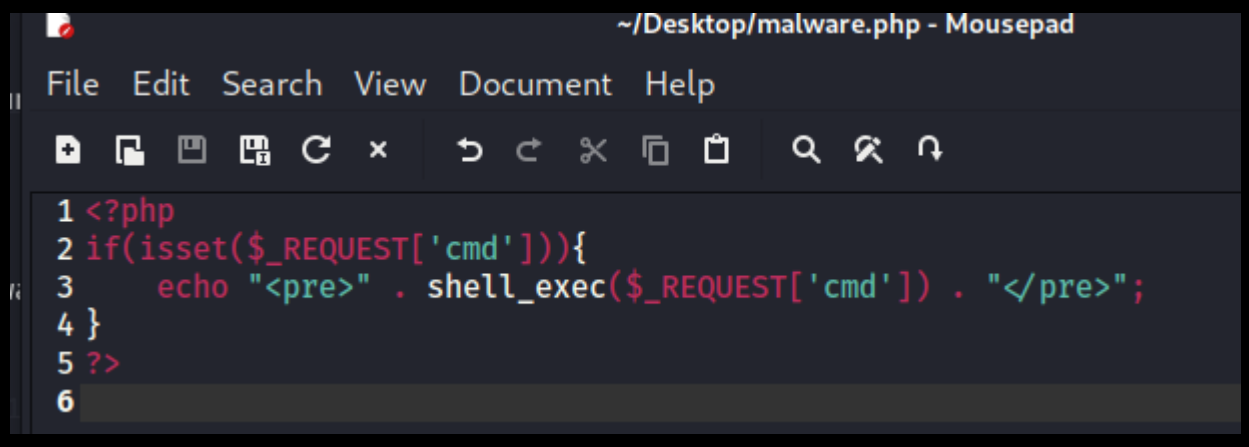
Exploit file upload

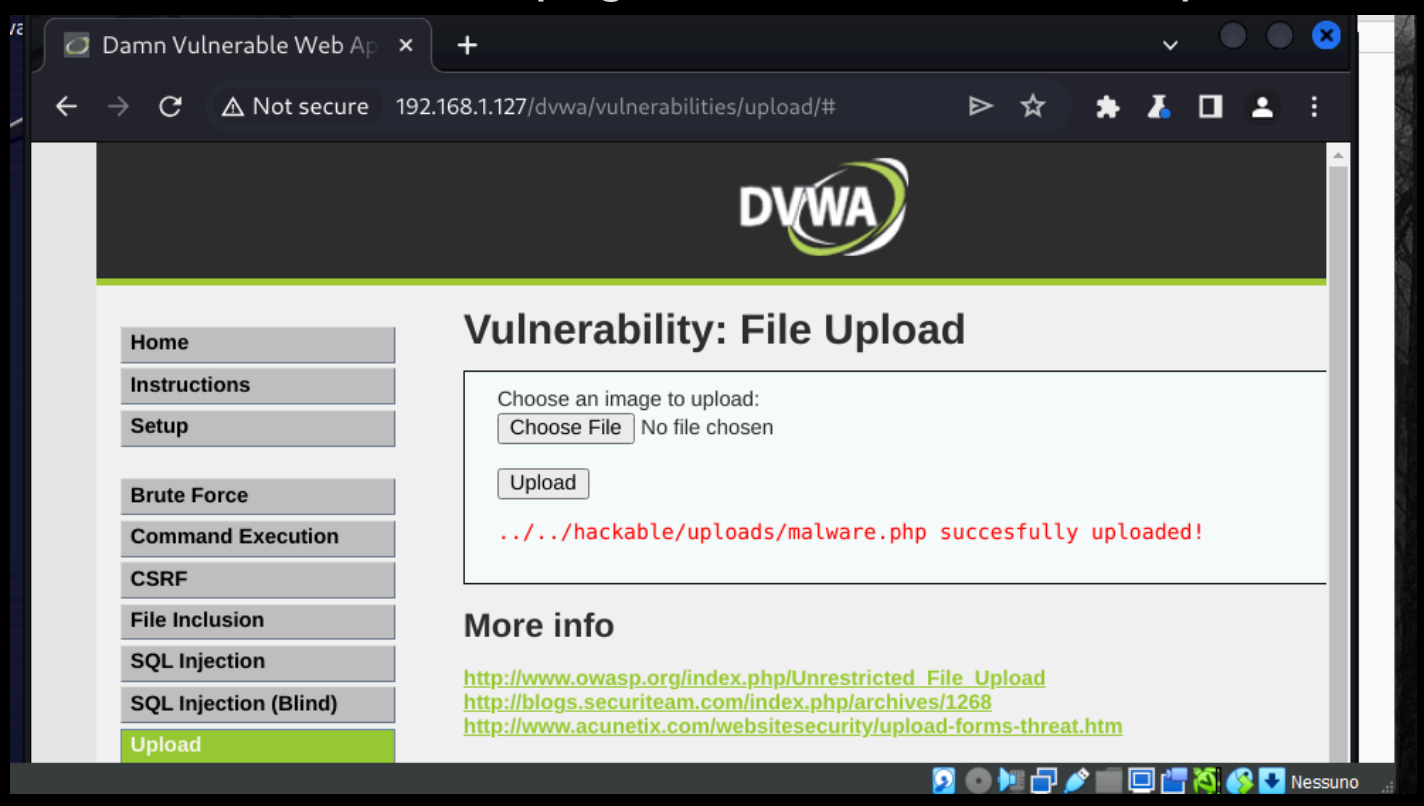
Richiesta: Sfruttare la vulnerabilità di «file upload» presente sulla DVWA per prendere controllo della macchina ed eseguire dei comandi da remoto tramite una shell in PHP, il tutto controllato tramite il programma burpsuite.

Script php:



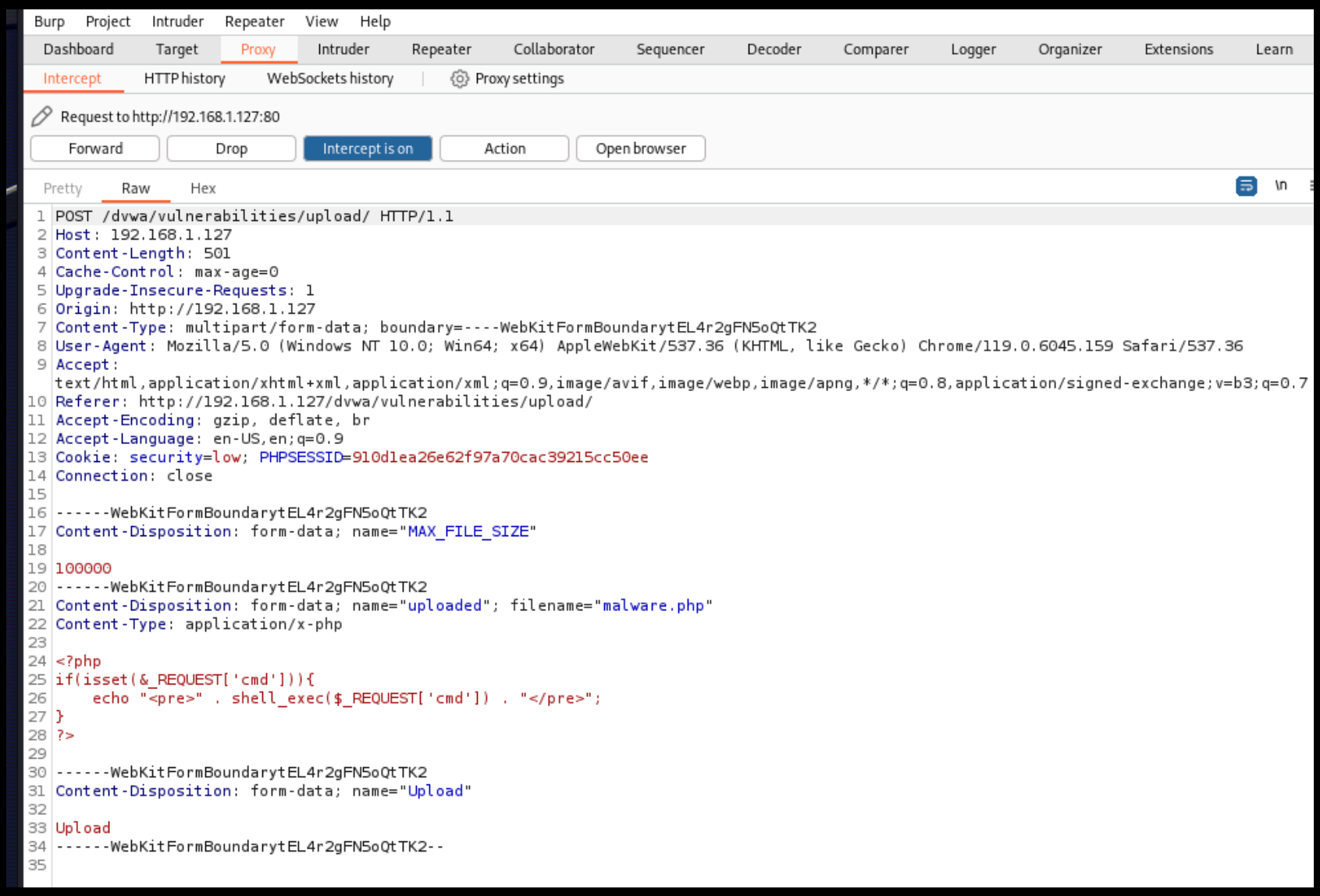
Tramite questo script potremo accedere alla shell della macchina vittima tramite browser.

Carichiamo il file nella pagina della dvwa di metasploitable:



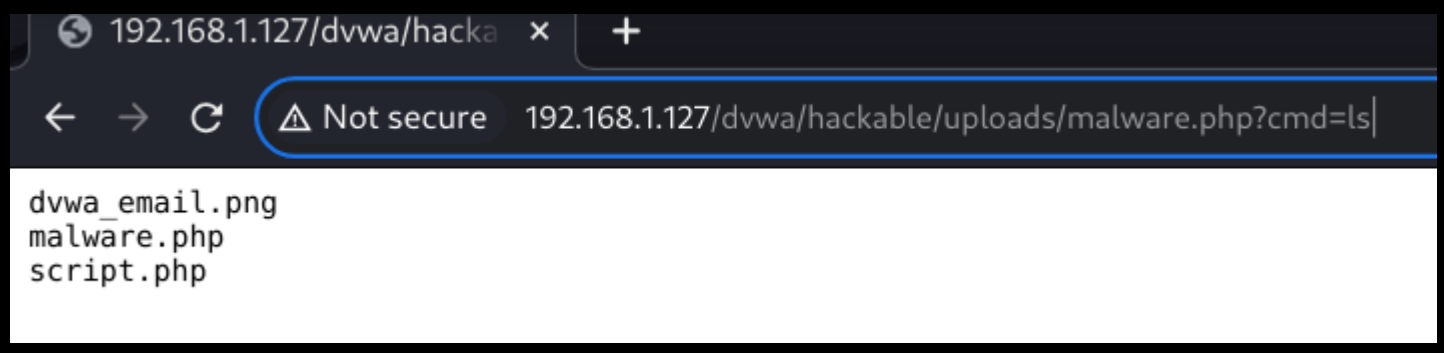
Qui il file è stato caricato con successo, viene indicato anche il path per raggiungerlo.

Adesso osserviamo le intercettazioni di burpsuite quando si prova a caricare il file:



Notiamo una richiesta POST (Hypertext Transfer Protocol), uno dei metodi di richiesta utilizzati dai client per inviare dati a un server.
Ci presenta anche il contenuto del file, capendo ovviamente che si tratta di un payload malevolo.

Proviamo adesso ad accedere alla shell tramite browser e digitiamo un comando di prova:



Utilizzando il comando ls riusciamo a leggere il contenuto della directory interessata.

L’attacco ha avuto successo.