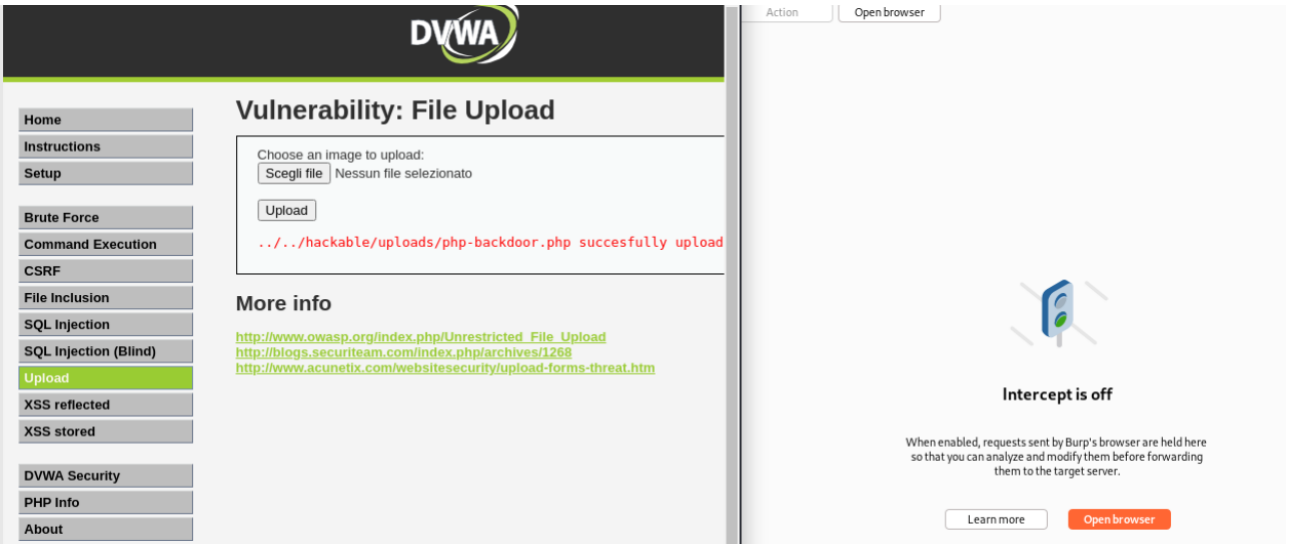
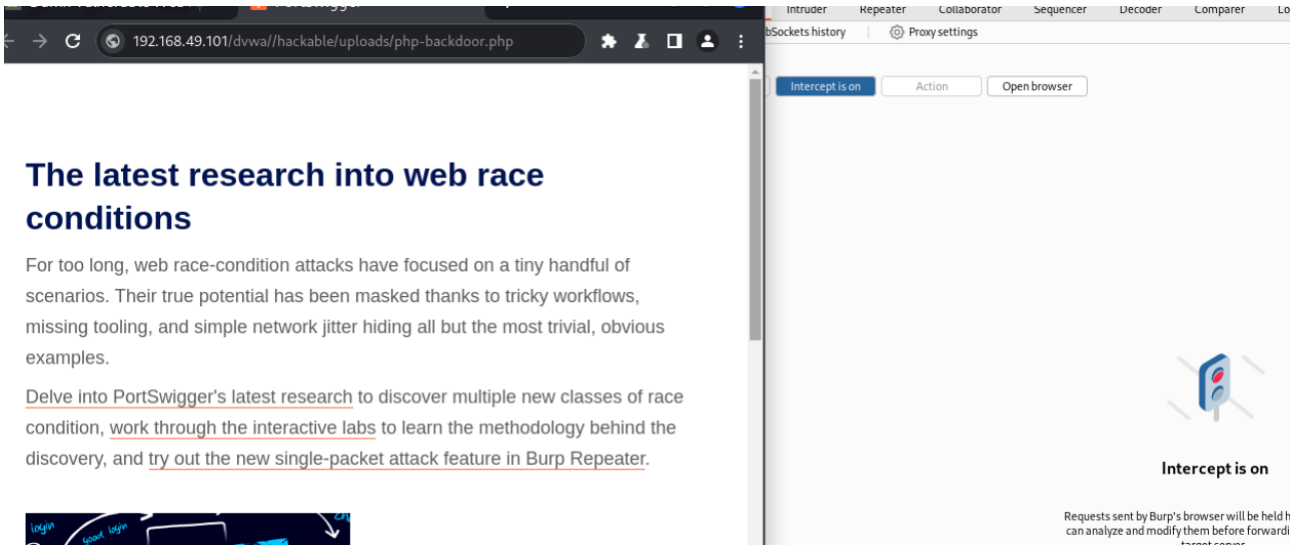
Esercitazione 2 Modulo 4 – Alessio Russo

Utilizzare delle shell su DVWA per esercitazione php – inserire shell complesse.

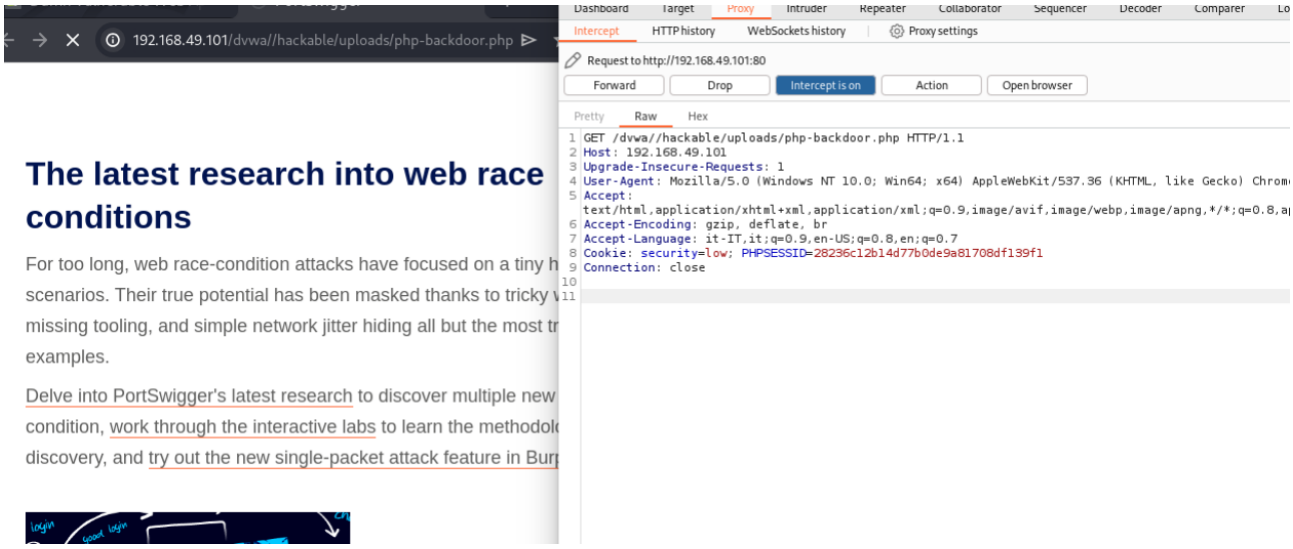
1) Una volta avviate le machine e burp suite, aperto I l browser e inserito l'ip di meta nella b arra delle ricerche, cliccato su DVWA ->Upload, carico innanzitutto un' immagine successivamente Carico sempre in DVWA la shell php-backdoor presente in kali -> usr/share/webshell/backdoor.php.



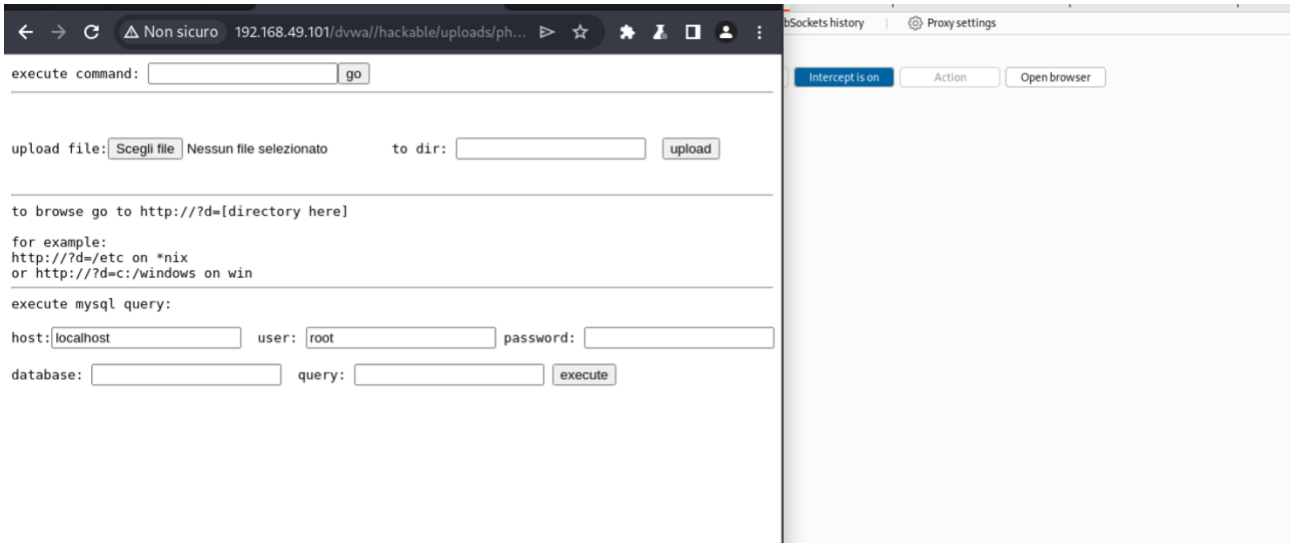
2) Inserisco il percorso della shell appena caricata dopo 192.168.49.101/dvwa -> percorso server e attivo intercepter in modo da permettere a burp suite di intercettare la chiamata browser.



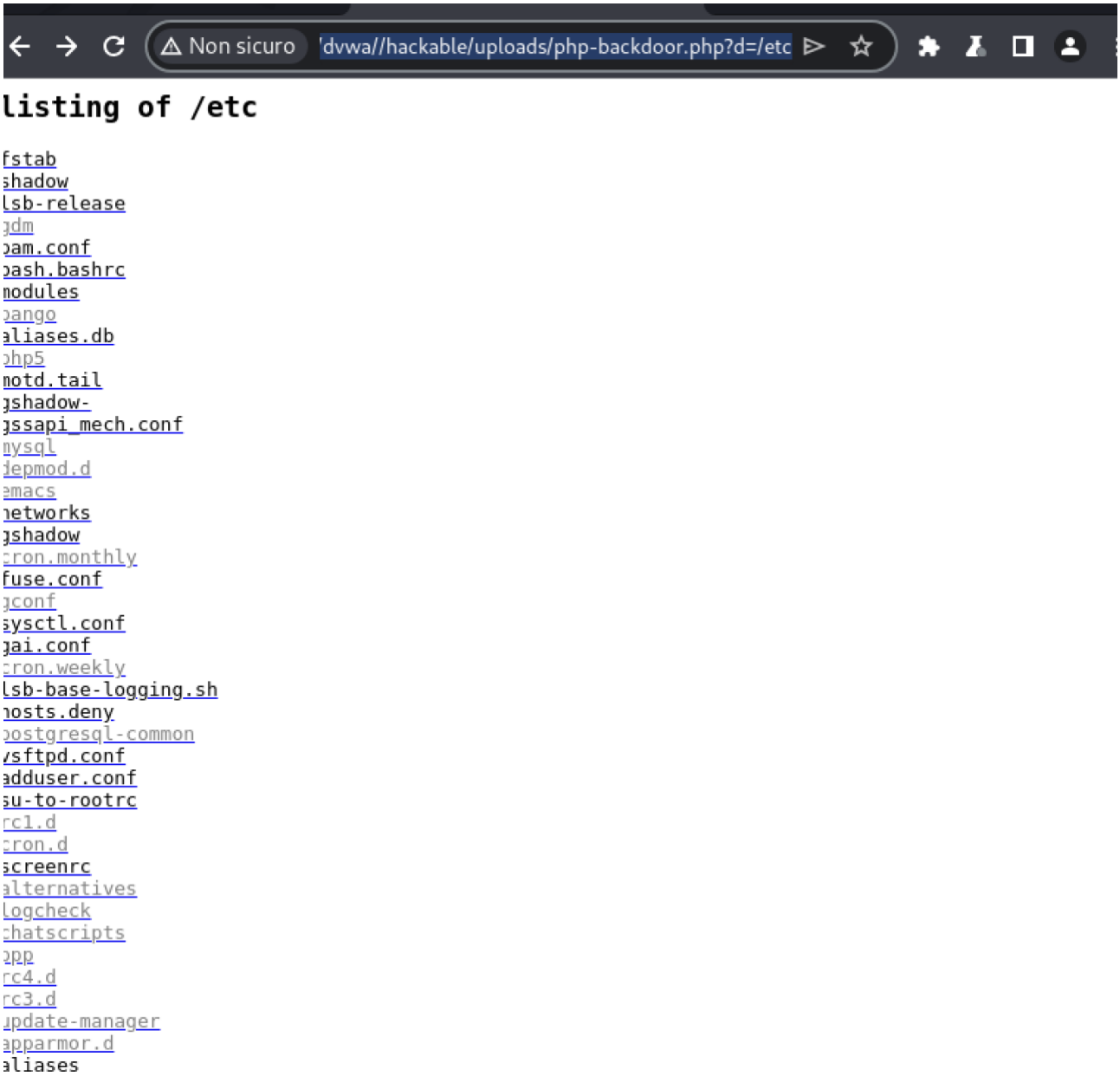
3) Avvio la webshell



Il risultato sarà il seguente troviamo un form dove possiamo andare ad inserire una serie di parametri permesso dalla backdoor appena creata.



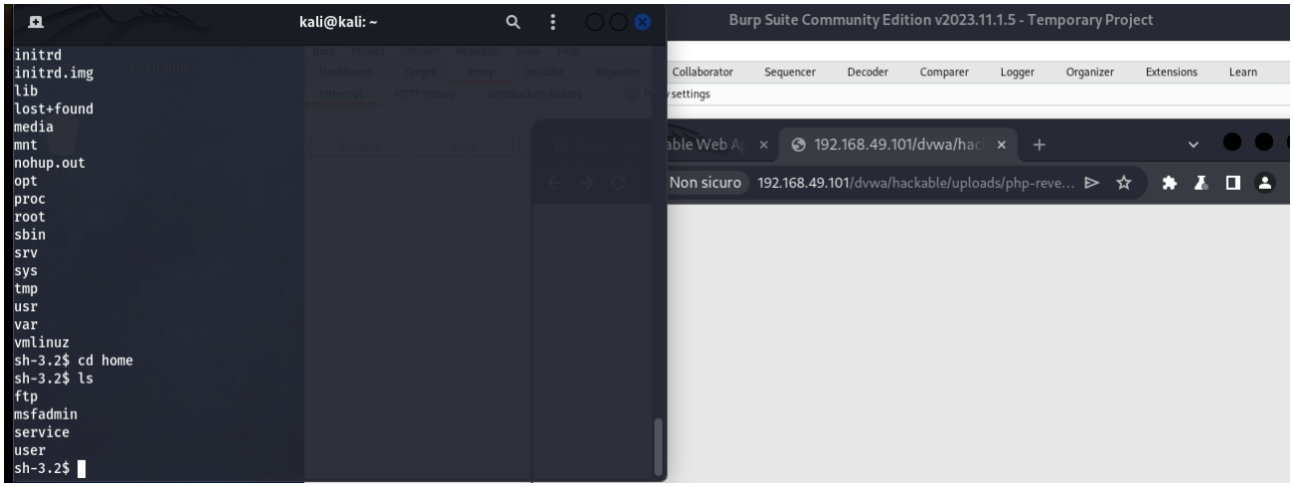
Possiamo ad esempio avere una lista di tutte le directory andando a completare l'indirzzo con:
? d=/etc - Il risultato sarà una lista di tutte le directory presenti in DB



4) test di shell reverseshell.php -> carico shell ed eseguo indirizzo kali, metto in ascolto kali con:

nc -l -p [porta] che in questo caso sarà 5005

inoltre nel file contenente il codice php della reverse shell vado ad inserire i parametri IP kali (192.168.50.100) e porta su cui vogliamo metterci in ascolto (5005)



Si vede chiaramente che sto controllando la macchina metasploitable infatti tra le disponibili nell'elenco a destra troviamo msfadmin su cui ho il completo controllo