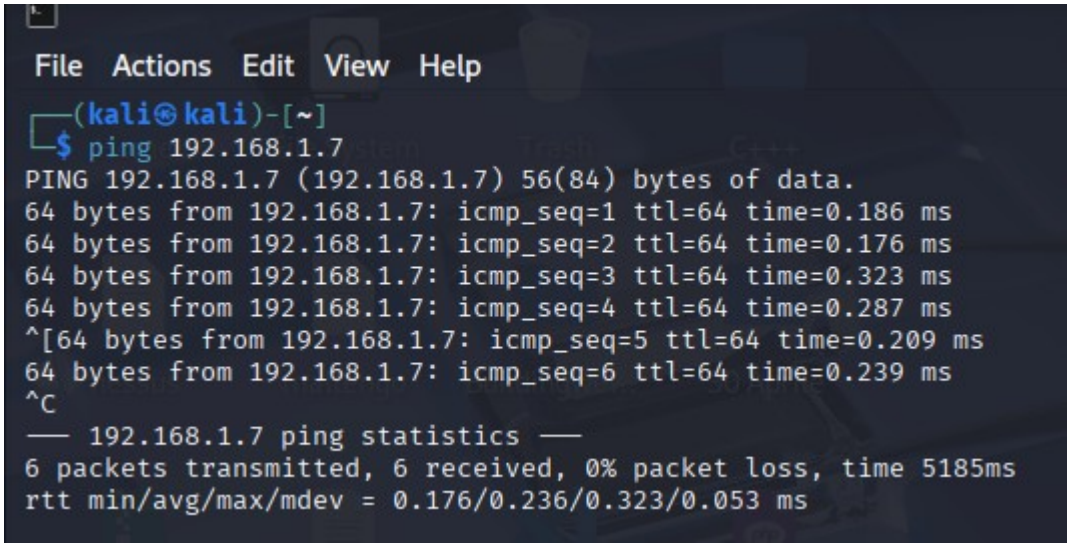
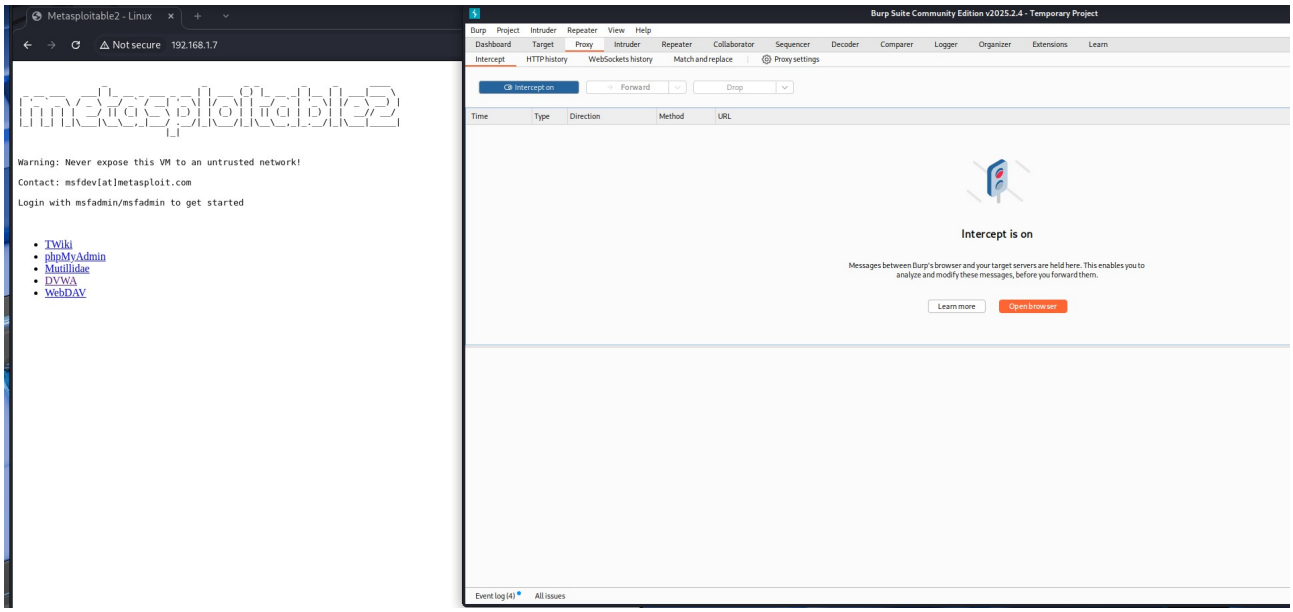
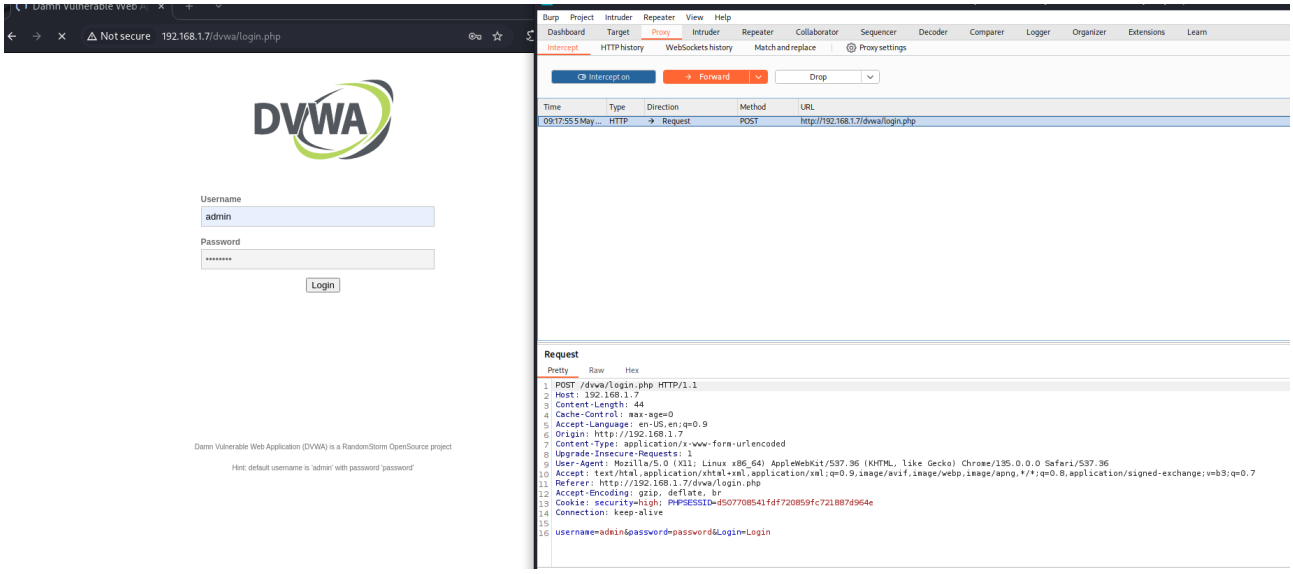
Sfruttamento di una vulnerabilità di File Upload sulla DVWA per l'inserimento di una shell in PHP

1.Per prima cosa andiamo a mettere in comunicazione le nostre 2 macchine virtuali. Una volta fatto ciò possiamo verificare che siano in comunicazione tramite il ping.



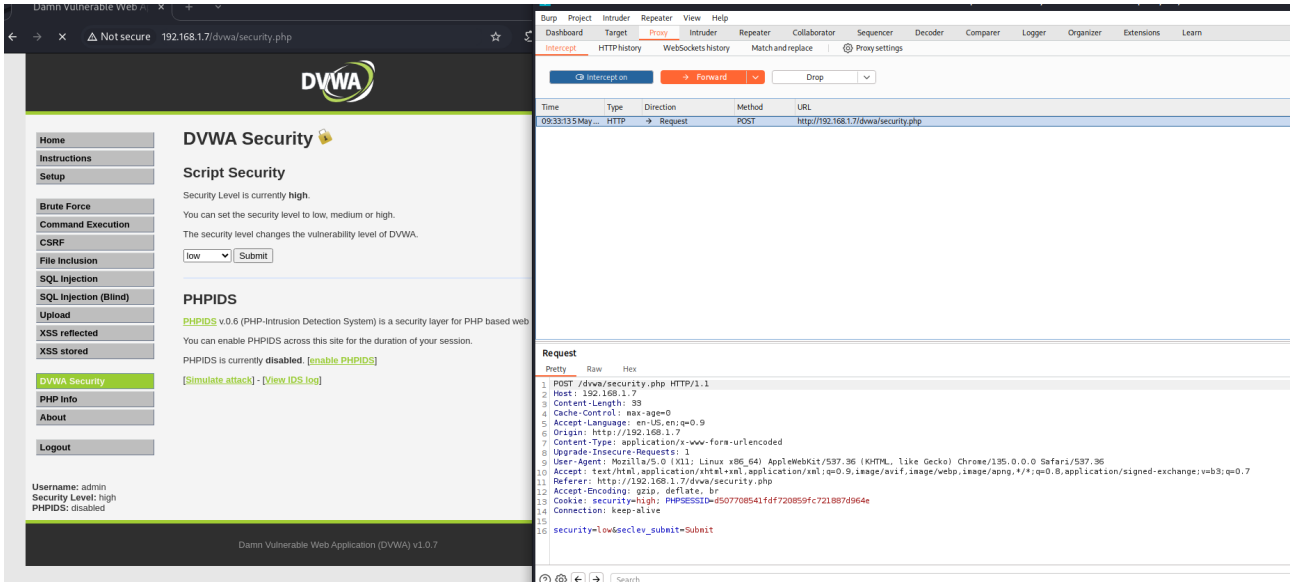
2.Andiamo adesso ad aprire **Burpsuite** avviamo **l'interceptor** e andiamo su **open browser.** Dalla sessione del browser appena aperta, connettiamoci alla nostra macchina Metasploitable, quindi selezioniamo DVWA.



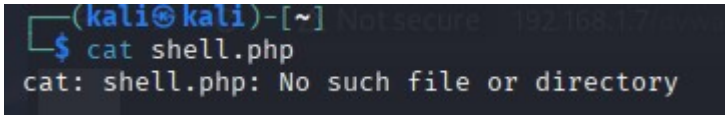


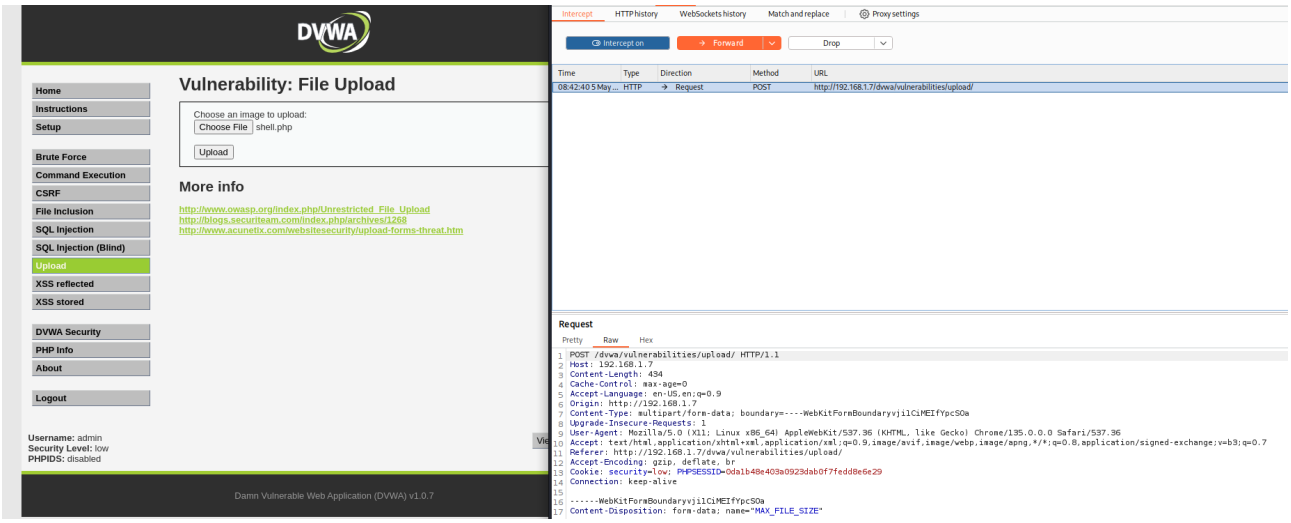
Possiamo notare come la richiesta http che riceviamo quando inseriamo le credenziali è **POST** (possiamo anche notare le credenziali scritte in basso quali sono).

Modifichiamo la sicurezza di DWVA da high a low, ottenendo la richiesta **POST**, in modo tal da poter caricare il file



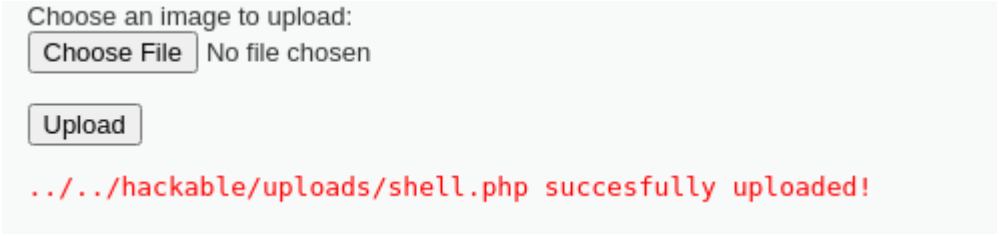
Andiamo nella sezione upload e carichiamo la shell.php, che ci garantisce un **accesso remoto** al server **tramite il sito**. Di seguito la shell caricata.



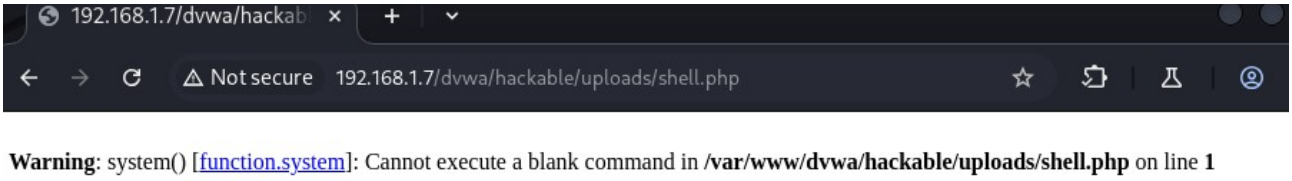


Anche in questo caso la richiesta che otteniamo e **POST**

3.Una volta caricato il file dovrebbe essersi salvato nella cartella server, al path:

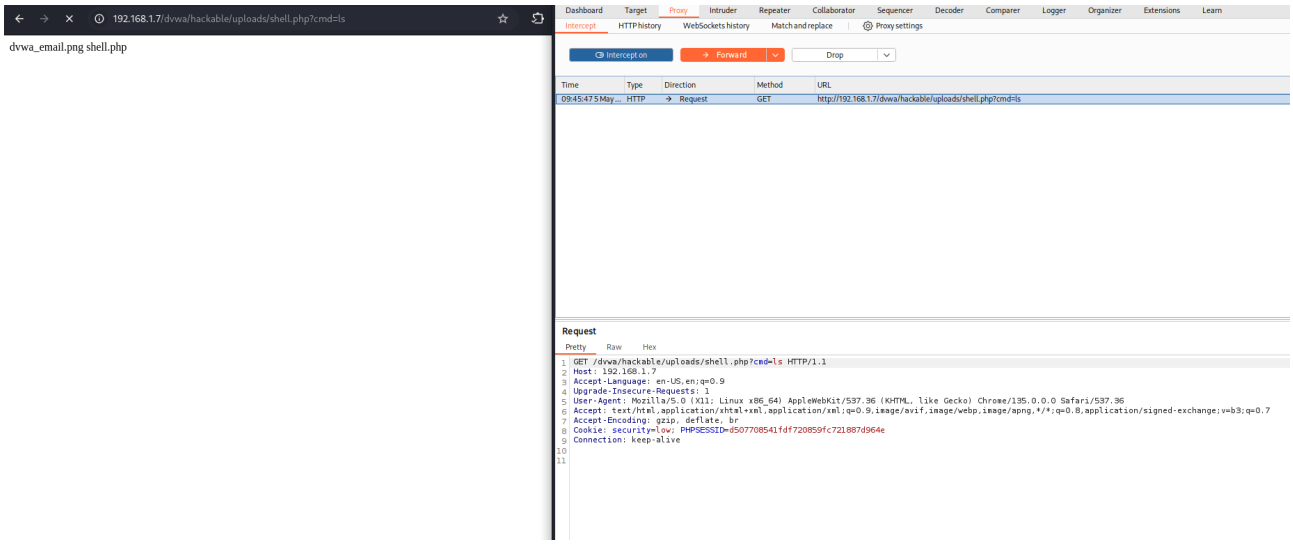


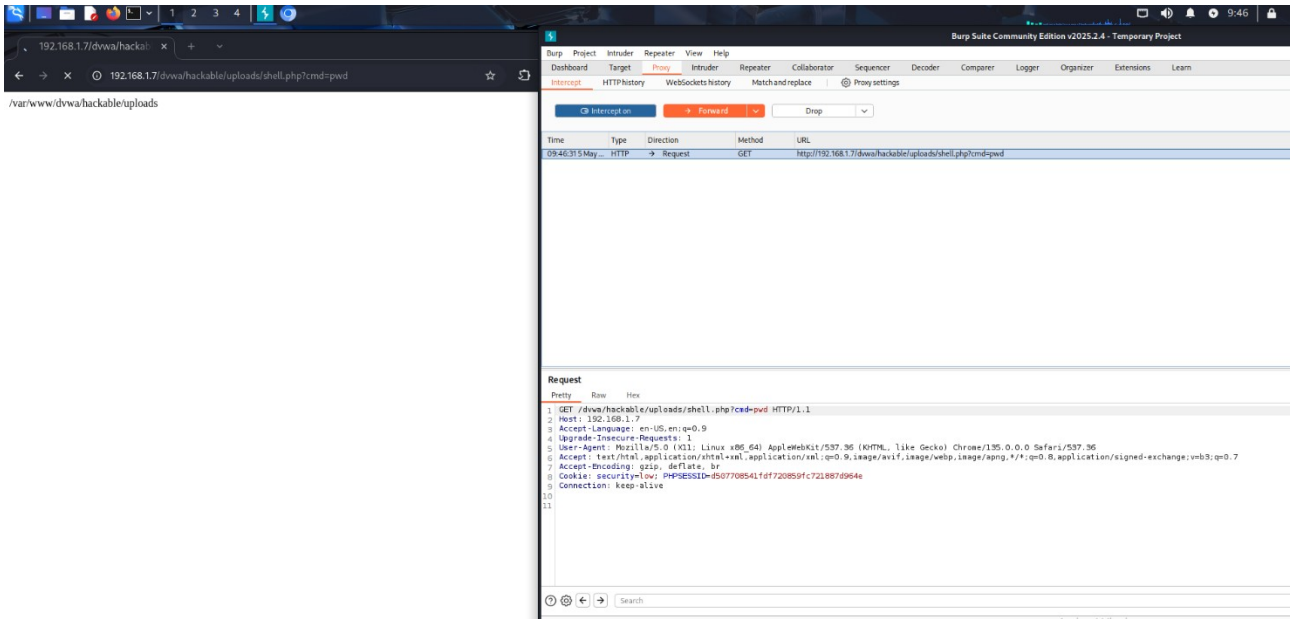
Una volta aperto questo URL notiamo che la pagina ci restituisce errore, perchè la shell non ha alcun parametro cmd (in una richiesta **GET**) che determinata il comando da eseguire.

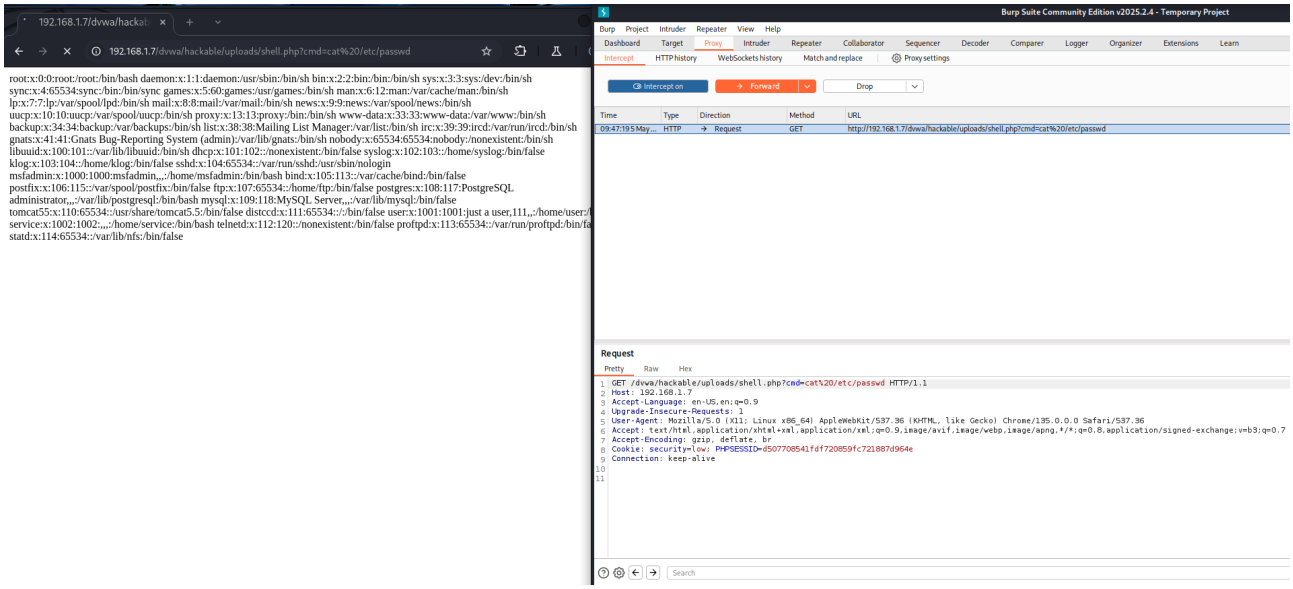


Per rimediare, andiamo ad aggiungere al path cmd=”comando” per fare in modo che la nostra shell esegua i comandi.

Andiamo ad eseguire 3 comandi: ls, pwd e, il più pericoloso, cat /etc/passwd







In tutti e tre i casi otteniamo la richiesta **GET**

4.Conclusione

L'esercizio ha dimostrato con successo come un errore nella gestione dell’upload dei file possa essere sfruttata per ottenere l’esecuzione remota di comandi sul server target. Questa è una grave vulnerabilità perchè un attaccante potrebbe rubare file (tramite il comando **cat /etc/passwd**), aggiungere utenti o scaricare virus e malware.