## Password cracking

Dopo l'SQL injection fatto ieri, son risalito alle password degli user sulla dvwa.



Successivamente ho preso queste password e le ho inserite in un file txt. Poi con il comando che segue, effettuo un attacco a dizionario.

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

john è un tool di cracking per password, supporta una vasta gamma di algoritmi di hash;

-format=raw-md5 sta ad indicare il tipo di crittografia ;

-wordlist andiamo a prendere la lista a dizionario "rockyou.txt;

Hash.txt è il file delle password da decriptare.

Come si vede nello screen, il tool ha trovato le password crittografate dal file hash.txt

```
(kali kali) - [~/Desktop]
$ john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
Created directory: /home/kali/.john
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8×3])
Warning: no OpenMP support for this hash type, consider --fork=6
Press 'q' or Ctrl-C to abort, almost any other key for status
password (?)
abc123 (?)
letmein (?)
charley (?)
4g 0:00:00:00 DONE (2023-06-07 03:12) 400.0g/s 307200p/s 307200c/s 460800C/s my3kids..dangerous
Warning: passwords printed above might not be all those cracked
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```

Una volta effettuata la decriptazione, per visualizzare le password craccate in un determinato file, bisogna eseguire il seguente comando:

## john --show -format=raw-md5 hash.txt