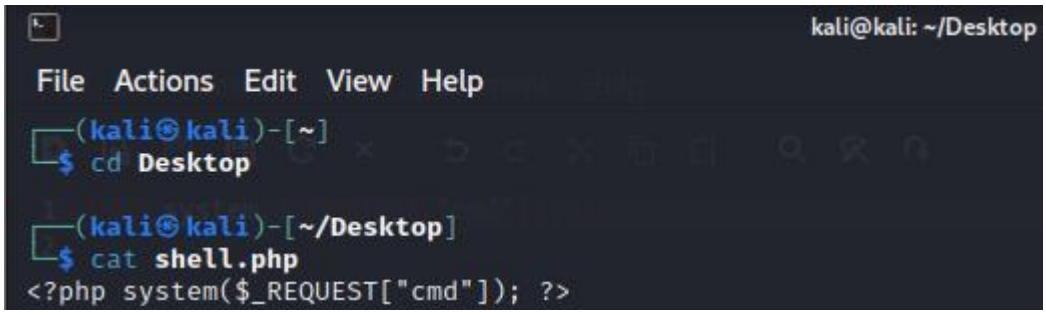
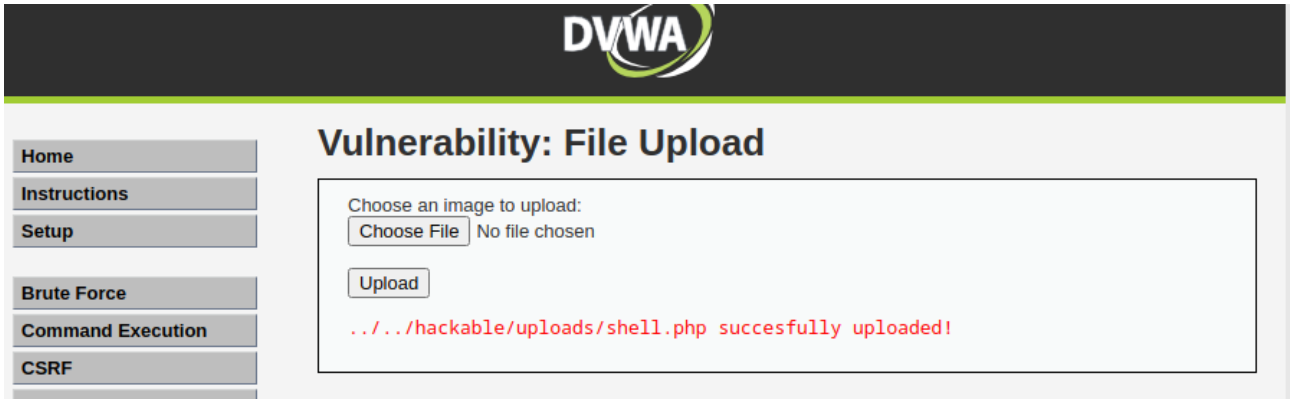
Vediamo come sfruttare un file upload sulla DVWA per caricare una semplice shell in PHP. Monitoreremo tutti gli step con BurpSuite:

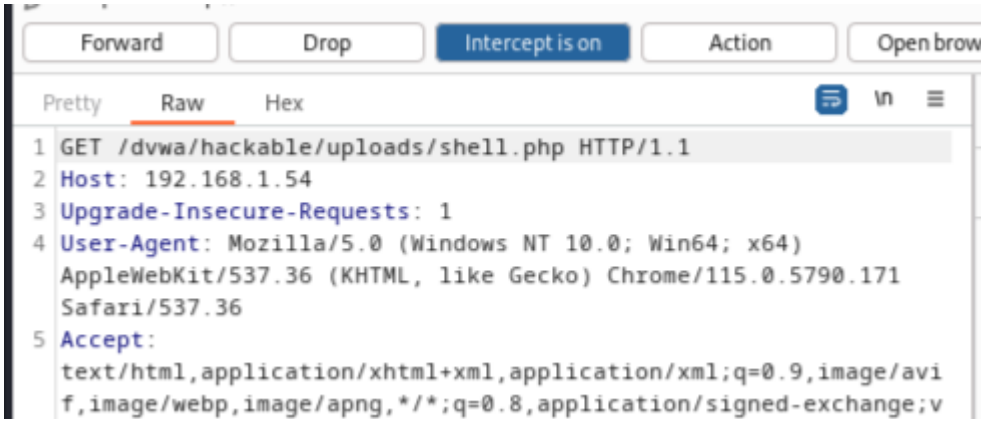
- Creiamo la nostra shell



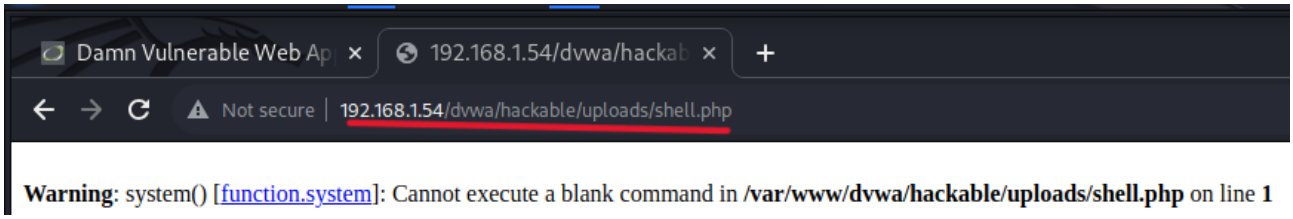
- Andiamo ad uploadare la nostra shell su DVWA, come notiamo ci viene restituito un messaggio, dove dice che il path "../../hackable/upload/shell.php" è stato caricato correttamente, ovvero che la nostra shell è stata caricata.



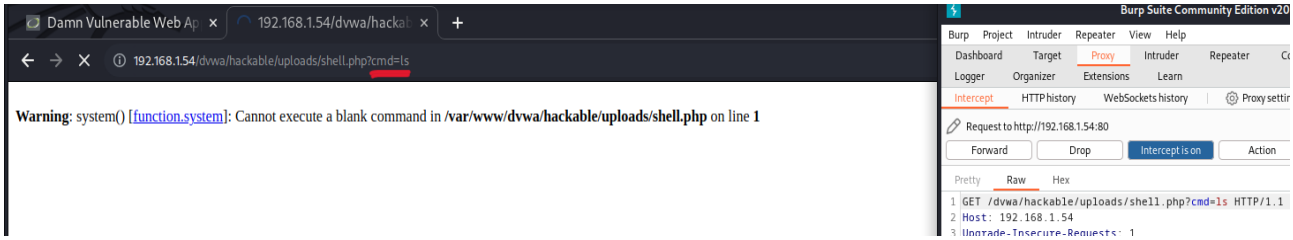
- Su Burpsuite, notiamo come appare la richiesta di tipo GET contenente per l'appunto il path



- Andando a digitare il path, notiamo come inizialmente ci dia un errore, questo perché la nostra shell si aspetta un parametro cmd nella GET con un comando da eseguire, mentre noi al momento non abbiamo passato nessun argomento.



- Aggiungiamo il parametro *cmd=ls* nella GET.



- L'applicazione ci ha restituito la lista dei file. Ciò significa che la richiesta «ls» è stata eseguita dalla shell. Notate nel rettangolo in rosso come viene passato il parametro da eseguire via GET.