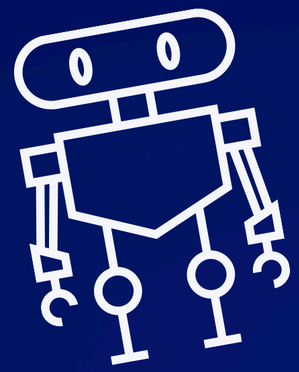
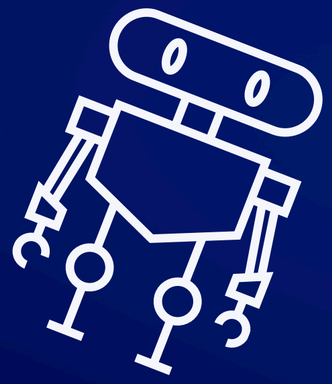
Exploit file upload

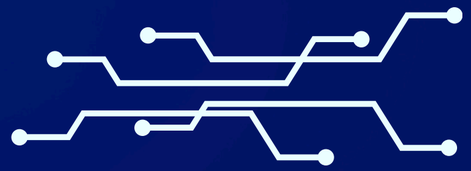
S6/L1





Mara Dello Russo

Traccia



Sfruttare la vulnerabilità di «file upload» presente sulla DVWA per prendere controllo della macchina ed eseguire dei comandi da remoto tramite una shell in PHP. Inoltre, per familiarizzare sempre di più con gli strumenti utilizzati dagli Hacker Etici, vi chiediamo di intercettare ed analizzare ogni richiesta verso la DVWA con BurpSuite.

GET DVWA

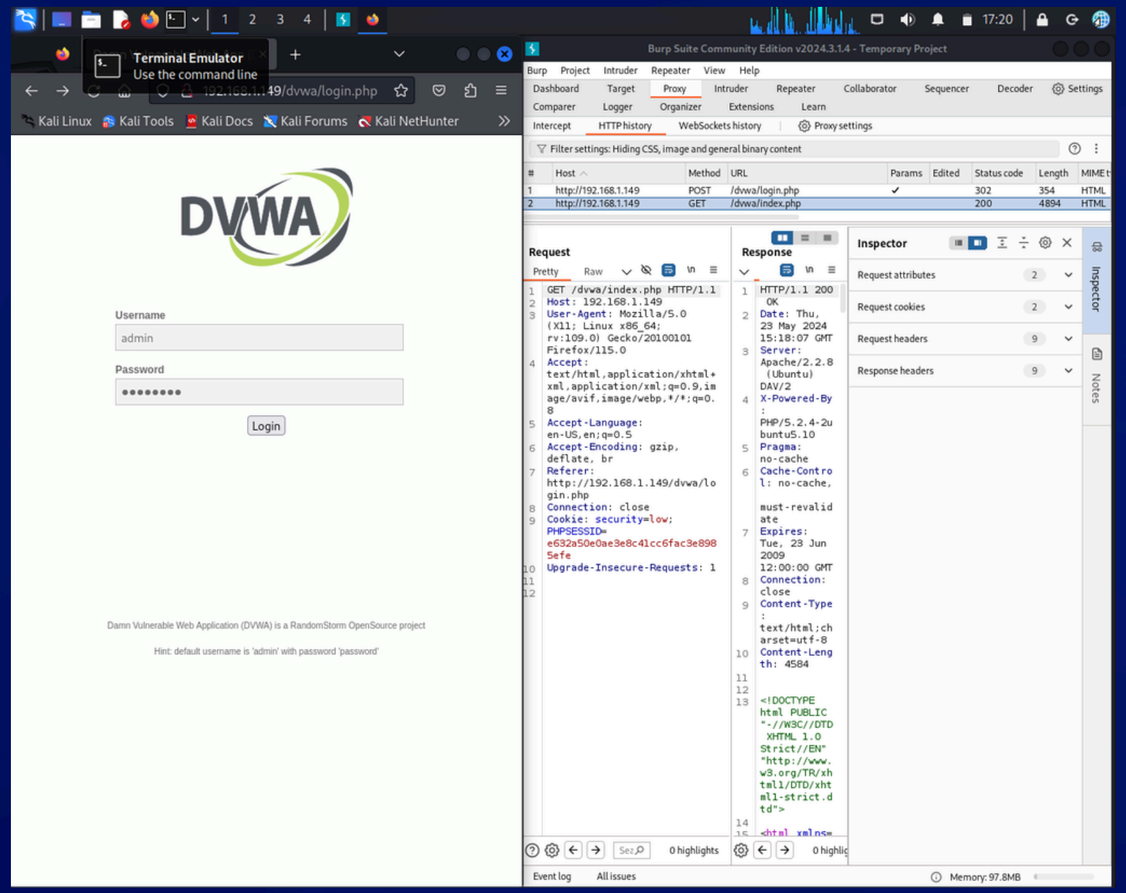
Dopo esserci assicurati che c’è connettività di rete tra la macchina kali (IP: 192.168.1.150) e la metasploitable (IP: 192.168.1.149) con un ping:

- Avviamo Burpsuite, proxy>intercept>intercept on

- Sul browser avviamo l’intercettazione con l’estensione proxyfoxy

- Carichiamo la pagina della DVWA al link http://192.168.1.149/dvwa/login.php

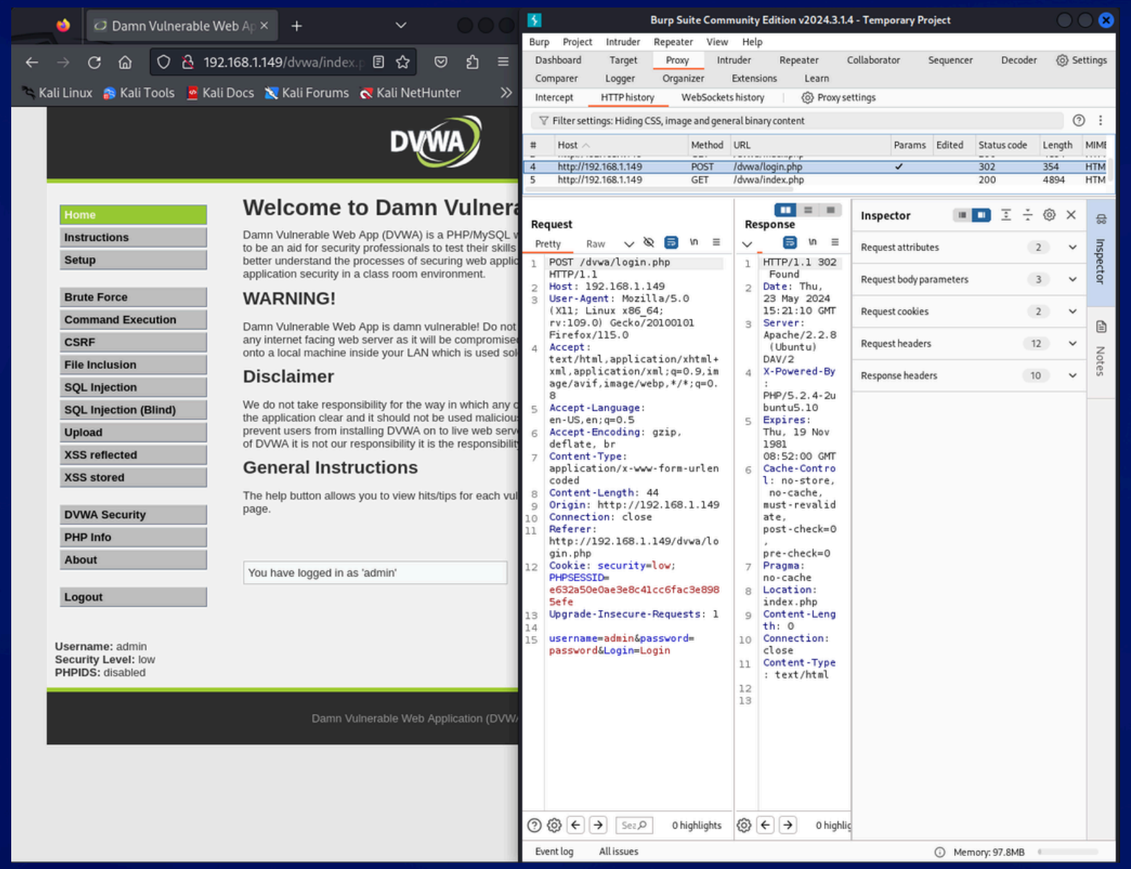
- Vediamo che il caricamento della pagina su burpsuite viene intercettato come richiesta GET



GET DVWA

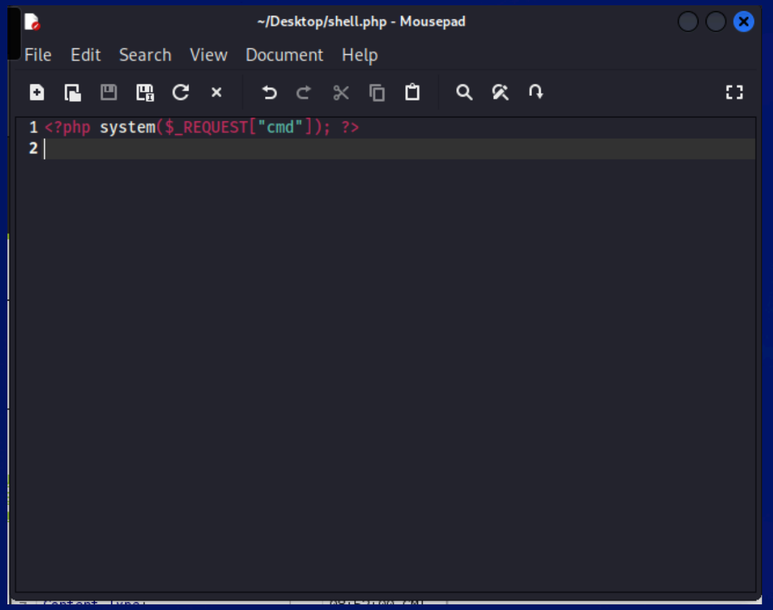
- Inseriamo le credenziali e clicchiamo su submit

- Su burpsuite notiamo come l'inserimento di username e password viene intercettato in una richiesta POST che contiene le credenziali da noi inserite.



SHELL.PHP

In un file di testo salviamo un semplice script della shell che dobbiamo caricare. Chiameremo il file “shell.php”.



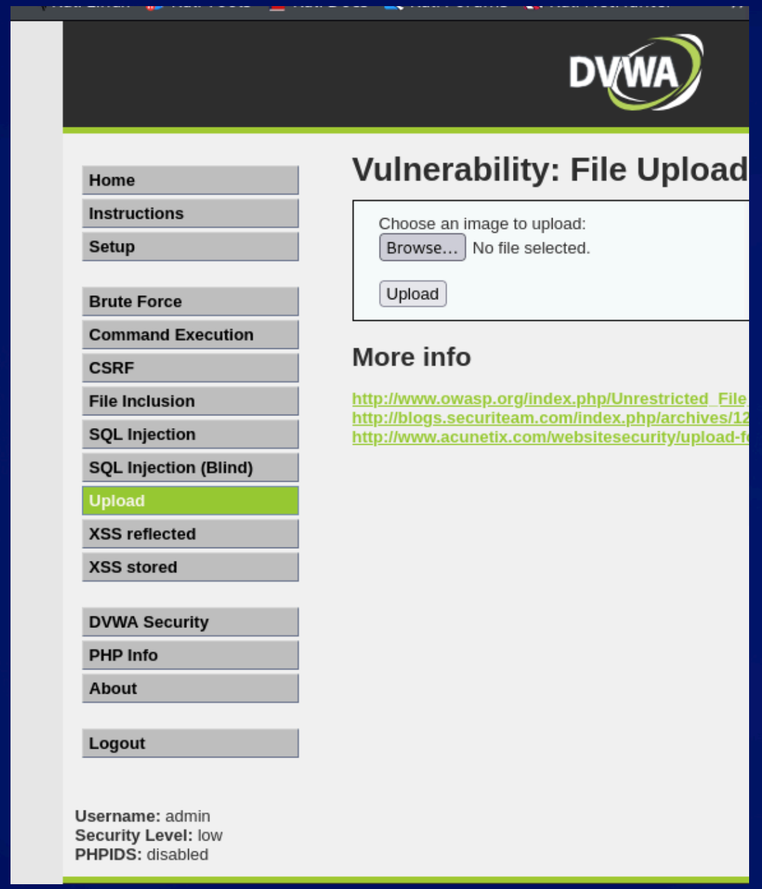
FILE UPLOAD

• Assicuriamoci che la DVWA Security sia impostata sul livello di sicurezza low.

• Andiamo nella sezione upload

• Cliccando su browser scegliamo il file shell.php precedentemente creato

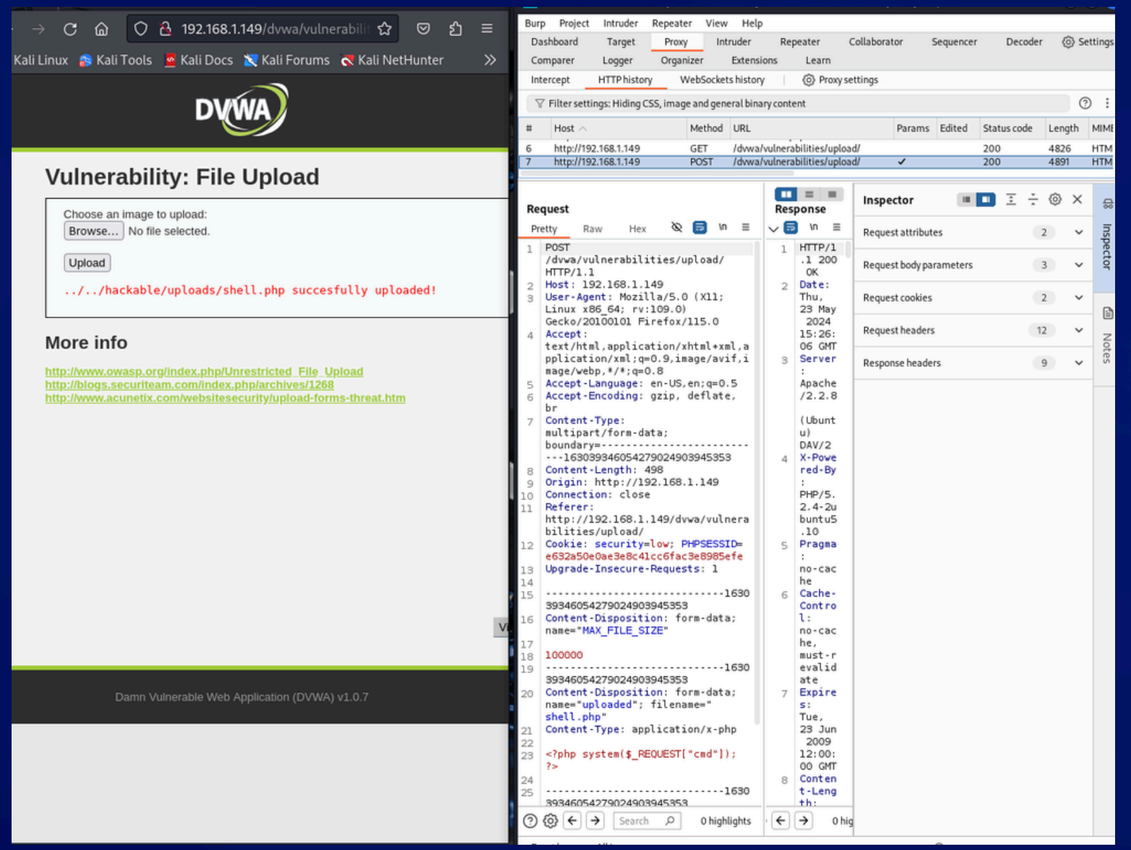
• Click su Upload



UPLOAD SHELL

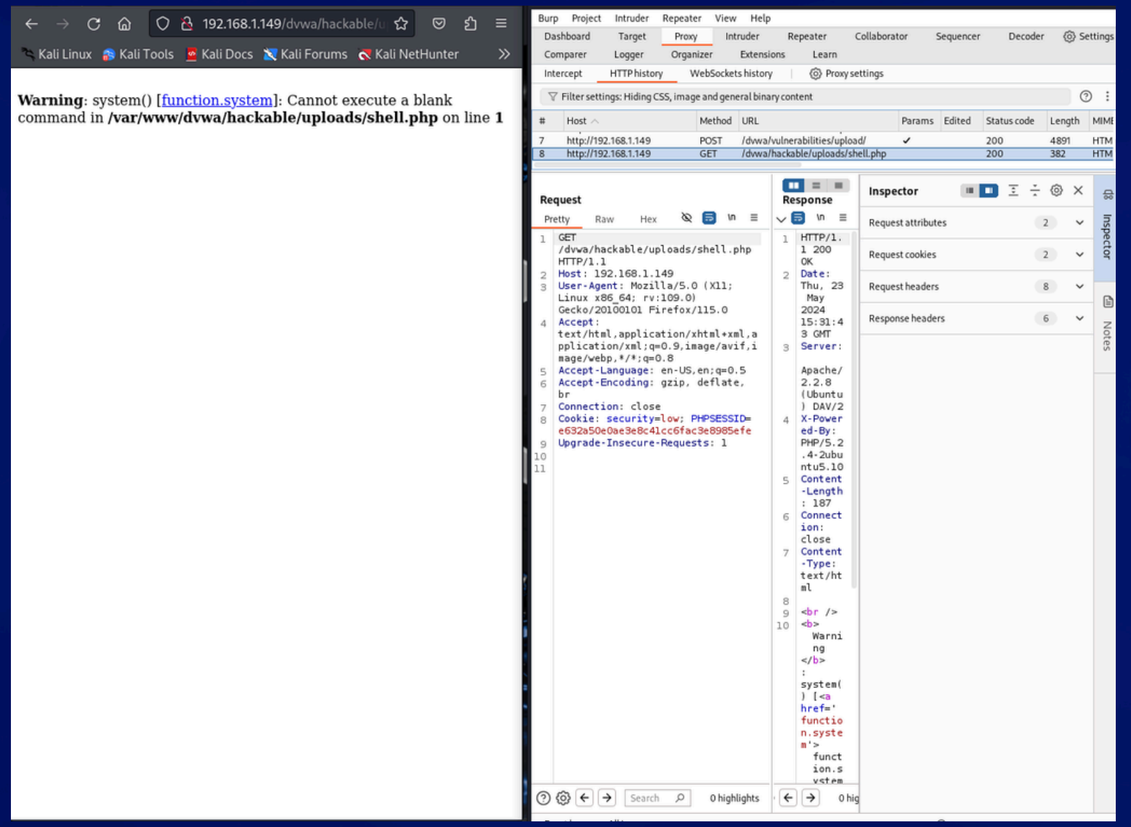
Dopo aver caricato la shell otteniamo il messaggio del caricamento avvenuto con successo (messaggio in rosso).

Da Burpsuite vediamo che la shell è stata caricata con una richiesta di POST.



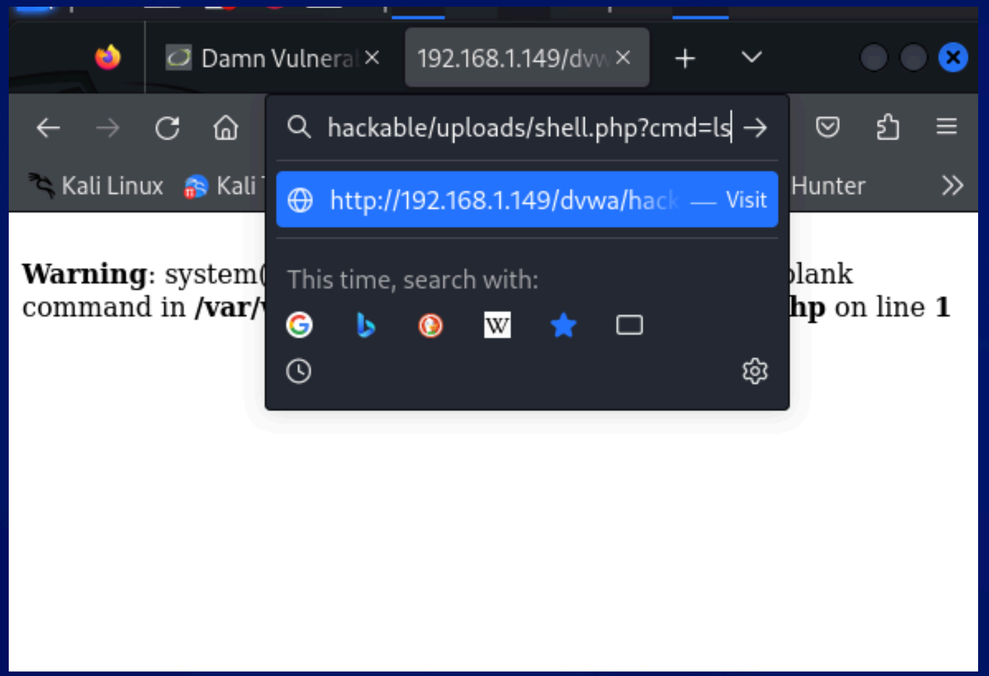
WARNING BLANK COMMAND

Collegandoci al path ottenuto prima nel messaggio in rosso riceveremo un messaggio di errore perché la shell si aspetta un parametro cmd con un comando da eseguire.



CMD in GET

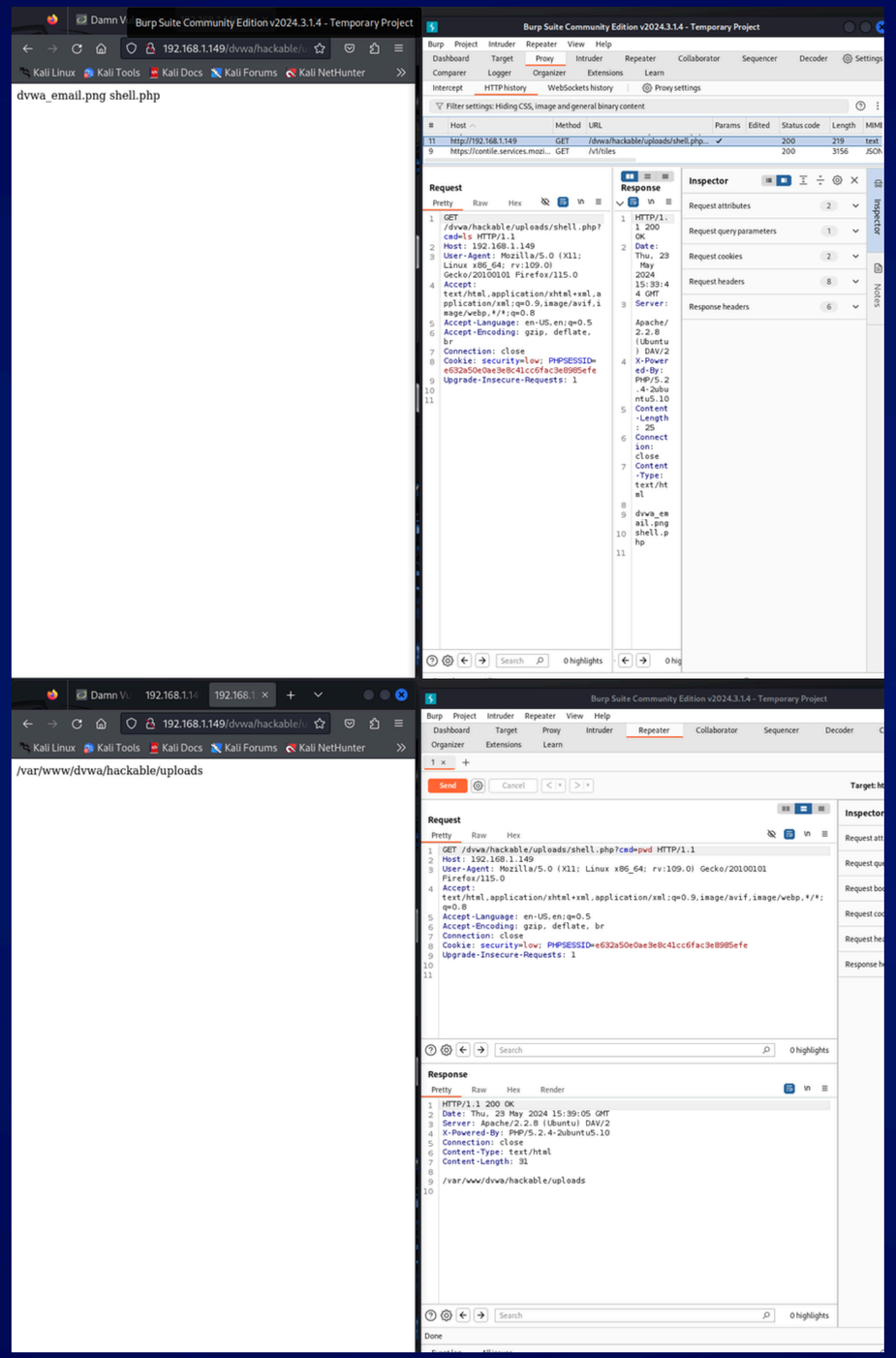
Inseriamo nella get il parametro cmd con il comando ls da eseguire e premiamo Enter



CMD in GET

Intercettiamo la richiesta GET con burpsuite dopo aver inserito il parametro cmd e inviamo, con il tasto destro del mouse, la richiesta al Repeater.

Dal Repeater modifichiamo il comando **ls** con **pwd** e clicchiamo su <send>.
Con tasto destro del mouse>show response in browser>copy copiamo il link della nuova richiesta get e incolliamolo nel browser. come risultato avremo una pagina web con il comando pwd eseguito dalla shell.



GRAZIE PER L'ATTENZIONE