S6/L4

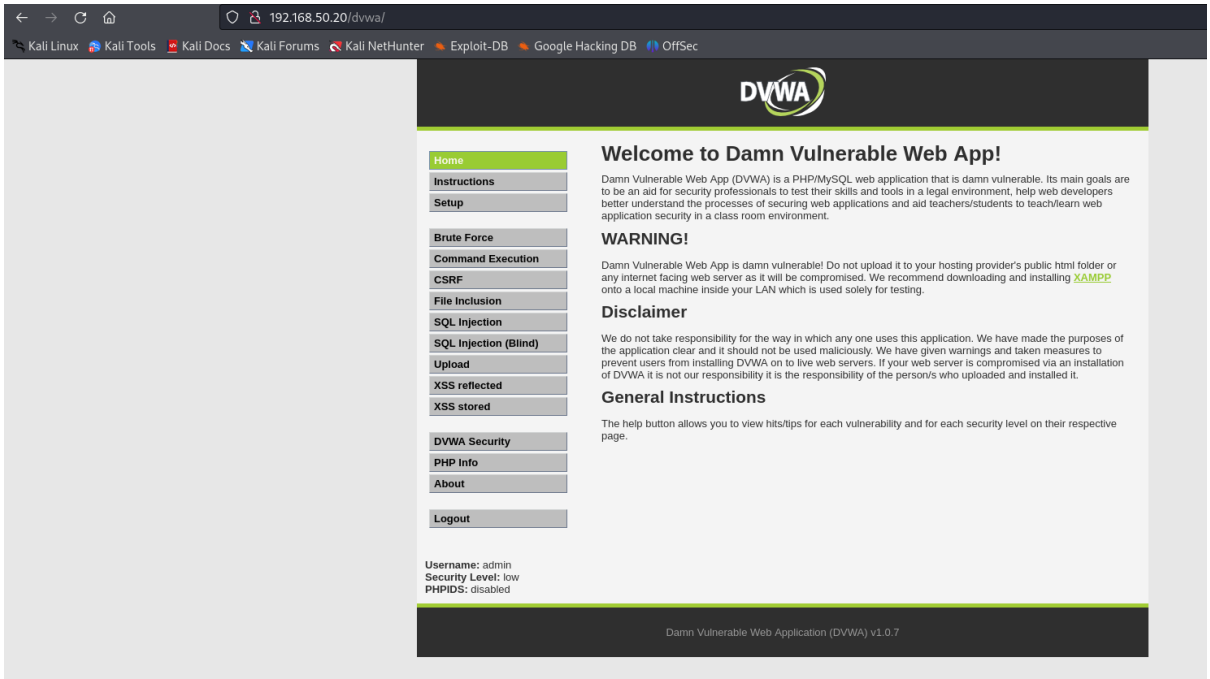
L’esercizio di oggi consiste nel recuperare le password hashate nel database della DVWA e eseguire sessioni di cracking per recuperare la loro versione in chiaro utilizzando i tool studiati nella lezione teorica.

La prima cosa che facciamo è accendere entrambi le macchine è assicurarci che comunicano tra di loro.

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.50.20
PING 192.168.50.20 (192.168.50.20) 56(84) bytes of data.
64 bytes from 192.168.50.20: icmp_seq=1 ttl=64 time=0.670 ms
64 bytes from 192.168.50.20: icmp_seq=2 ttl=64 time=0.341 ms
^C
── 192.168.50.20 ping statistics ──
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.341/0.505/0.670/0.164 ms
```

Una volta verificato dobbiamo andare all’interno della DVWA di metasploitable tramite mozilla.

http://192.168.50.20

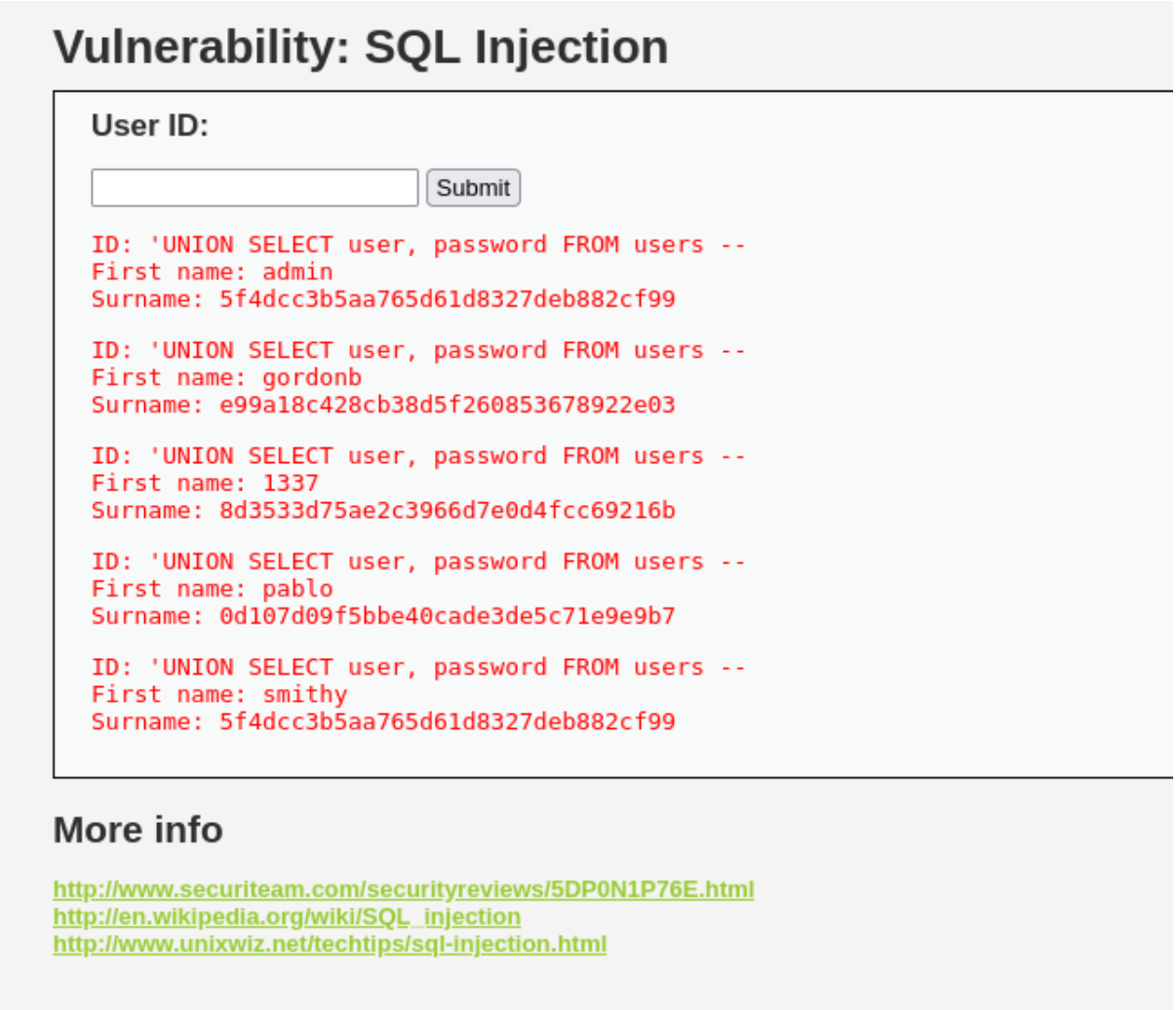


E andiamo su SQL Injection (dopo aver impostato la sicurezza su low).

Eseguiamo questa ricerca all'interno

```
'UNION SELECT user, password FROM users --
```

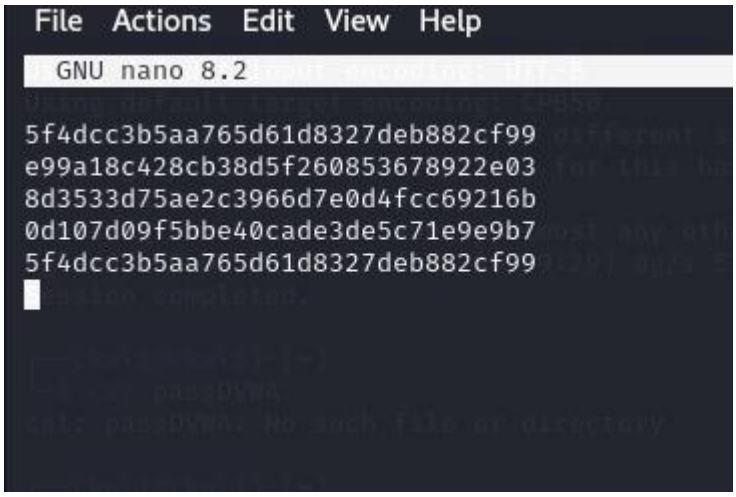
Una volta eseguito ci darà i seguenti risultati:



Dove First name sono gli user mentre Surname sono le password che come vediamo sono hashate.

Ci sono vari modi per verificare di che tipo è l'hash oggi giorno soprattutto si utilizzano dei tool, ma si può fare anche contando i caratteri infatti il tipo MD5 utilizza sempre 32 caratteri come le password che abbiamo noi.

Ora invece dobbiamo decriptarle, come prima cosa dobbiamo inserirle in un unico file.



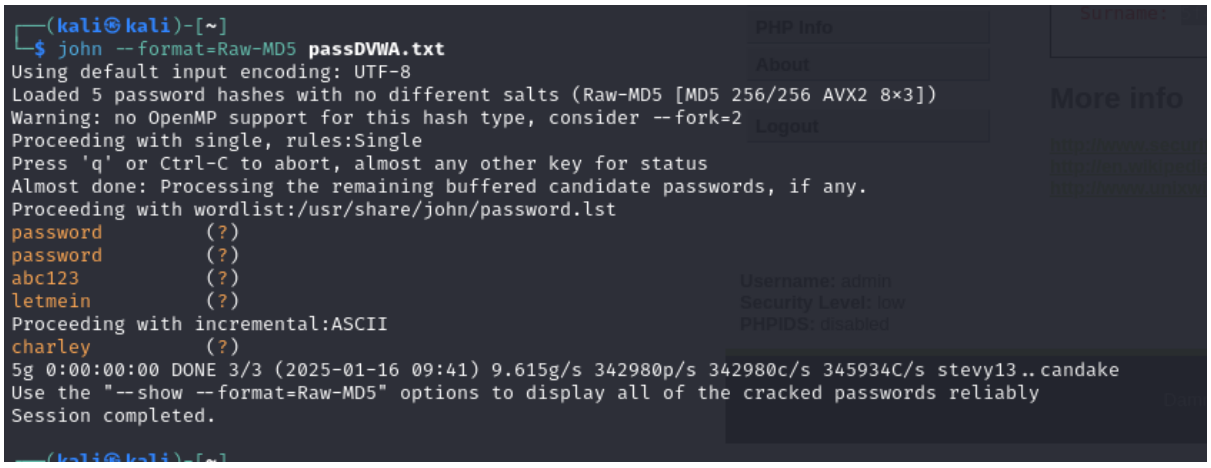
Io le ho inserite in un file chiamato passDVWA.txt

Dopo di che dobbiamo utilizzare il nostro tool John the ripper dove andremo ad eseguire il seguente comando:

“john --format=Raw-MD5 passDVWA.txt”

Dove essendo che sappiamo il formato lo specifichiamo in modo da rendere il lavoro più leggero, e poi il file con all’interno le password hashate.

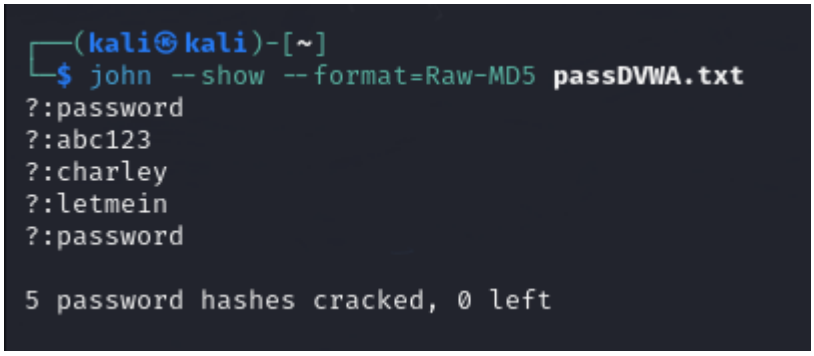
Tutte le altre impostazioni invece sono automatiche.



Per visualizzarle dopo invece dobbiamo eseguire questo commando:

“john --show --format=Raw-MD5 passDVWA.txt”

E avremo questo output:



Notiamo anche che la prima è l'ultima sono uguali.