

Per la risoluzione dell'esercizio odierno siamo andati ad effettuare prima una sql injection per recuperare le password in hash, subito dopo abbiamo utilizzato il tool john the ripper per tentare un attacco a libreria ed un attacco pure brute force, in entrambi i casi andiamo a vedere l'ordine delle password tramite un comando inserito successivamente.

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ john --wordlist=/usr/share/wordlists/rockyou.txt --format=raw-md5 ./Desktop/Hash.txt  
Using default input encoding: UTF-8  
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE2 4x3])  
Warning: no OpenMP support for this hash type, consider --fork=2  
Press 'q' or Ctrl-C to abort, almost any other key for status  
password (???)  
abc123 (???)  
letmein (???)  
charley (???)  
4g 0:00:00:00 DONE (2024-02-28 15:16) 57.14g/s 41142p/s 41142c/s 54857C/s my3kids..s  
occer9  
Warning: passwords printed above might not be all those cracked  
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords re  
liably  
Session completed.  
(kali@kali)-[~]  
$ john --show --format=raw-md5  
Password files required, but none specified  
(kali@kali)-[~]  
$ john --show --format=raw-md5 ./Desktop/Hash.txt  
?:password  
?:abc123  
?:charley  
?:letmein  
?:password  
  
5 password hashes cracked, 0 left  
(kali@kali)-[~]  
$
```

Attacco a dizionario prendendo il file txt rockyou come dizionario.

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ john --incremental --format=raw-md5 ./Desktop/Hash.txt  
Using default input encoding: UTF-8  
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE2 4x3])  
Warning: no OpenMP support for this hash type, consider --fork=2  
Press 'q' or Ctrl-C to abort, almost any other key for status  
abc123 (???) (format)  
charley --pair-max (???) Override max. number of word pairs generated (60)  
password --le-pair (???) Disable single word pair generation  
letmein --le-pair (???) guess Override config for SingleWordPairness  
4g 0:00:00:00 DONE (2024-02-28 16:00) 5.479g/s 3498Kp/s 3498Kc/s 4106Kc/s letebru..l  
etmish  
Warning: passwords printed above might not be all those cracked (at PRINCE)  
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords re  
liably  
Session completed.  
(kali@kali)-[~]  
$ john --show --format=Raw-MD5  
Password files required, but none specified  
(kali@kali)-[~]  
$ john --show --format=Raw-MD5  
Password files required, but none specified  
(kali@kali)-[~]  
$ john --show --format=Raw-MD5  
?:password  
?:abc123  
?:charley  
?:letmein  
?:password  
5 password hashes cracked, 0 left
```

Attacco bruteforce incrementale.