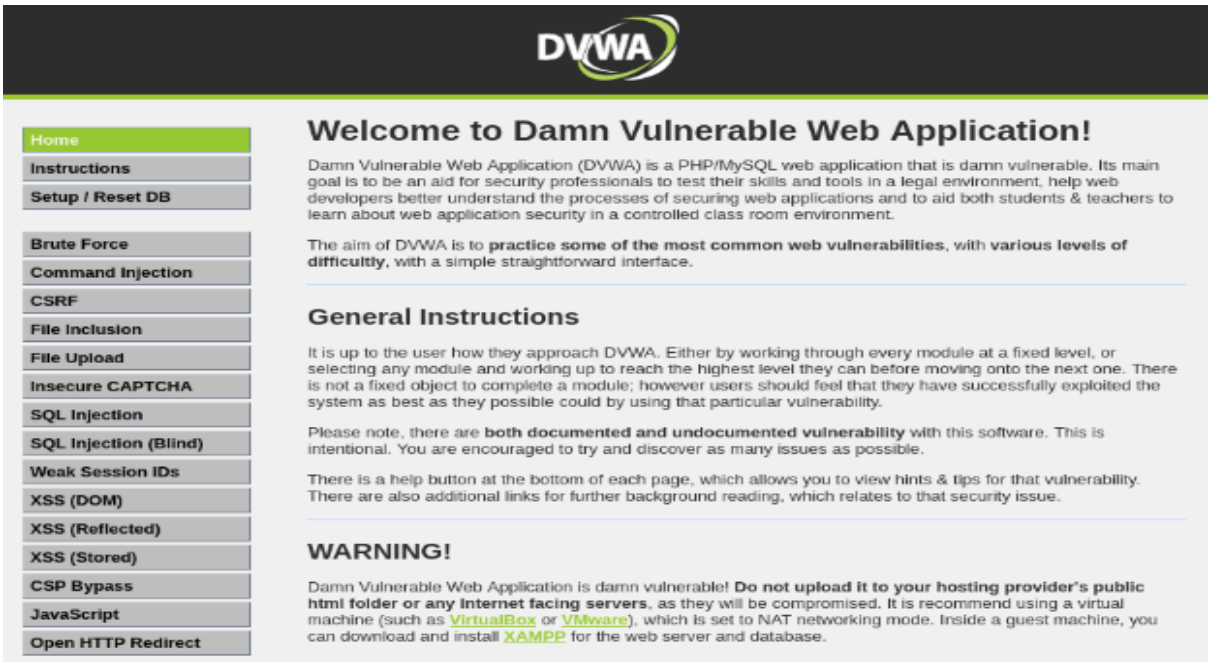
REPORT S3/L1

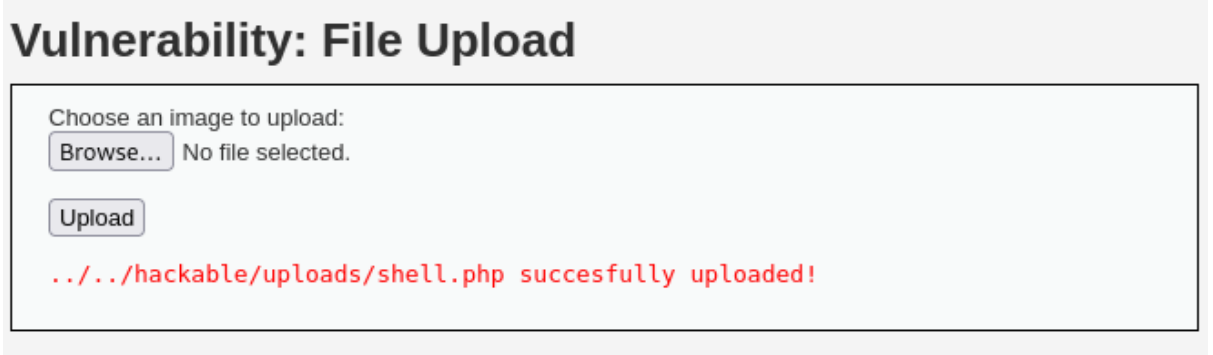
Obiettivo: Sfruttamento di una vulnerabilità di File Upload sulla DVWA per l'inserimento di una shell in PHP.

SVOLGIMENTO

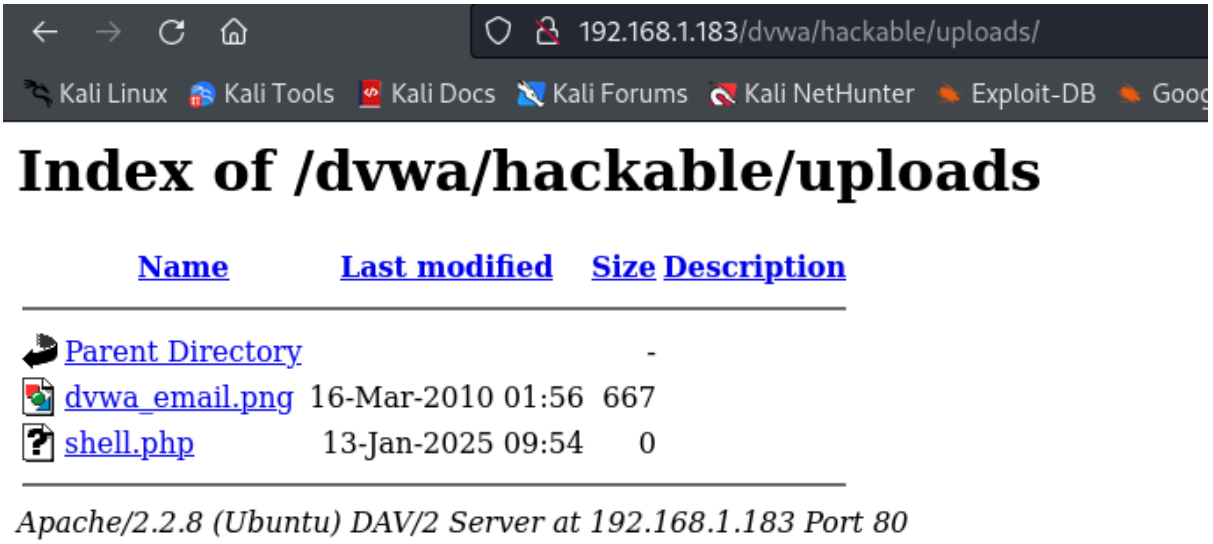
Dopo aver verificato la connessione tra le due macchine virtuali, Kali Linux e Metasploitable, ho proceduto ad accedere alla DVWA tramite il browser di Kali.



Ho realizzato un file shell.php e l'ho caricato nella sezione upload.



Successivamente, ho ottenuto l'accesso alla shell caricata attraverso il browser.



Infine ho utilizzato BurpSuite come proxy per intercettare le richieste HTTP/HTTPS effettuate durante il processo di upload e di esecuzione della shell.