Relazione Tecnica: Sfruttamento Vulnerabilità File Upload su DVWA

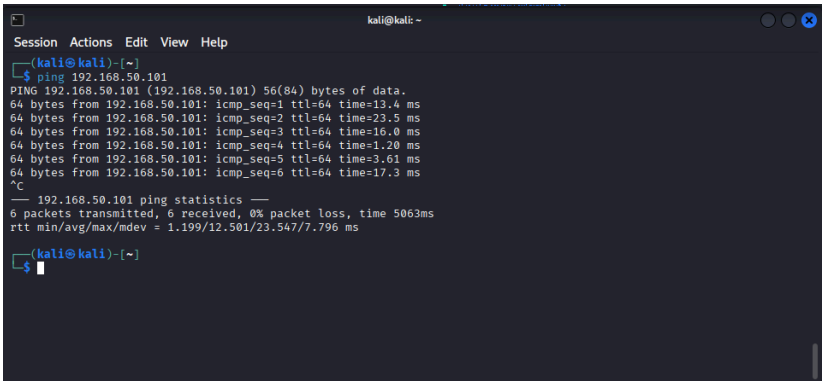
1. Introduzione e Obiettivi

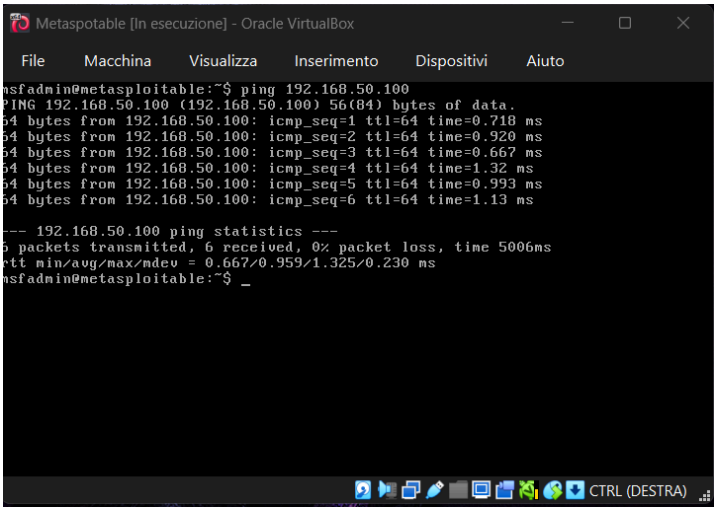
L'obiettivo dell'esercitazione è dimostrare come l'assenza di controlli adeguati nel caricamento di file possa permettere a un utente malintenzionato di ottenere il controllo remoto (Remote Code Execution) di un server. Per l'attività è stata utilizzata la piattaforma **Damn Vulnerable Web Application (DVWA)**.

2. Configurazione dell'Ambiente di Laboratorio

Prima di procedere con l'exploit, è stata configurata l'infrastruttura di rete per garantire la comunicazione tra la macchina attaccante e il bersaglio:

- **Macchina Attaccante:** Kali Linux (IP: `192.168.50.100`).
- **Macchina Bersaglio:** Metasploitable (IP: `192.168.50.101`).
- **Verifica Connettività:** È stato eseguito un test di `ping` bidirezionale per confermare la comunicazione tra i due sistemi.

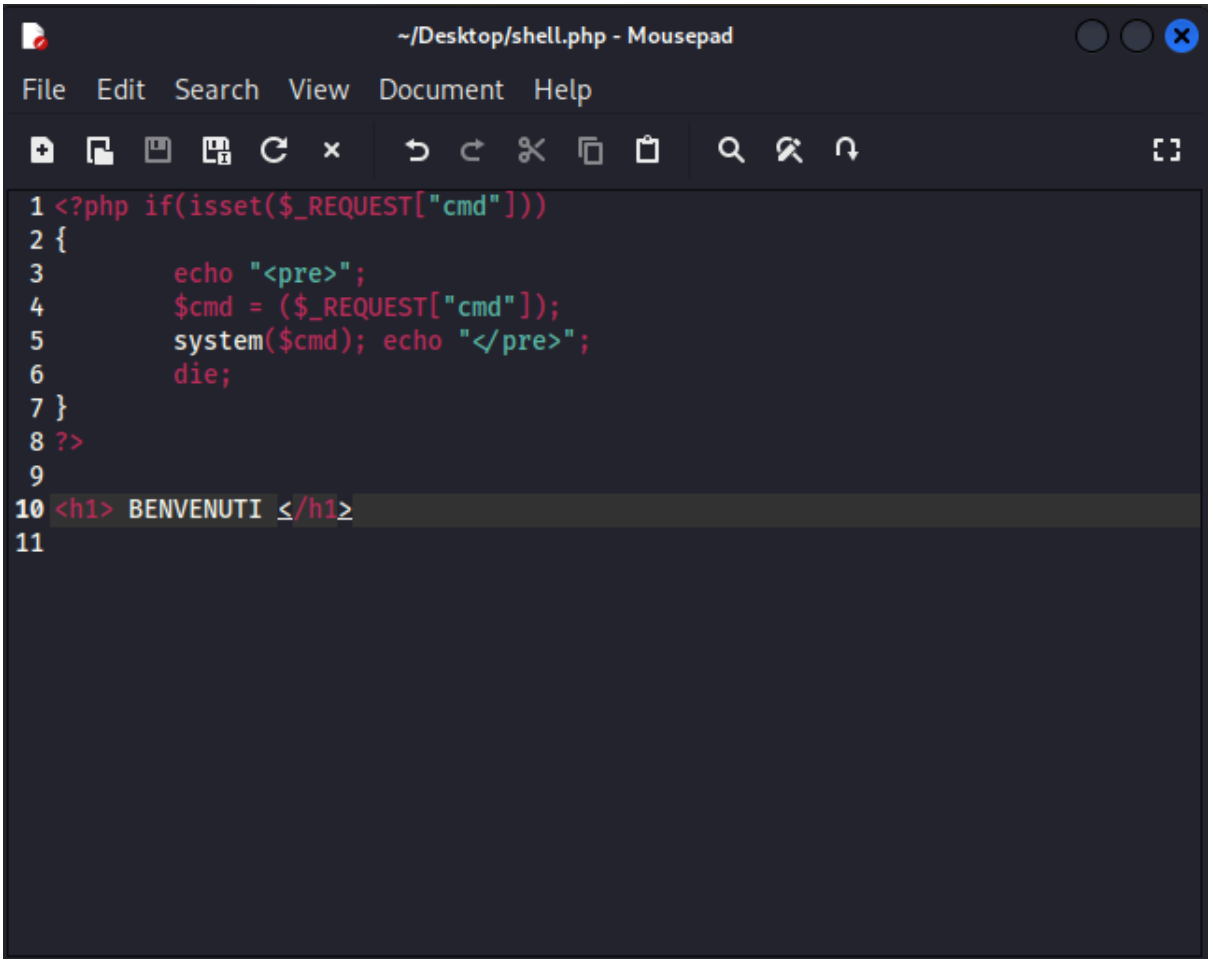




3. Preparazione della Shell PHP

Seguendo le indicazioni della traccia , è stata creata una shell PHP minimale denominata `shell.php`.

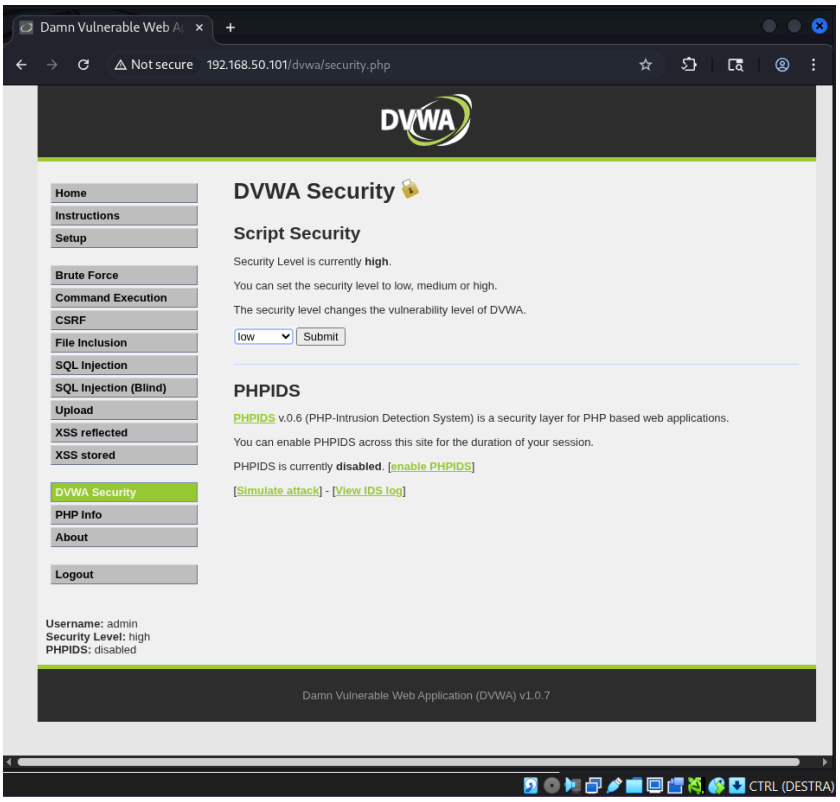
- **Codice della Shell:** Lo script utilizza la variabile `$_REQUEST` per catturare input tramite il parametro `cmd` ed eseguirlo sul sistema tramite la funzione `system()`.
- È stato aggiunto un tag `<h1>` con il testo "BENVENUTI" per facilitare la verifica visiva del caricamento.



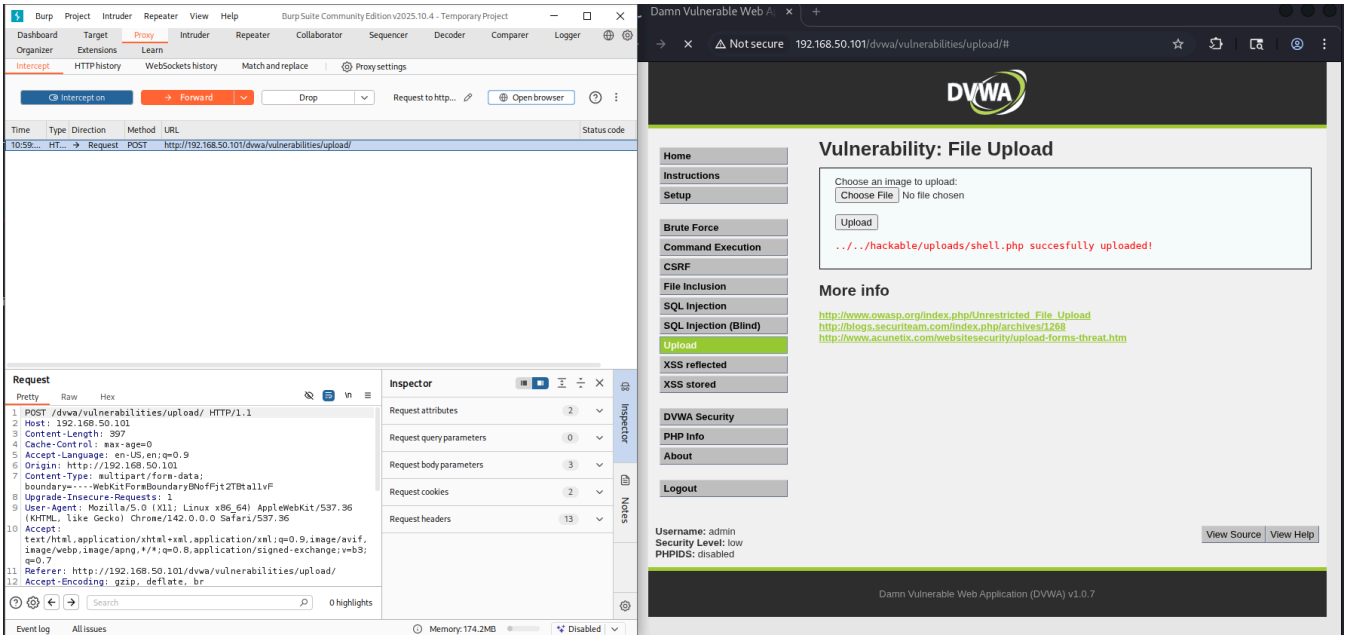
4. Esecuzione dell'Exploit (File Upload)

Per procedere con l'attacco, è stato necessario configurare correttamente l'applicazione:

1. **Livello di Sicurezza:** Il "Security Level" di DVWA è stato impostato su **LOW** per consentire il caricamento del file senza restrizioni lato server.



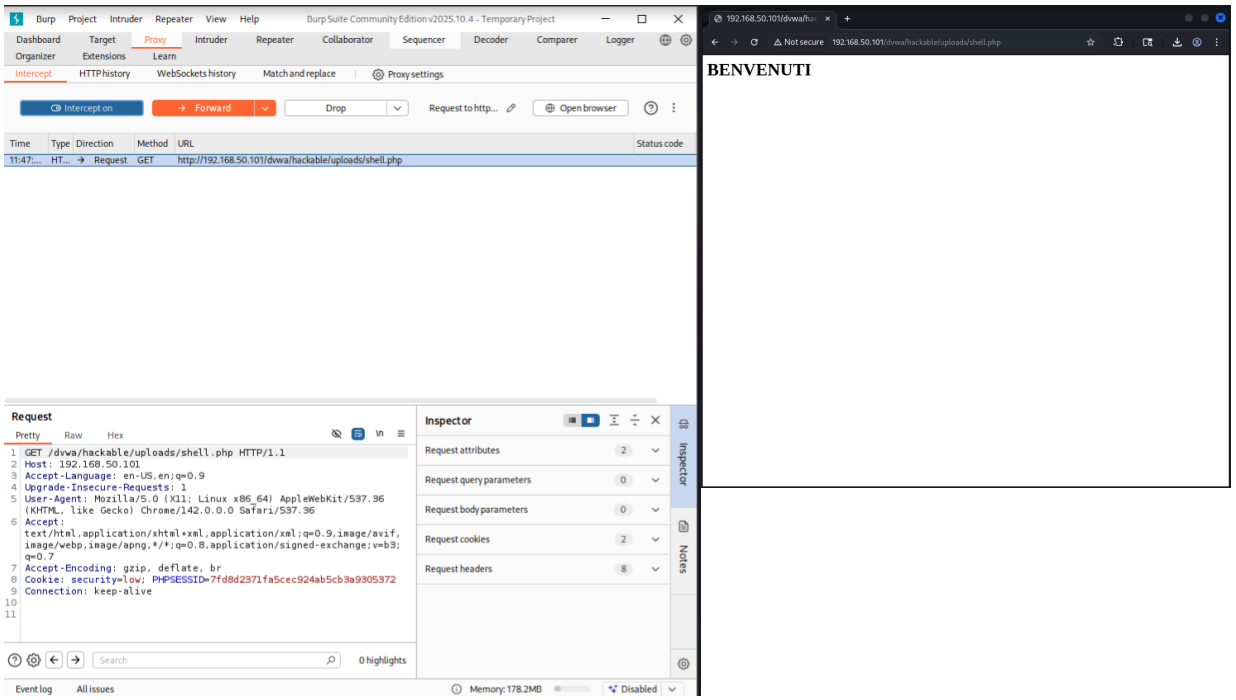
2. **Upload:** È stato utilizzato il modulo presente nella sezione "File Upload" per caricare il file `shell.php`.
3. **Conferma:** L'applicazione ha confermato il corretto caricamento indicando il percorso relativo del file: `../../hackable/uploads/shell.php`.



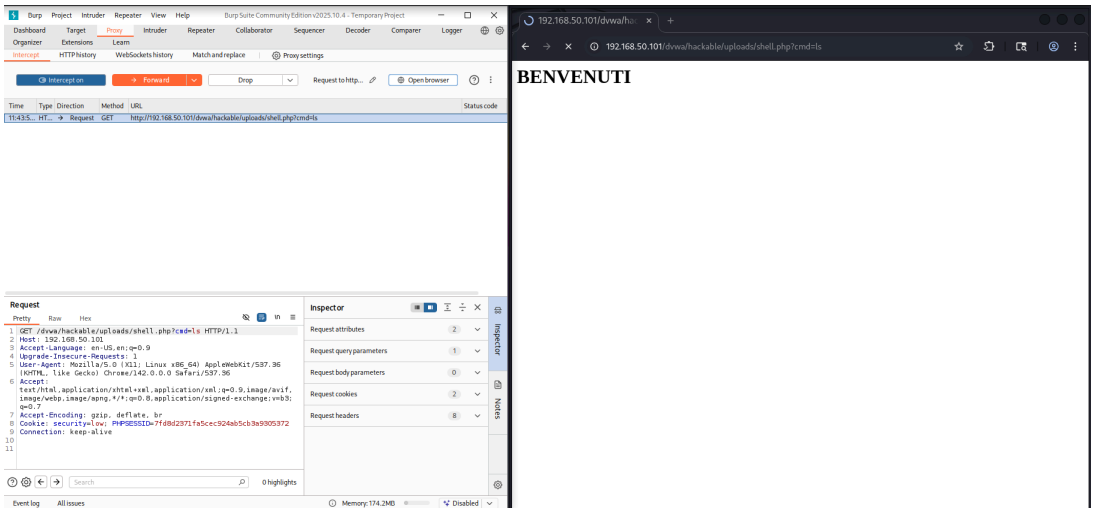
5. Esecuzione Remota di Comandi (RCE)

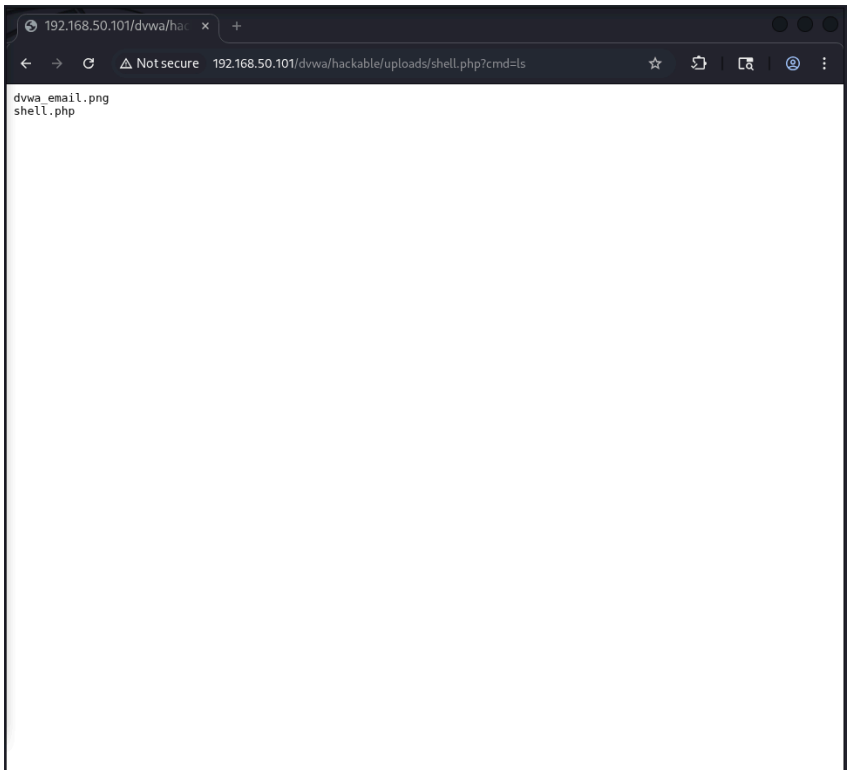
Una volta caricata, la shell è stata richiamata tramite il browser per interagire con il sistema operativo della Metasploitable.

- **Accesso Iniziale:** Navigando all'URL della shell, il server ha restituito la stringa "BENVENUTI".



- **Esecuzione Comando:** È stato inviato il comando `ls` tramite il parametro GET (`?cmd=ls`).
- **Risultato:** Il server ha risposto elencando i file presenti nella cartella di upload, tra cui `dvwa_email.png` e la stessa `shell.php`, confermando l'avvenuta Remote Code Execution.





6. Analisi con BurpSuite

Durante tutto il processo, BurpSuite è stato utilizzato come proxy per intercettare e analizzare il traffico HTTP.

- È stata analizzata la struttura delle richieste `POST` (per l'upload) e `GET` (per l'esecuzione).
- L'analisi ha confermato che i parametri vengono passati correttamente nel campo URL per i comandi shell.