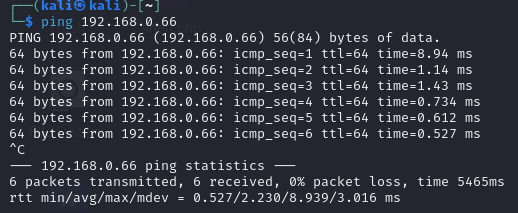
**PRATICA 04 NOVEMBRE 2024**

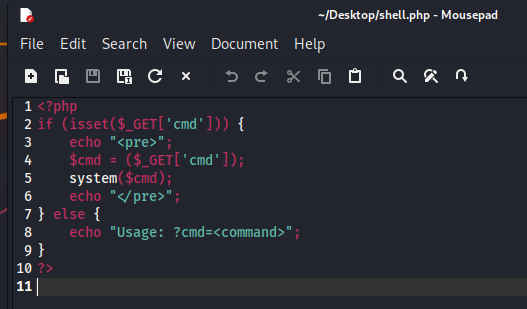
**Exploit File Upload**  
  
Oggi andremo a simulare un attacco **MITM** (Man in the middle) utilizzando **burpsuite** come attaccante e Metasploitable2 come vittima.  
  
L’obiettivo è utilizzare il metodo **PUT** del protocollo HTTP per modificare la DVWA della macchina vittima.

**Fase 0**

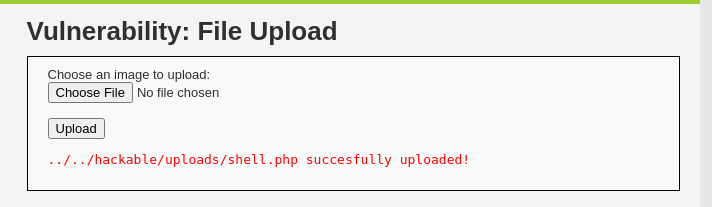
Controlliamo la comunicazione tra Kali Linux (192.168.0.222) e Metasploitable2(192.168.0.66) 

**Fase 1**

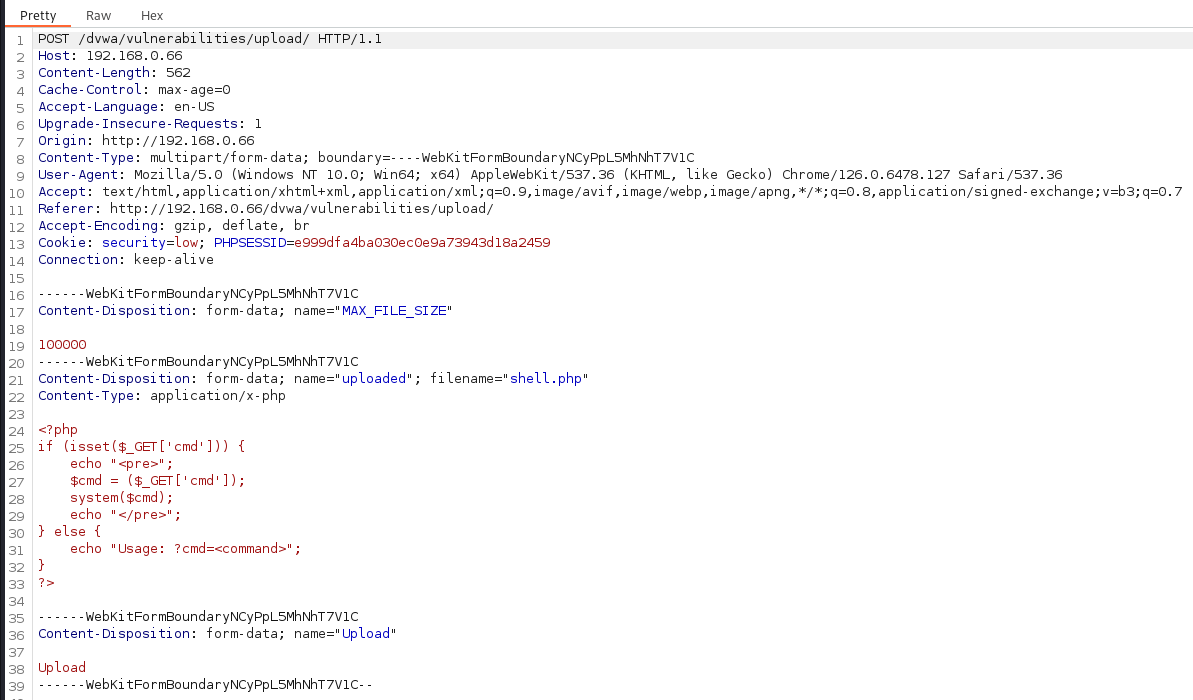
Passiamo alla creazione della shell che andremo inserire all’interno della DVWA. In questo caso utilizzeremo la seguente shell:



**Fase 2**  
Utilizzando burpsuite, adesso, accederemo alla DVWA di Metasploitable2 e caricheremo il file php.

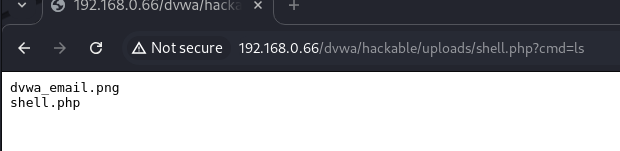


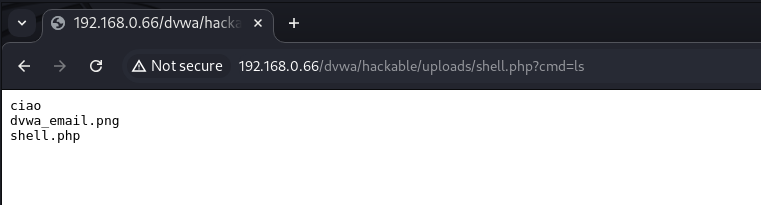
Di seguito anche l’intercettazione effettuata da burpsuite



**Fase 3**

Una volta caricata la shell, adesso utilizzeremo il metodo GET per modificarlo. Di seguito le immagini che mostrano come è stato modificato il file.  
  
Prima della modifica



Dopo la modifica  


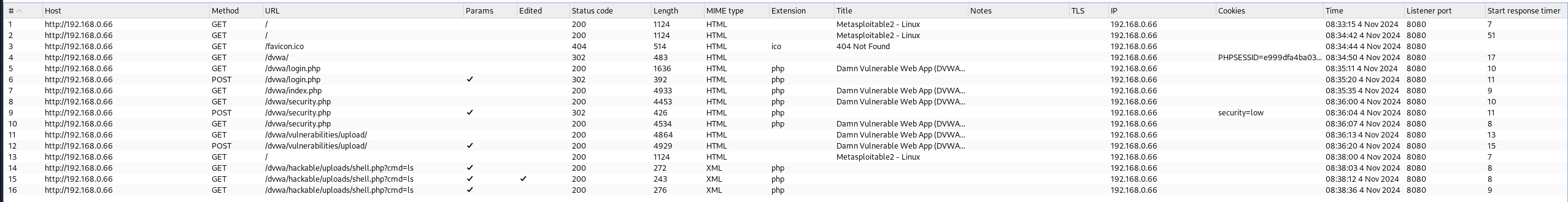
Abbiamo utilizzato burpsuite per modificare il file:

Input prima della modifica



Input dopo la modifica



Per concludere, uno screen di tutti i passaggi catturati da burpsuite: