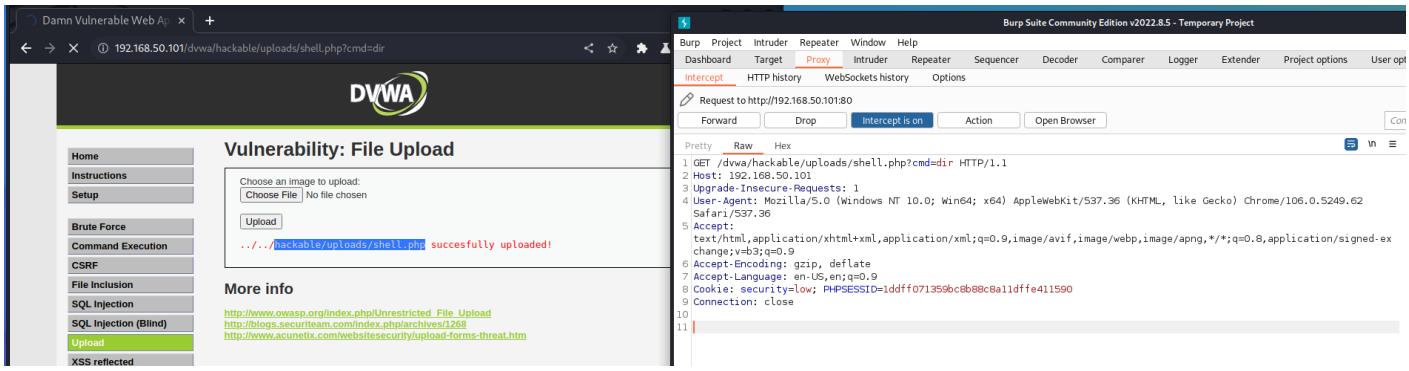
CUORE ANDREA

28-11-2022

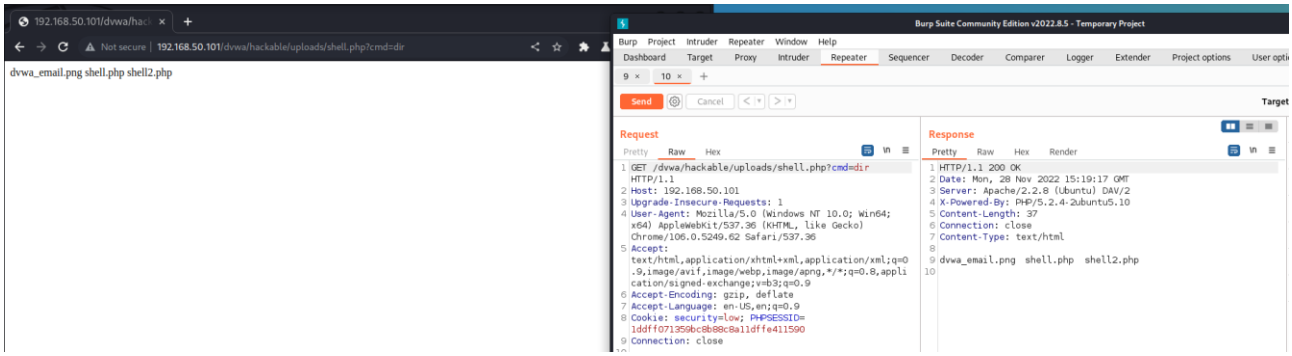
EXPLOIT SHELL PHP

SHELL PHP 1:

Nell’primo upload di codice malevolo ho seguito il codice fornito dalla traccia che ci permette di prendere il controllo della webshell

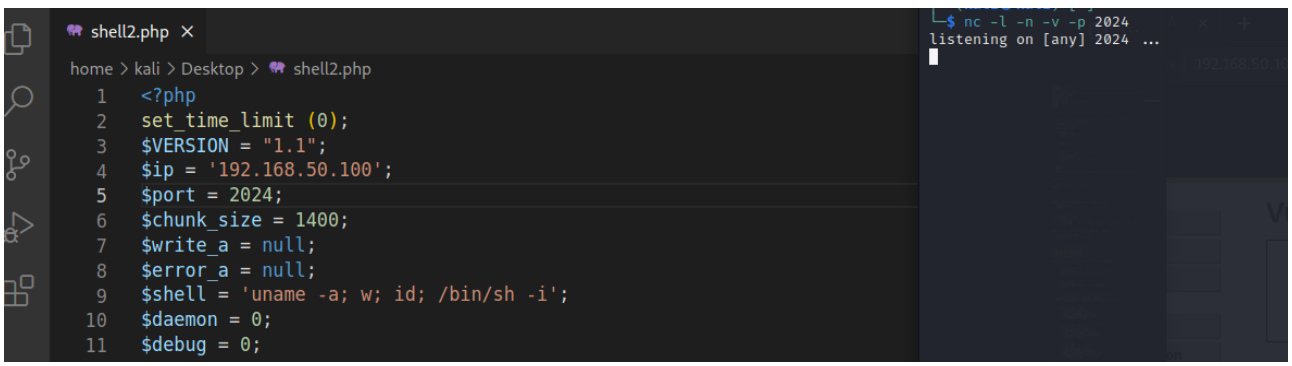


Questa è la parte dove vado a fare upload di codice malevolo in .php, e successivamente inserisco come URL il path con l’azione che voglio svolgere da cmd (ovver dir)

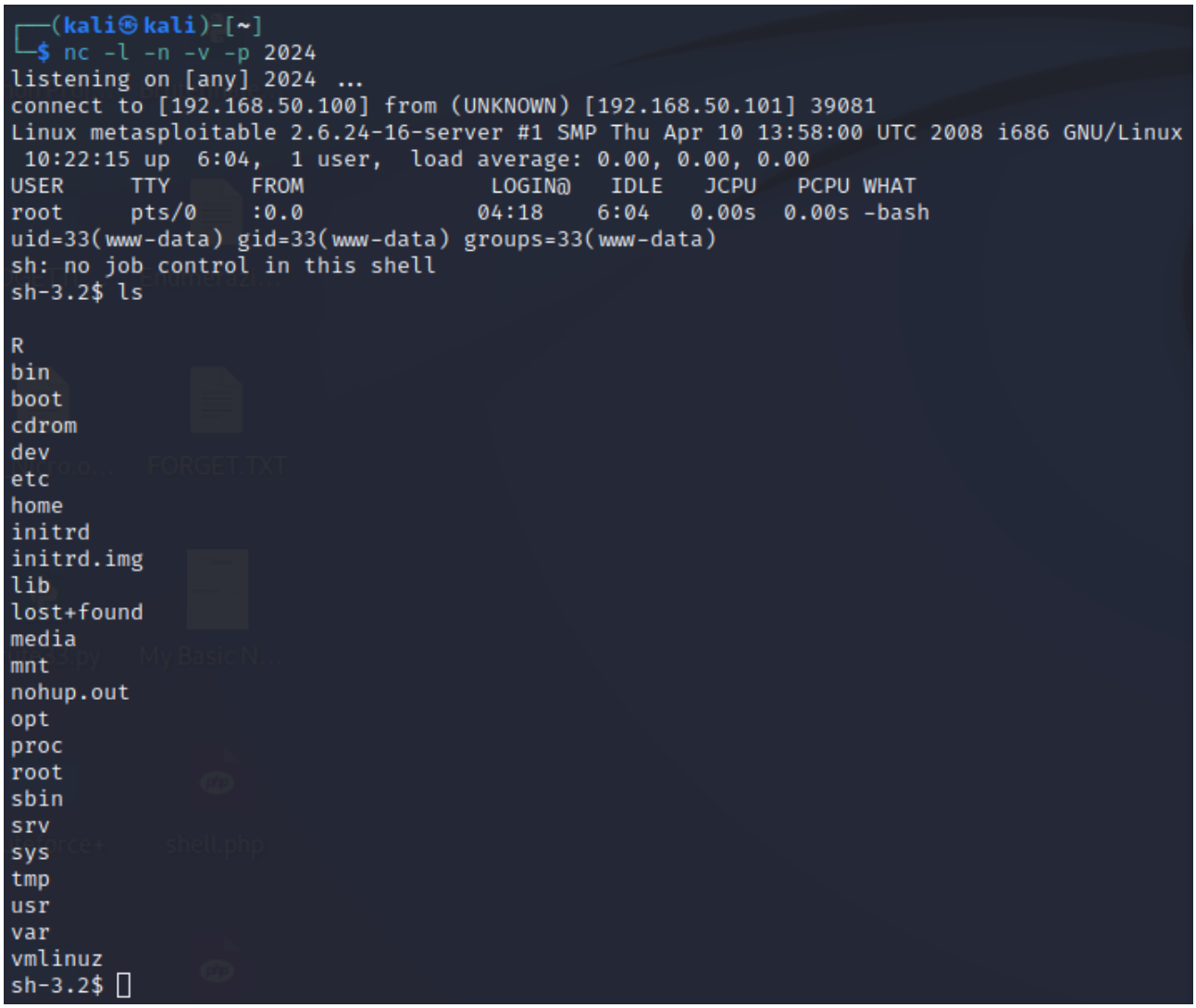


SHELL 2. REVERSE SHELL:

In questa parte ho deciso di andare oltre e fare upload di codice malevolo che mi instaura una connessione su una porta a nostra scelta, che sarà in ascolto su netcat



Qui metto netcat in ascolto sulla porta 2024 e configuro l’exploit per stabilire una connessione, inserendo indirizzo IP e porta in ascolto



Inserendo nell’url il path dell’upload del nostro file, le due macchine vanno in comunicazione e otteniamo l’accesso completo alla shell