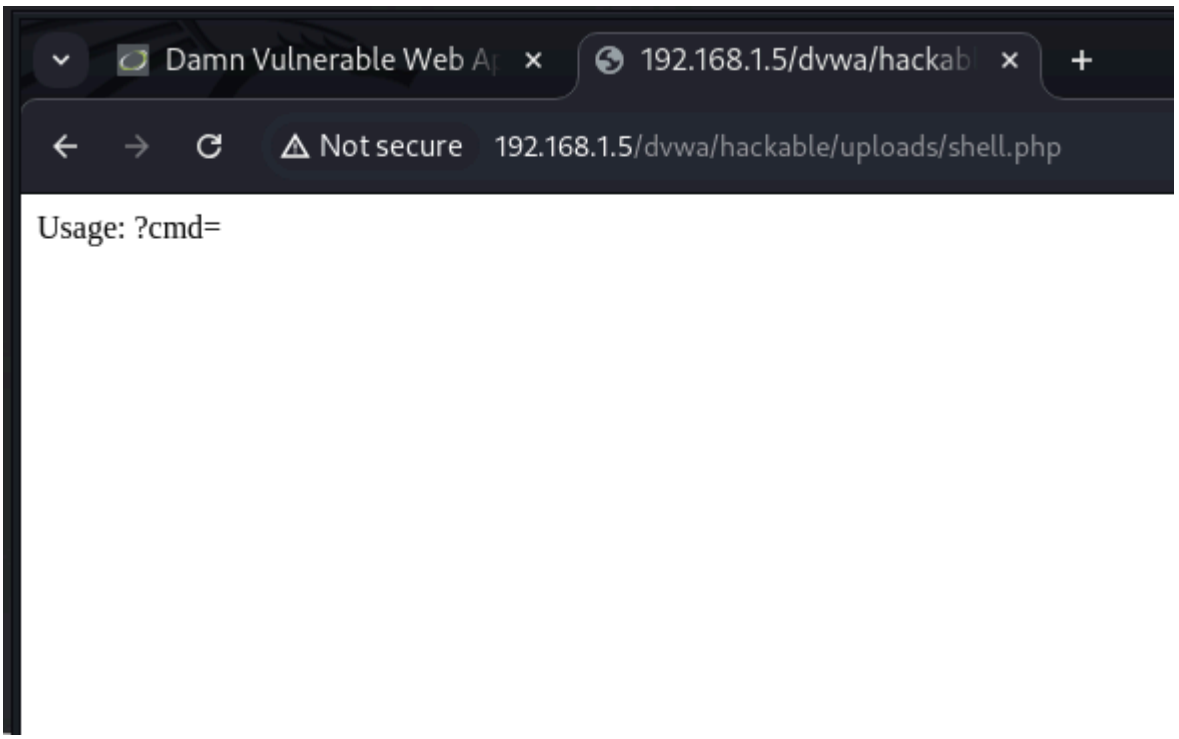
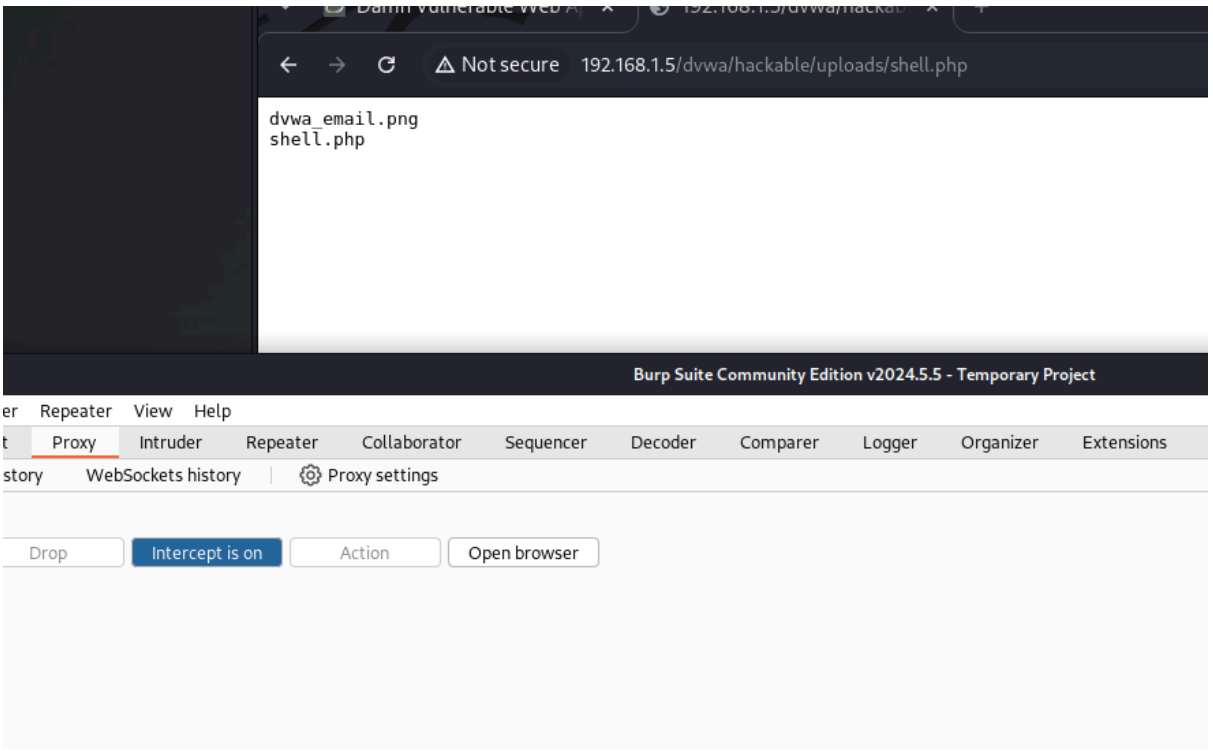
**Esercizio S6L1 - Upload di un programma .php su Metasploitable**

L'esercizio di oggi prevedeva la messa in pratica della fase di exploit caricando caricando un file .php sulla macchina Metasploitable2.

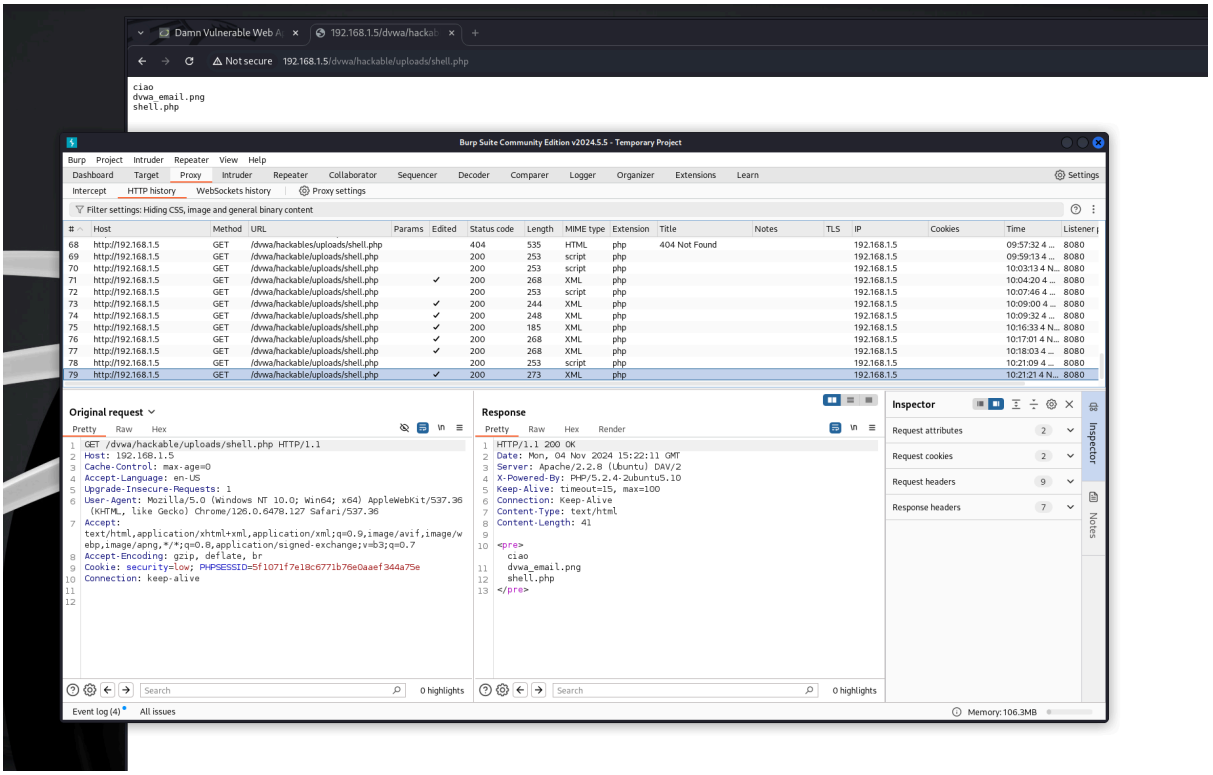
Dopo aver settato la sicurezza della macchina a "low" per permettere l'upload del file stesso, visitando la pagina dove è stato caricato il file possiamo vedere che, come da programma php datoci in fase di consegna, il codice ci avvisa che per utilizzarlo per i vari scopi (malevoli o non) per cui stiamo facendo l'upload, bisogna utilizzare il comando ?cmd= e il comando stesso da eseguire; questo è dato dal costrutto if else scritto nel nostro file shell.php, che restituisce questa stringa qualora non sia stato eseguito nessun comando di quelli previsti.



Inserendo quindi nella stringa di BurpSuite da cui stiamo aprendo il browser già intercettato, possiamo inserire ?cmd=ls e ottenere la lista dei file interni all'URL che stiamo considerando, in questo caso, come da screenshot, dvwa_email.png e shell.php.



Aggiungendo il comando “echo%20ciao” invece riusciamo anche ad ottenere la ripetizione della parola “ciao” come dimostrato in quest’ultimo screen. Utilizzando tutti i comandi legati a cmd possiamo ottenere diversi risultati a seconda delle nostre esigenze.




Questa è la dimostrazione pratica di cosa si può ottenere attraverso GET in un sistema (in questo caso volutamente) vulnerabile e quali possano essere i rischi relativi nelle mani sbagliate. Qualora il nostro “shell.php” fosse stato un codice malevolo a cui far eseguire comandi più complessi e sofisticati, avremmo potuto compromettere l'intero sistema, sottrarre dati sensibili o alterare la configurazione della macchina target.