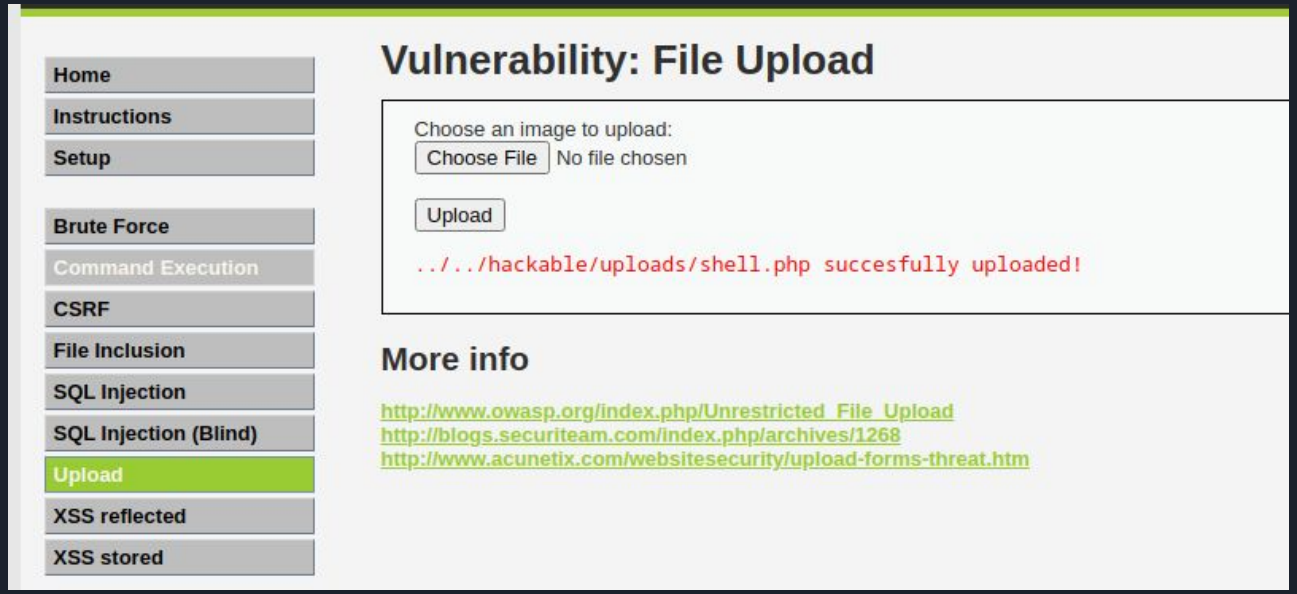
EXPLOIT FILE UPLOAD

CODICE PHP UTILIZZATO:

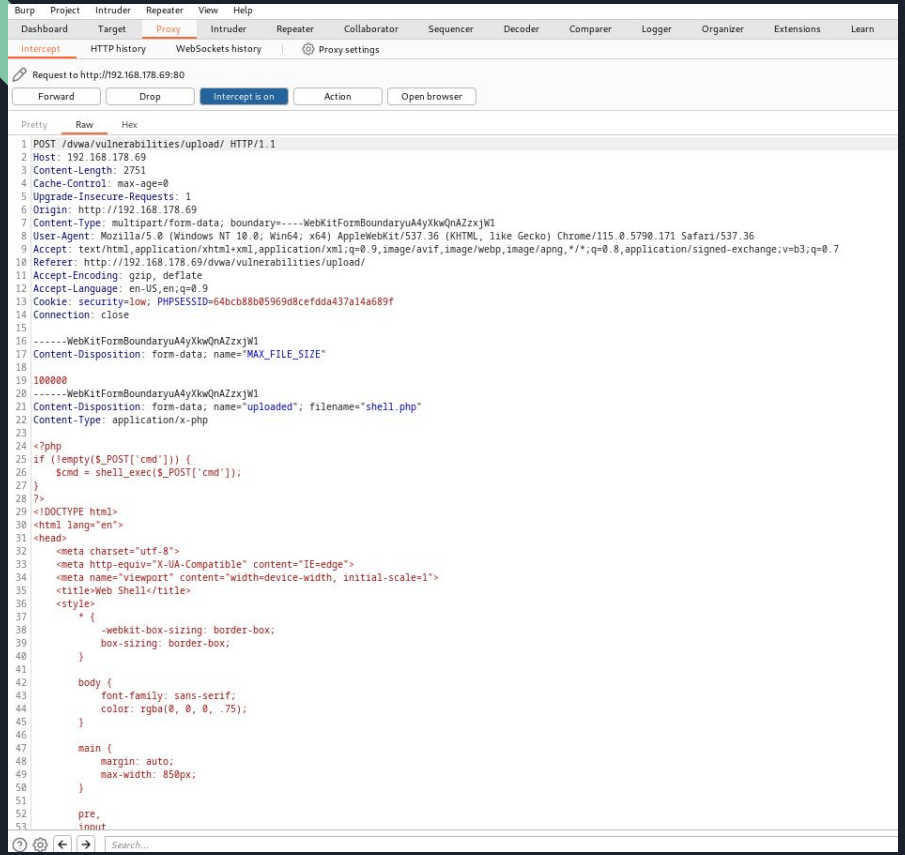
- Come codice php dello script ho utilizzato un codice che contiene un’interfaccia grafica per facilitare l’utilizzo. Lo script permette di accedere ad un'istanza CMD dal server in modo da inviare comandi a nostro piacimento.

Link al codice PHP GitHub

RISULTATO CARICAMENTO



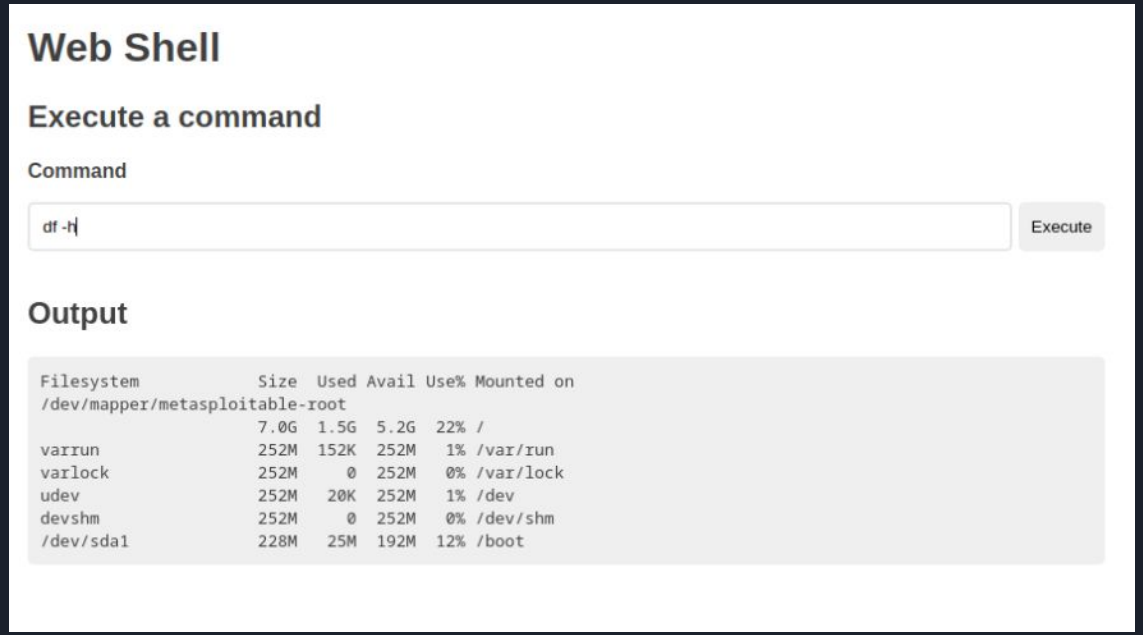
INTERCETTAZIONI



- Come si può notare dallo screen di Burp Suite. Lo script e stato inserito correttamente

RISULTATO

- Una volta caricato ho inserito l'indirizzo: **192.168.50.101/dvwa/hackable/uploads/shell.php**



abbiamo accesso all'interfaccia grafica della Web Shell dove abbiamo modo di inserire i vari comandi. Nell'esempio abbiamo usato il comando df -h che ci da una "visuale" dello spazio utilizzato del disco del sistema.
Come altri test abbiamo usato:
netstat
whoami