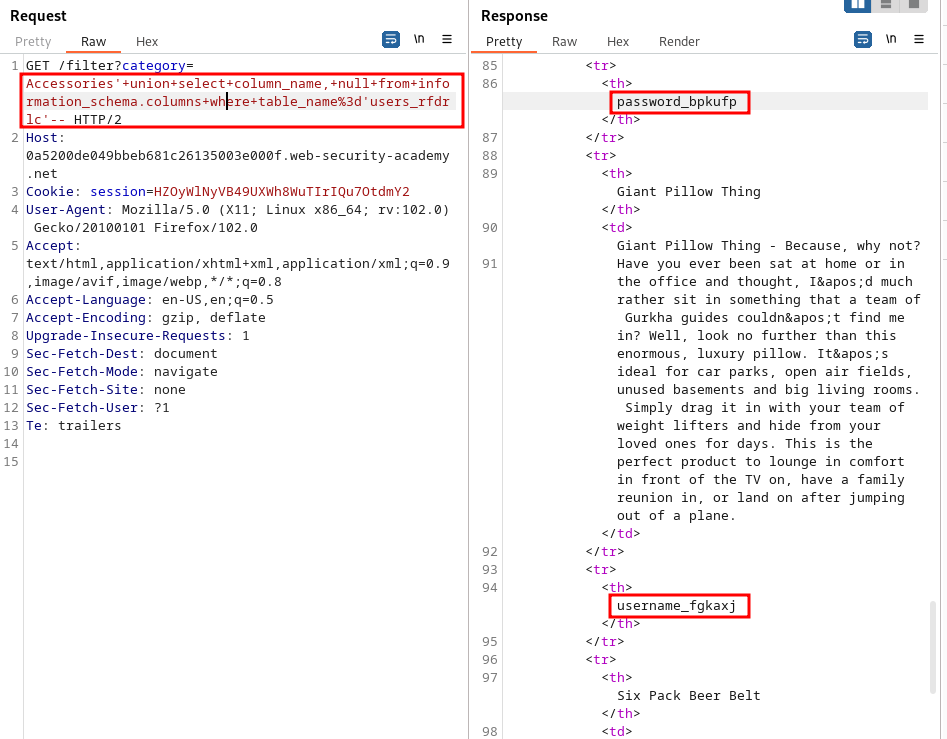
Next, we can print out the tables present in this database.

**'+UNION+SELECT+table\_name,+NULL+FROM+information\_schema.tables—**

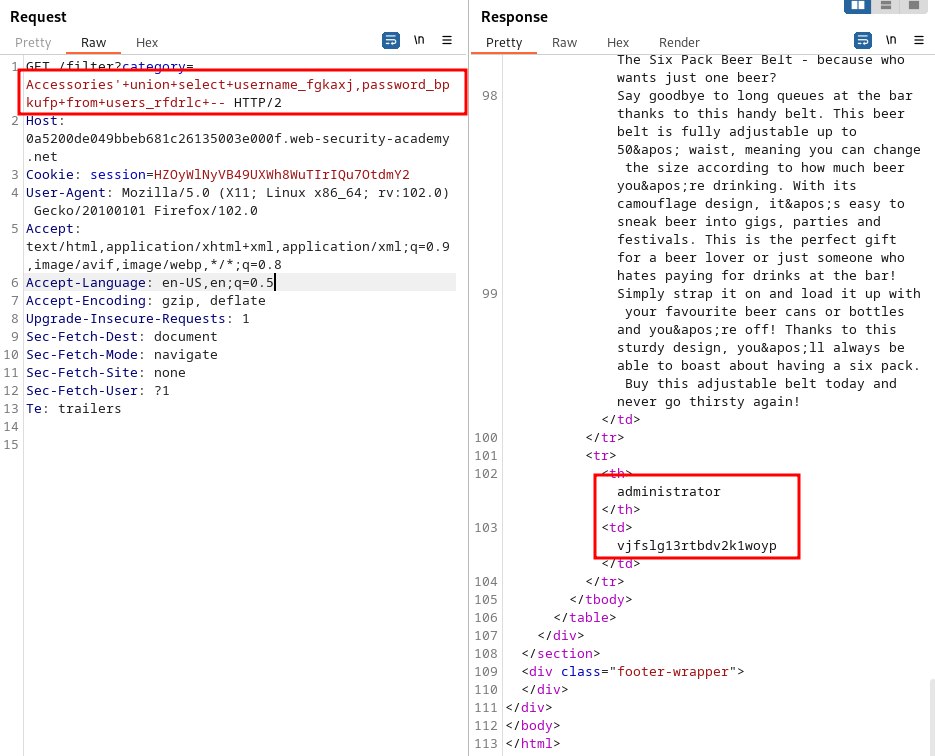


Here, we can see a list of tables in this database, we can find one users\_rfdrlc table

**'+union+select+column\_name,+null+from+information\_schema.columns+where+table\_name%3d'users\_rfdrlc'—**



**Accessories'+union+select+username\_fgkaxj,password\_bpkufp+from+users\_rfdrlc+--**



Next, we can login to the administrator account using these credentials.

