

## Traccia: password cracking

Abbiamo visto come sfruttare un attacco SQL injection per recuperare le password degli utenti di un determinato sistema.

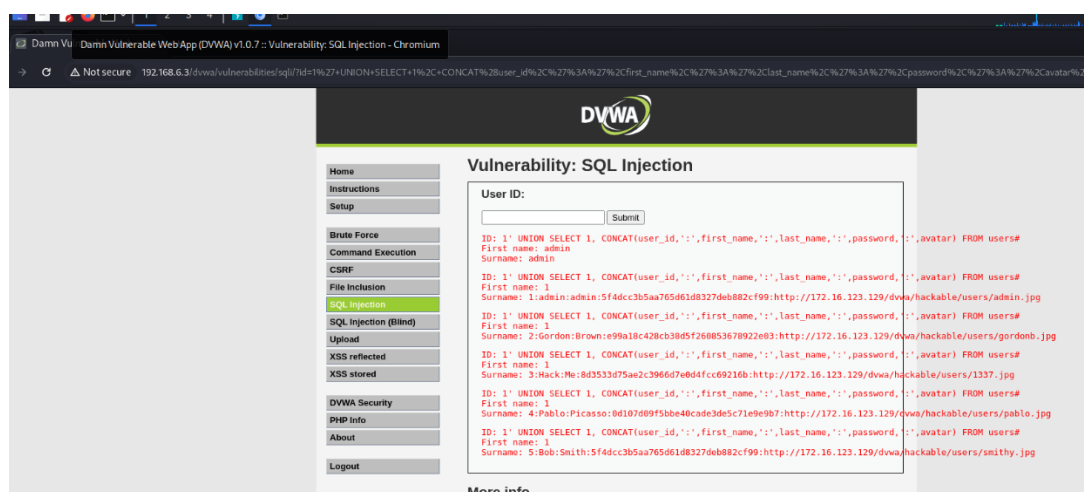
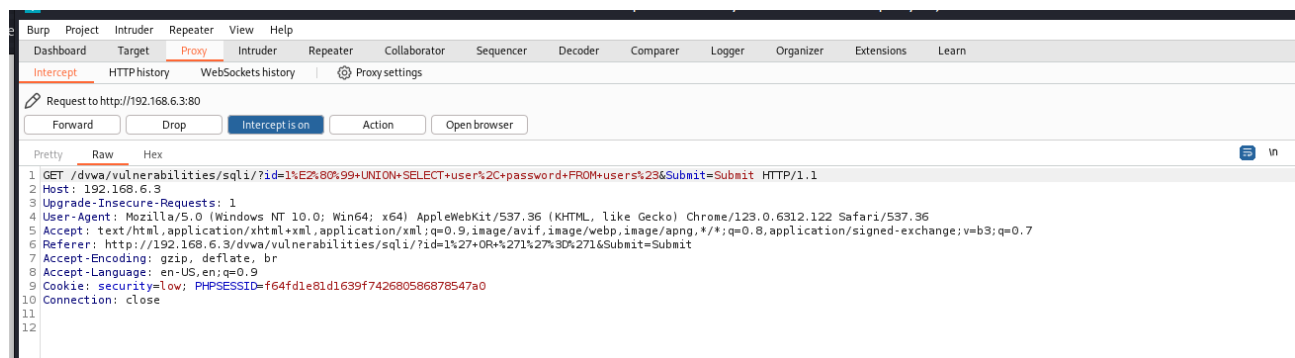
Se guardiamo meglio alle password trovate, non hanno l'aspetto di password in chiaro, ma sembrano più hash di password MD5.

Recuperate le password dal DB come visto, 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. L'obiettivo dell'esercizio di oggi è craccare tutte le password trovate precedentemente.

## Svolgimento :

come abbiamo visto nell'esercizio precedente, abbiamo scoperto l'username e la password delle utente su DVWA in formato hash MD5. Di seguito elencato lo screen dell'attacco sql injection :



## John the ripper

**John the Ripper** è uno strumento di cracking delle password utilizzato principalmente per testare la sicurezza delle password. È in grado di individuare password deboli o compromesse utilizzando diversi metodi di attacco, tra cui:

- **Attacco a dizionario:** Prova un elenco di parole comuni come password.

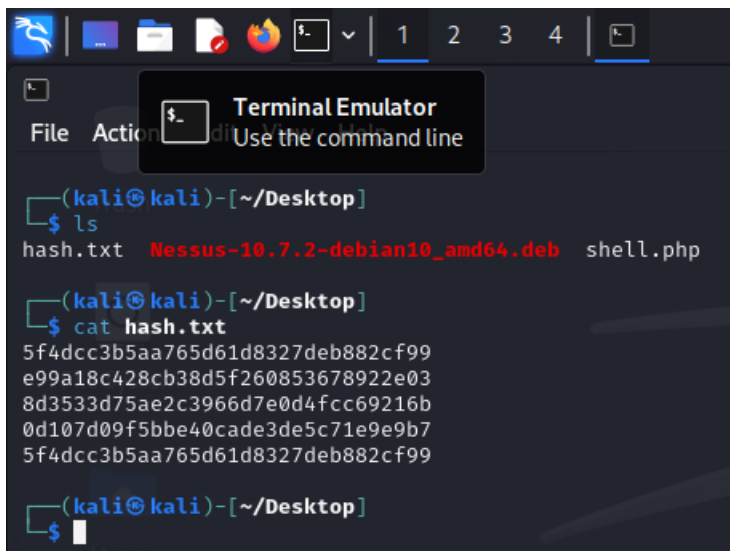
- **Attacco brute force:** Tenta tutte le possibili combinazioni di caratteri.

Supporta vari formati di hash delle password, come MD5, SHA-1 e bcrypt, e funziona su diversi sistemi operativi, tra cui Linux, macOS e Windows.

Funziona localmente sul tuo computer o server, analizzando i file delle password per cercare di crackarle senza la necessità di una connessione a internet. Questo lo rende utile per eseguire test di sicurezza su sistemi isolati e senza esporre i dati sensibili a rischi esterni.

## Creazione del file contenente le password

Per poter craccare le password recuperate dobbiamo creare un semplice file .txt che chiameremo **hash.txt**

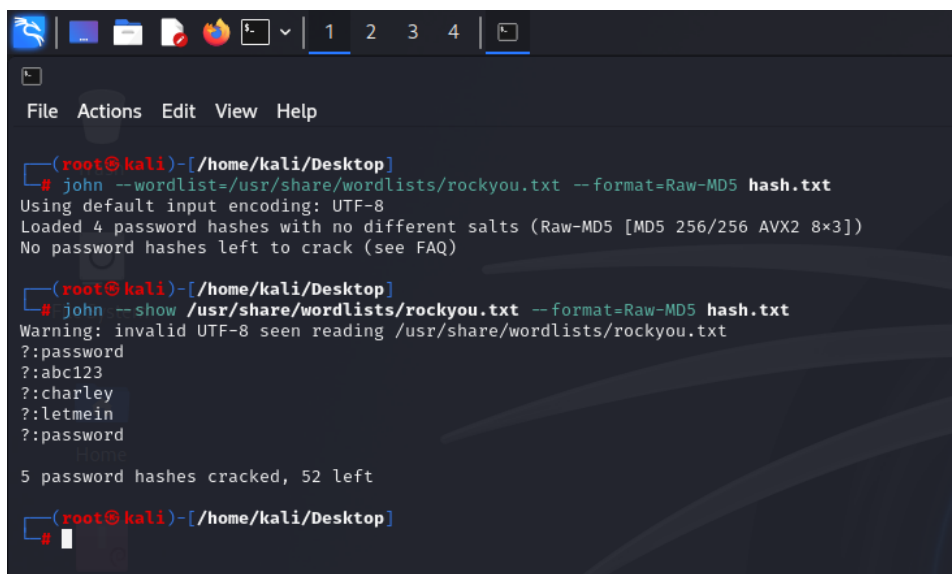


The screenshot shows a Kali Linux terminal window titled "Terminal Emulator". The prompt is `(kali㉿kali)~[~/Desktop]`. The user enters `ls`, and the output shows `hash.txt`, `Nessus-10.7.2-debian10_amd64.deb`, and `shell.php`. Then, the user enters `cat hash.txt`, and the output displays five lines of MD5 hashes: `5f4dcc3b5aa765d61d8327deb882cf99`, `e99a18c428cb38d5f260853678922e03`, `8d3533d75ae2c3966d7e0d4fcc69216b`, `0d107d09f5bbe40cade3de5c71e9e9b7`, and `5f4dcc3b5aa765d61d8327deb882cf99`. The terminal window has a menu bar with "File" and "Action" options, and a toolbar with icons for file operations.

## Cracking delle password

John the Ripper prova le parole del file **rockyou.txt** per decifrare le password cifrate in formato MD5 presenti in "hash.txt".

- **--wordlist=/usr/share/wordlists/rockyou.txt:** Usa il file **rockyou.txt** come elenco di parole da provare come password.
- **--format=Raw-MD5:** Indica che le password da crackare sono cifrate usando il formato Raw-MD5.
- **hash.txt:** Specifica il file contenente le password cifrate da decifrare.



A terminal window with a dark background and a menu bar (File, Actions, Edit, View, Help). The terminal shows the execution of John the Ripper commands. The first command is `john --wordlist=/usr/share/wordlists/rockyou.txt --format=Raw-MD5 hash.txt`, which loads 4 password hashes. The second command is `john --show /usr/share/wordlists/rockyou.txt --format=Raw-MD5 hash.txt`, which displays the cracked passwords: `password`, `abc123`, `charley`, and `letmein`. The output indicates that 5 password hashes were cracked, leaving 52 left.

```
(root@kali)-[/home/kali/Desktop]
# john --wordlist=/usr/share/wordlists/rockyou.txt --format=Raw-MD5 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)

(root@kali)-[/home/kali/Desktop]
# john --show /usr/share/wordlists/rockyou.txt --format=Raw-MD5 hash.txt
Warning: invalid UTF-8 seen reading /usr/share/wordlists/rockyou.txt
?:password
?:abc123
?:charley
?:letmein
?:password
5 password hashes cracked, 52 left

(root@kali)-[/home/kali/Desktop]
#
```