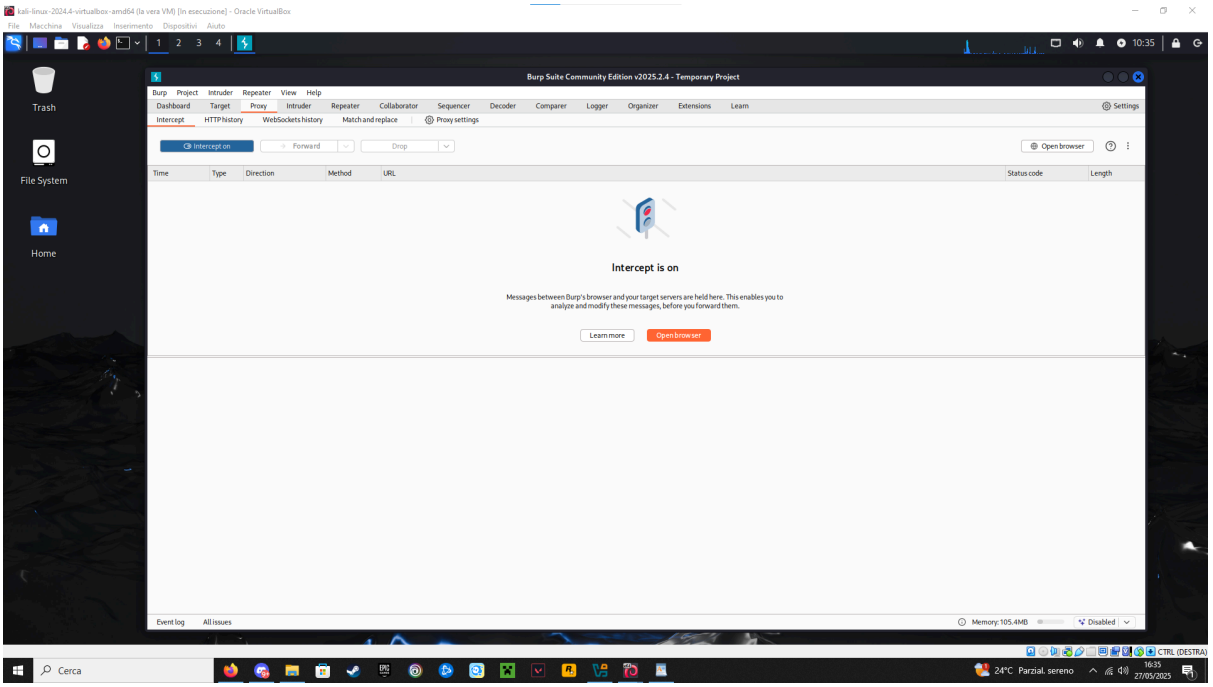
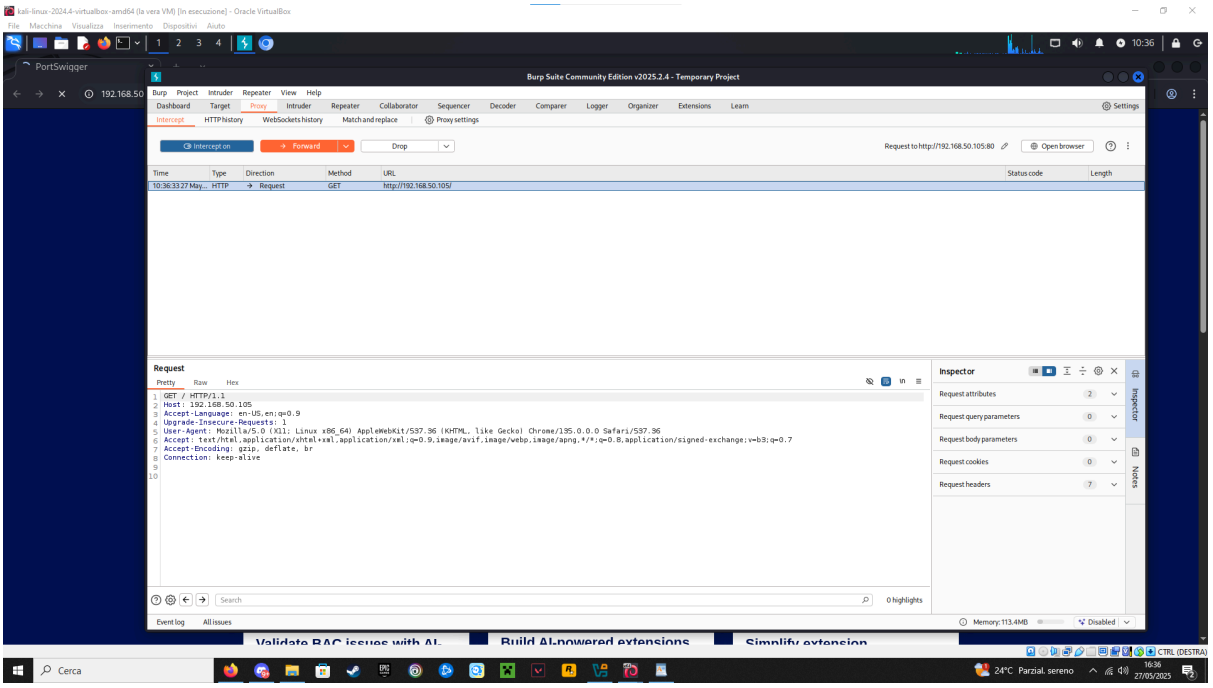
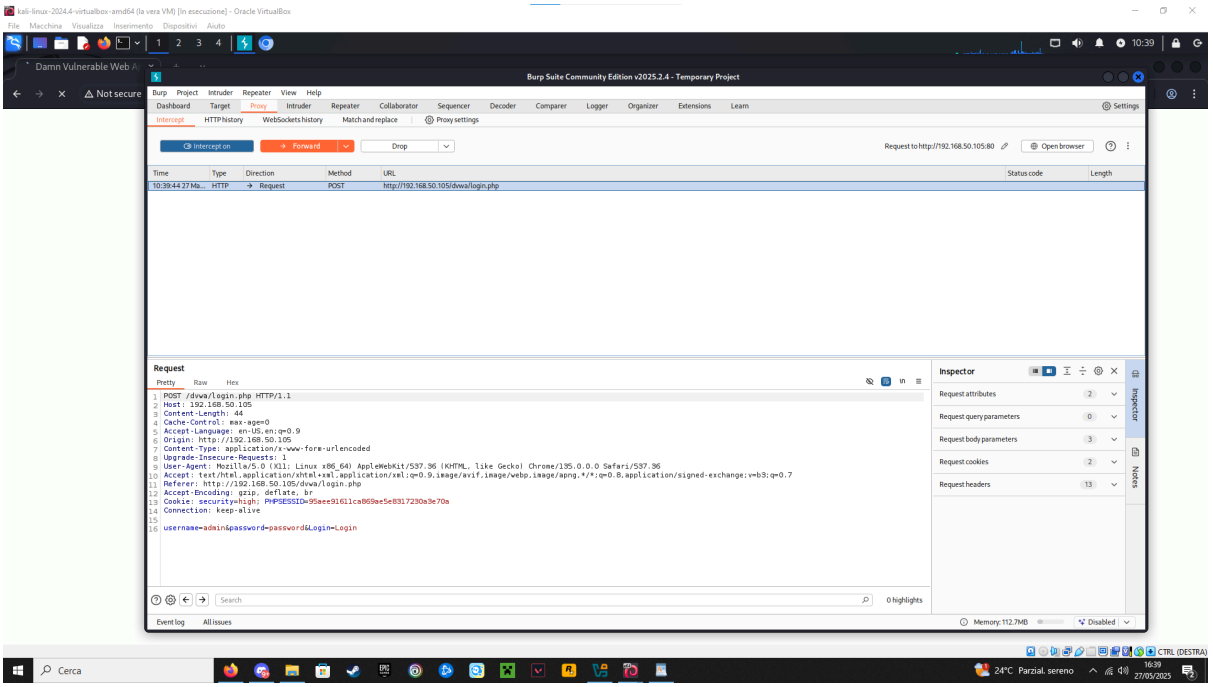


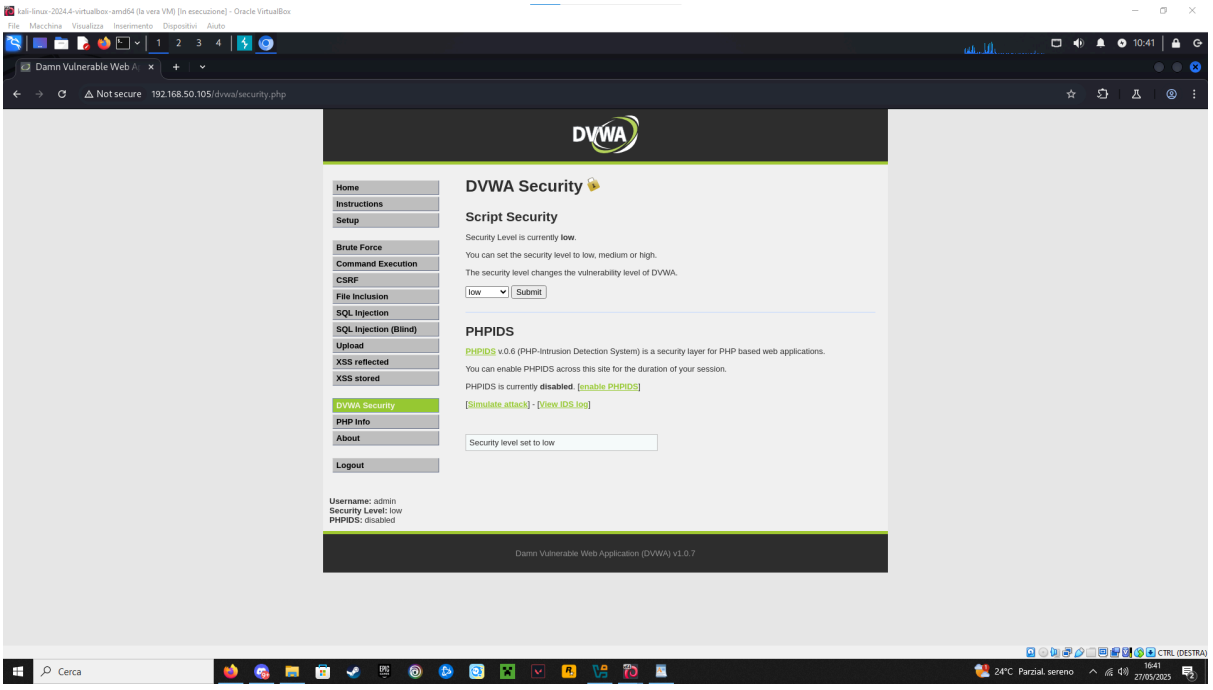
assicuriamoci che burpsuite sia su ON e poi fare open browser



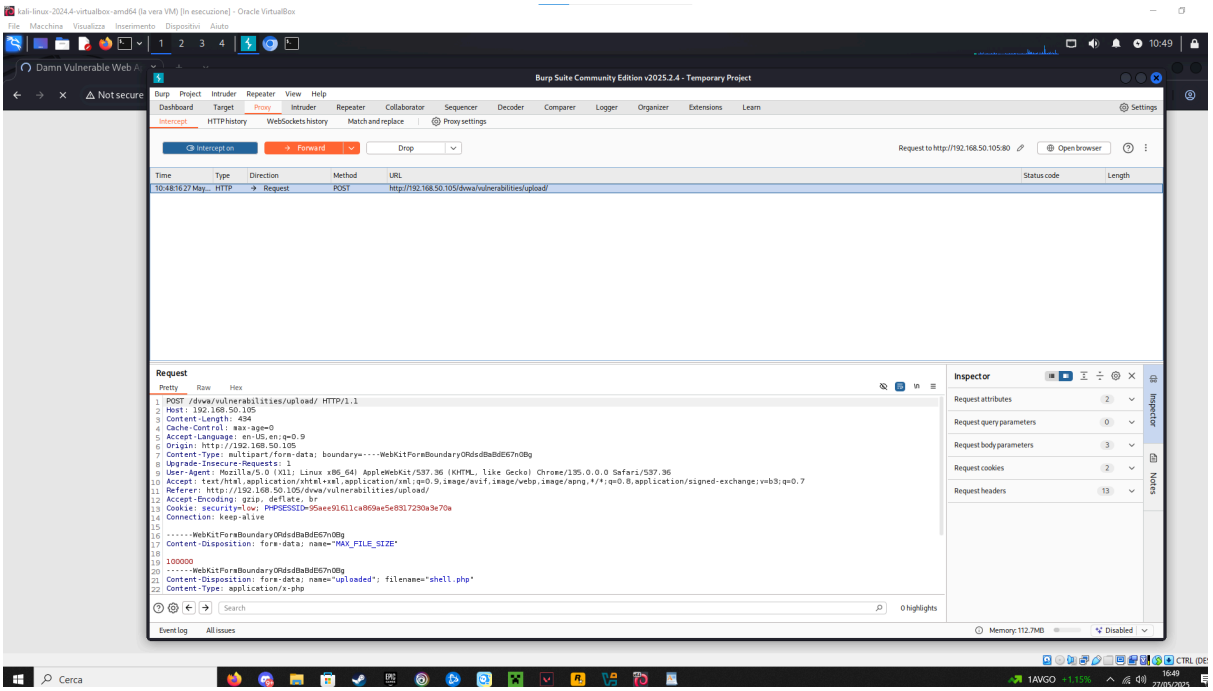
adesso dovremmo accettare ogni richiesta per proseguire sul sito da burpsuite



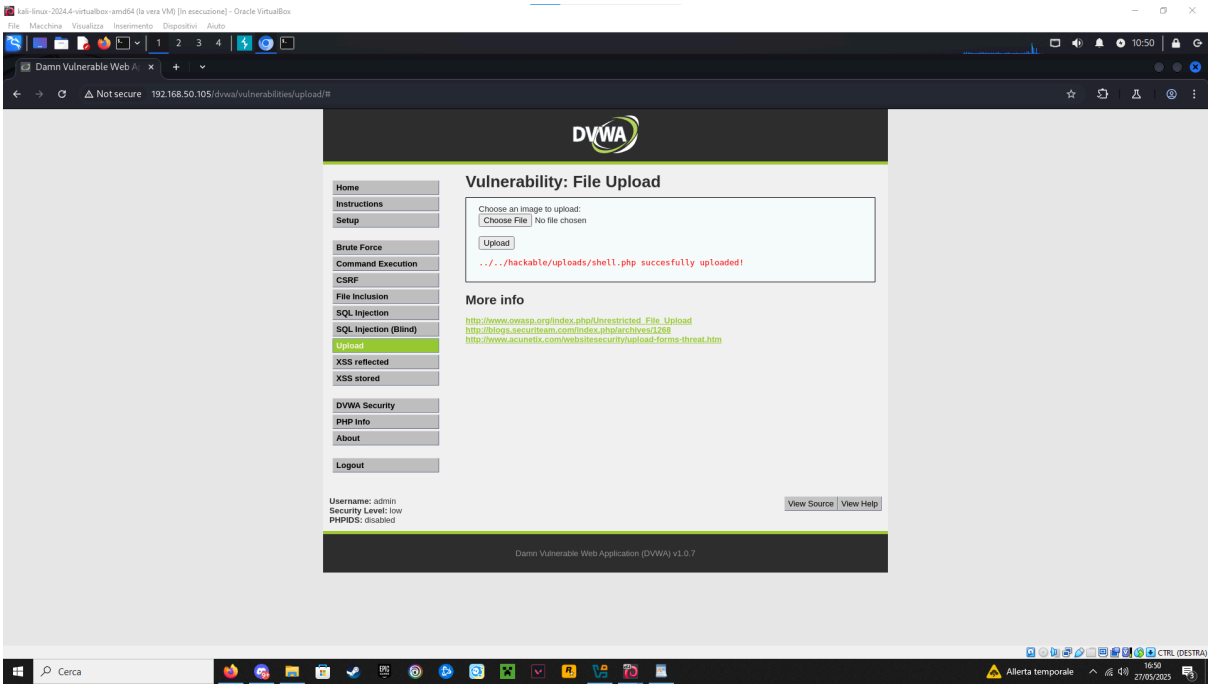
una volta messo le credenziali su dvwa , da burpsuite vediamo il corpo della richiesta POST con le credenziali appena inserite



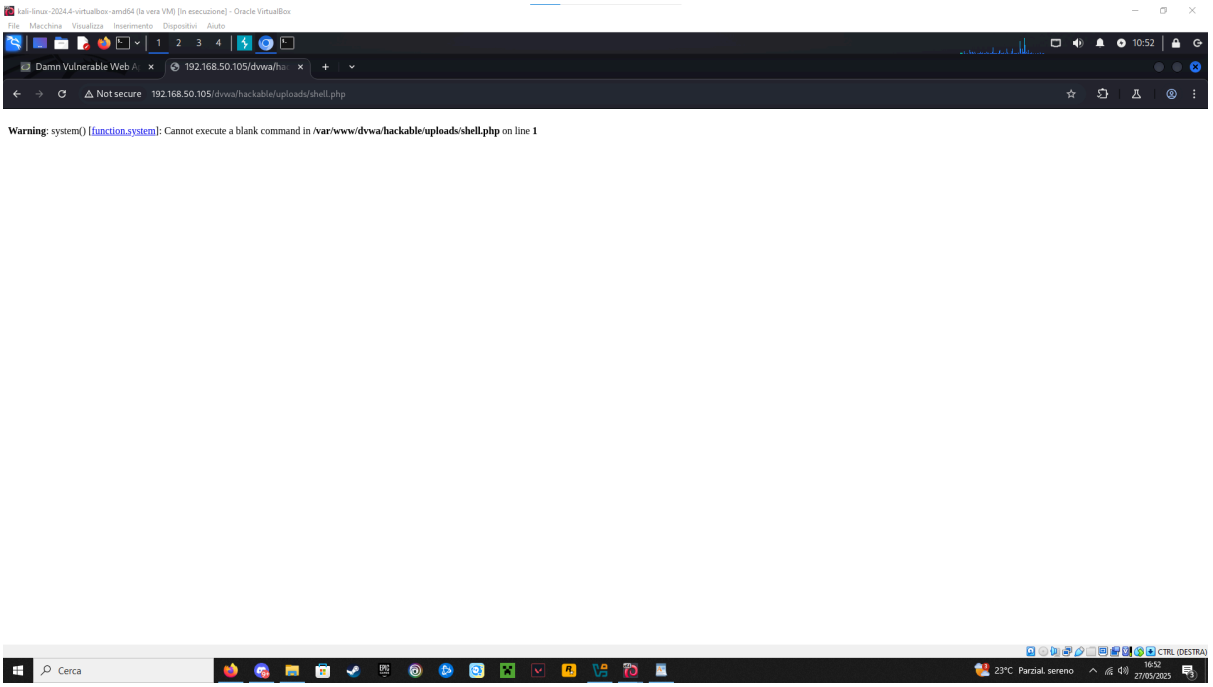
inseriamo LOW



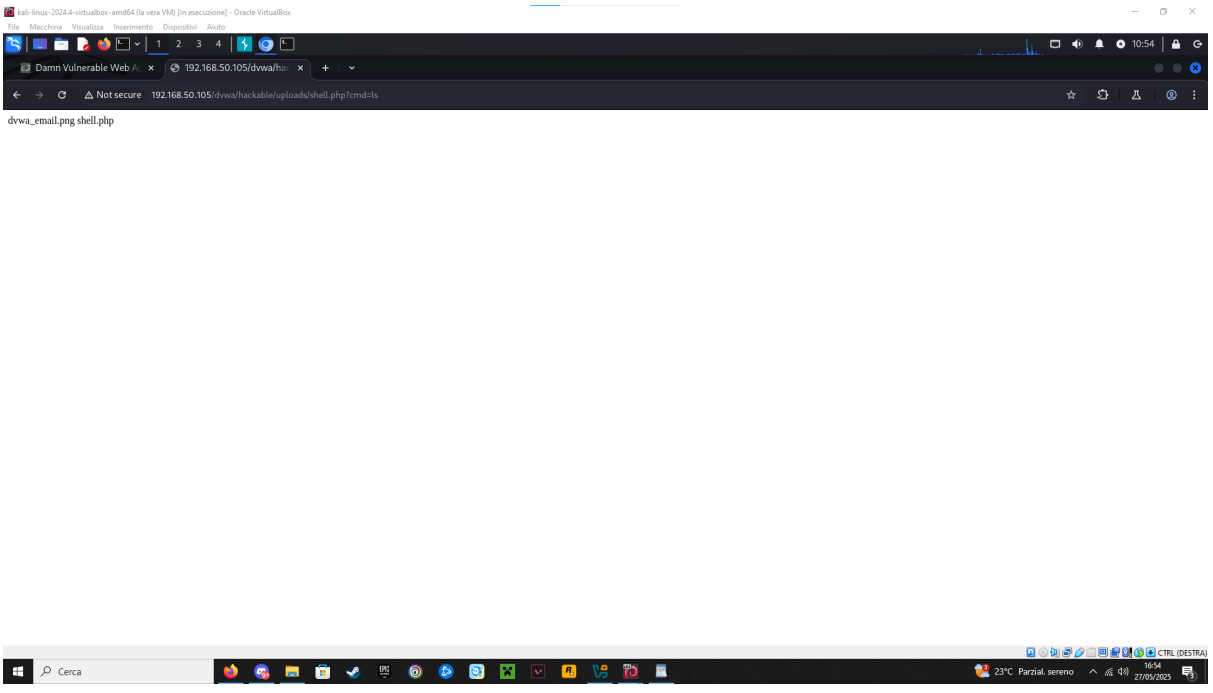
dopo aver messo il file shell.php , e cliccato su upload, noteremo su burpsuite che la richiesta per l'upload è come ci aspettavamo una richiesta POST



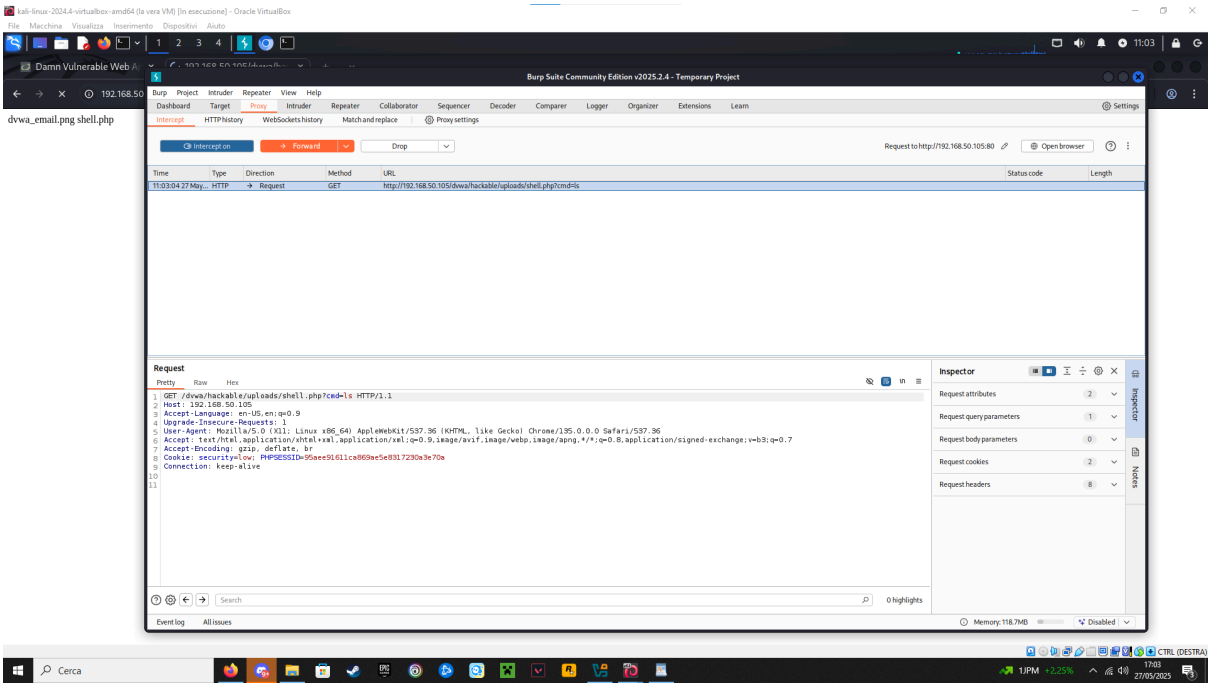
la shell è stata caricata a questo path



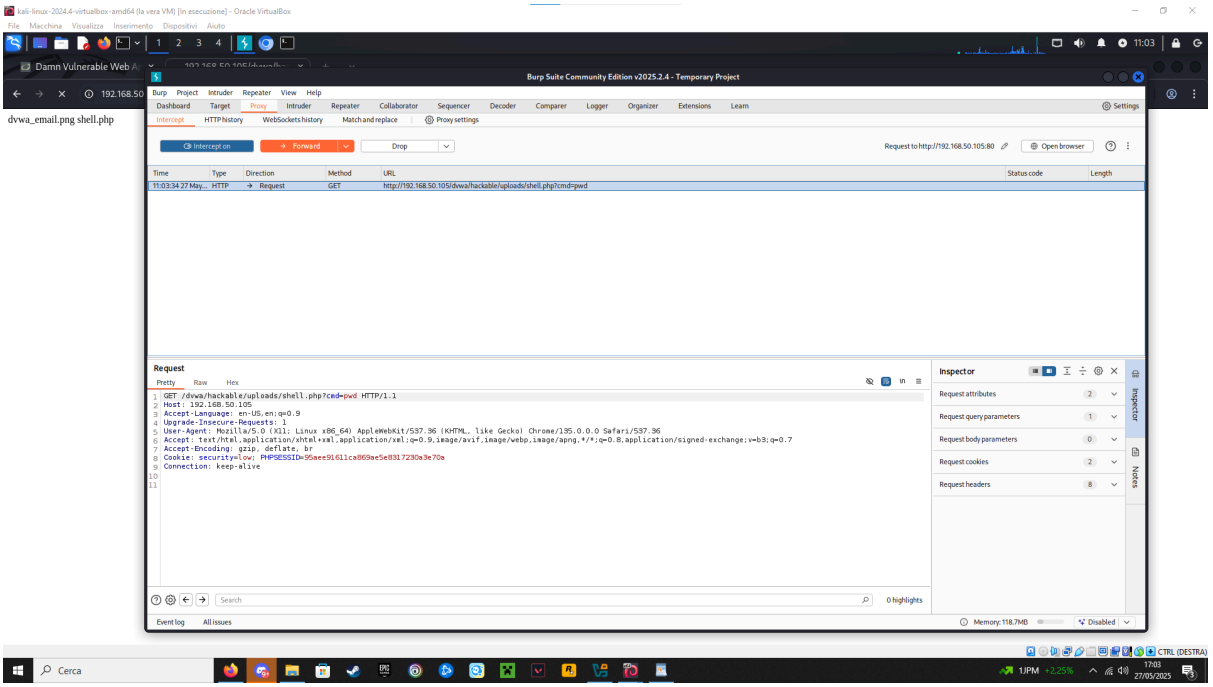
l’errore seguente è perchè aspetta un parametro cmd da eseguire

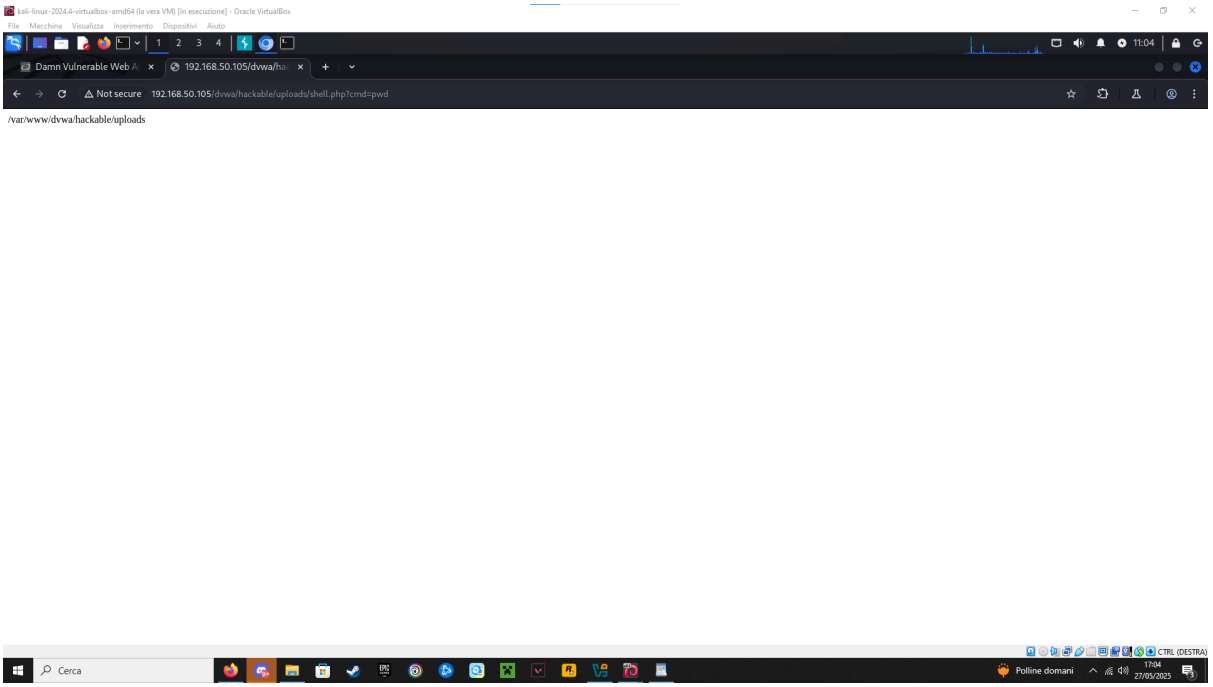


in questo caso ho usato “ls” e ci ha restituito la lista dei file e quindi la richiesta è stata eseguita dalla shell . cmd=ls viene passato come parametro da eseguire via GET.



Nella figura sotto proviamo a scrivere “pwd”





il risultato sarà questo

Il risultato sarà diverso se imposteremo la difficoltà su **medio o alto** non permettendoci cosi' facilmente di eseguire dei comandi tramite uno script php