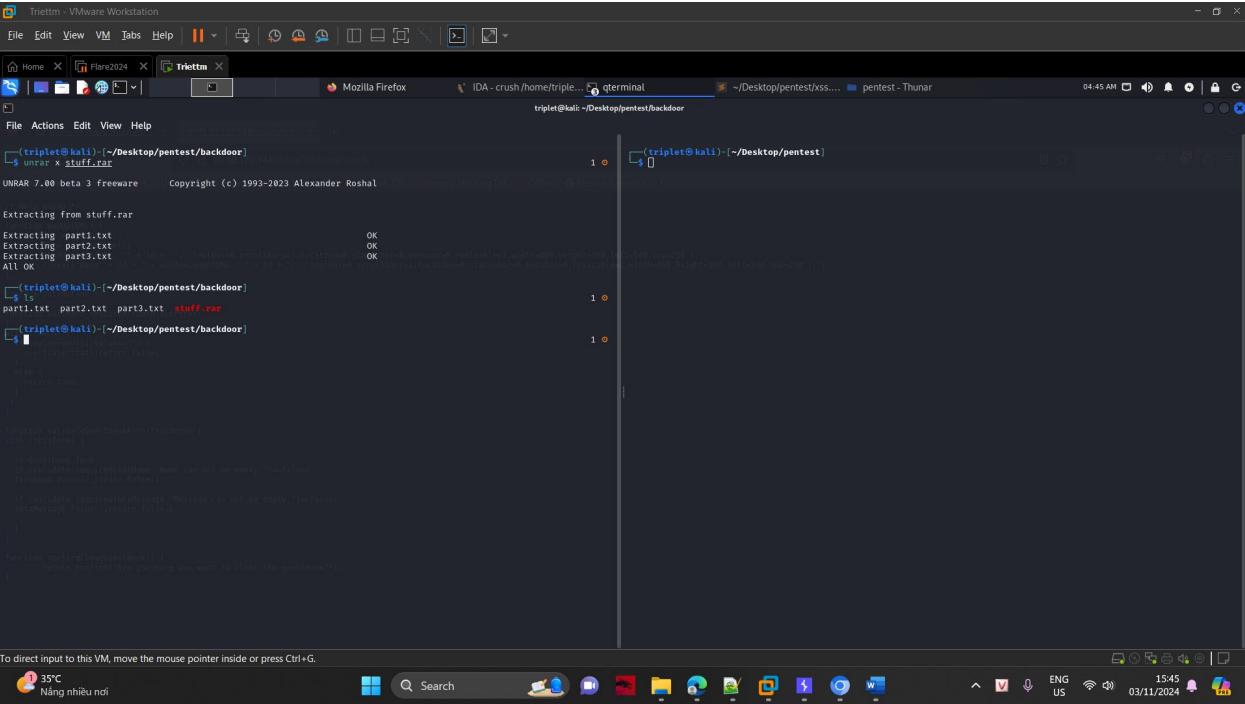
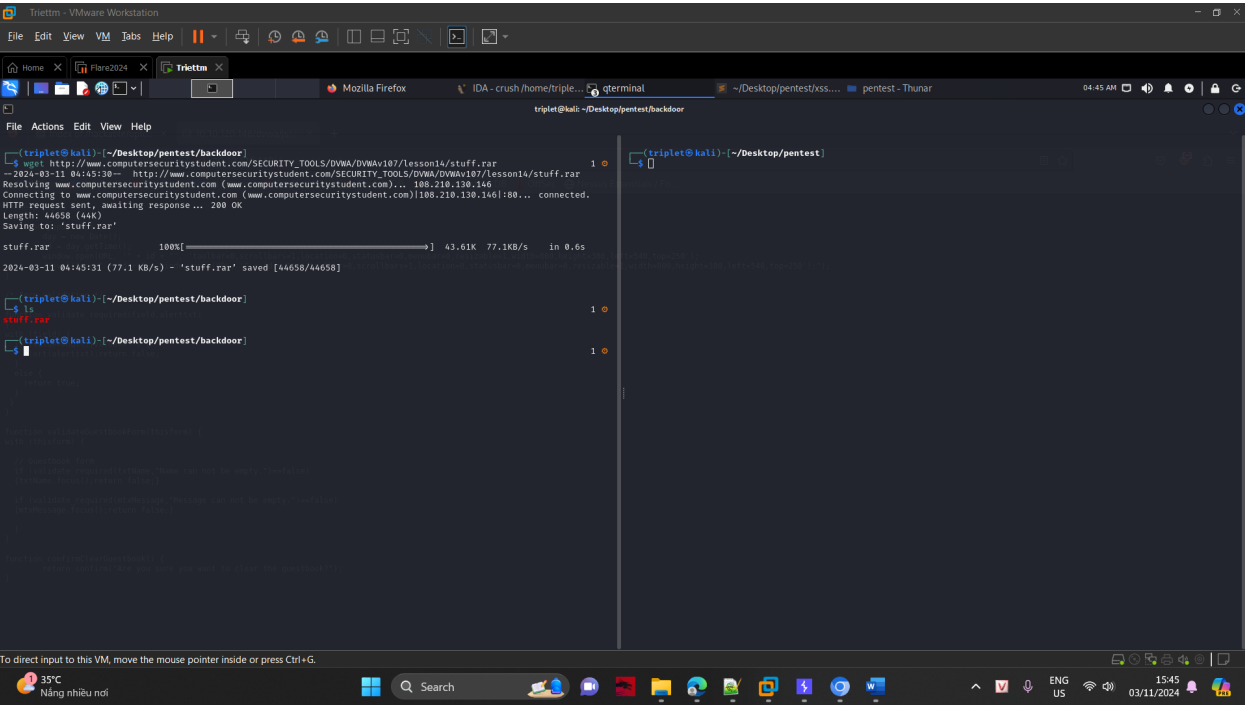


Lab 14: Upload and use C99.php Backdoor shell	
Name	Tran Minh Triet
Student ID	SE172241

Download c99:php



```
Trietm - VMware Workstation
File Edit View VM Tabs Help
Home X Flare2024 X Trietm X
Mozilla Firefox IDA - crush/home/triple... qterminal ~/Desktop/pentest/xss.... pentest - Thunar 04:46 AM
triplet@kali: ~/Desktop/pentest/backdoor

(triplet@kali)~/Desktop/pentest/backdoor
$ cat part1.txt part2.txt part3.txt > c99.php

(triplet@kali)~/Desktop/pentest/backdoor
$ cp c99.php c99.php.bkp

(triplet@kali)~/Desktop/pentest/backdoor
$ ls -l
total 504
-rw-r--r-- 1 triplet triplet 43822 Dec 23 2015 part1.txt
-rw-r--r-- 1 triplet triplet 56829 Dec 23 2015 part2.txt
-rw-r--r-- 1 triplet triplet 53424 Dec 23 2015 part3.txt
-rw-r--r-- 1 triplet triplet 44658 Dec 23 2015 stuff.rar
-rw-r--r-- 1 triplet triplet 153275 Mar 11 04:46 c99.php
-rw-r--r-- 1 triplet triplet 153275 Mar 11 04:46 c99.php.bkp

(triplet@kali)~/Desktop/pentest/backdoor
$ cat
cat: c99.php: No such file or directory
cat: c99.php.bkp: No such file or directory

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
```

```
Trietm - VMware Workstation
File Edit View VM Tabs Help
Home X Flare2024 X Trietm X
Mozilla Firefox IDA - crush/home/triple... qterminal ~/Desktop/pentest/xss.... pentest - Thunar 04:47 AM
triplet@kali: ~/Desktop/pentest/backdoor

(triplet@kali)~/Desktop/pentest/backdoor
$ head -1 c99.php
<?

(triplet@kali)~/Desktop/pentest/backdoor
$ sed -i '1 s/?.*</php/g' c99.php

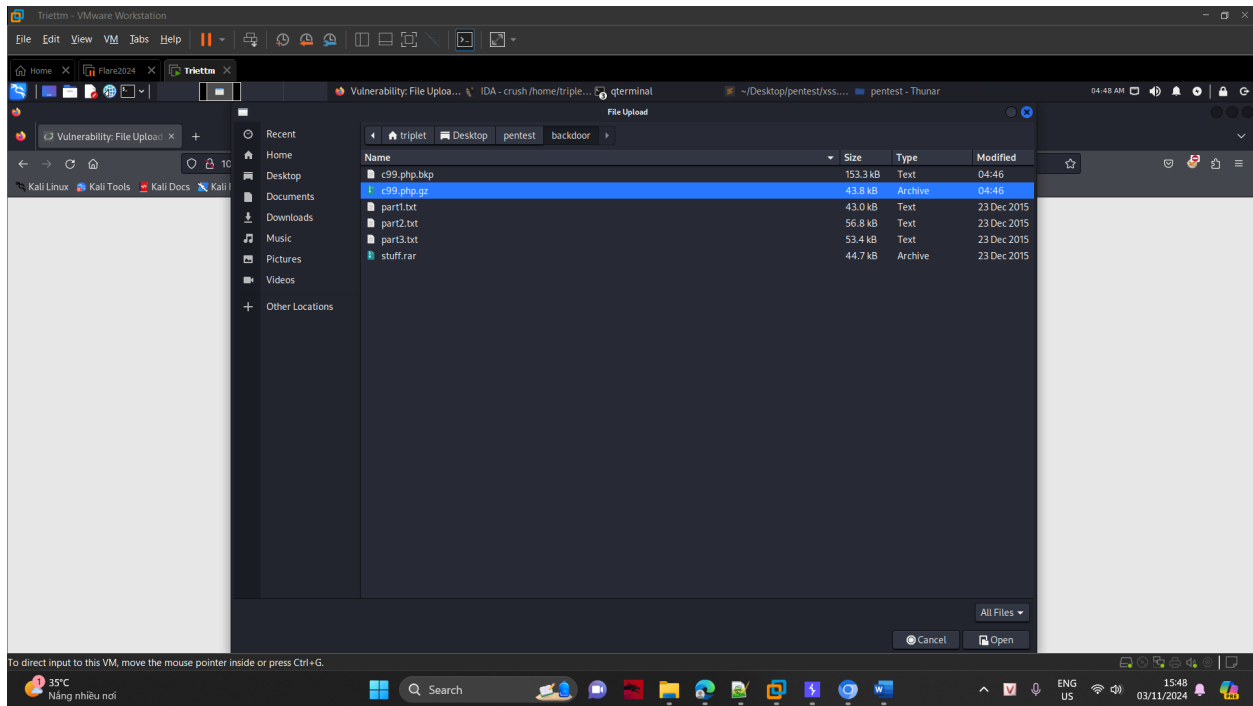
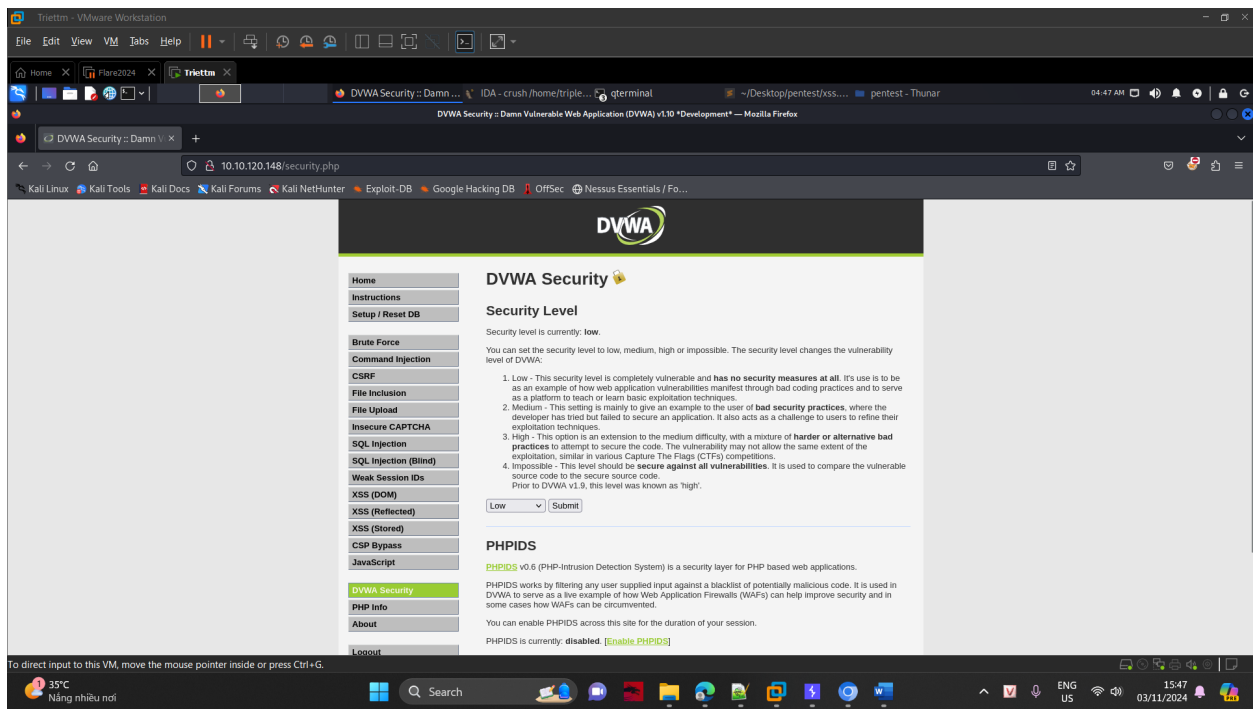
(triplet@kali)~/Desktop/pentest/backdoor
$ head -1 c99.php
<?php

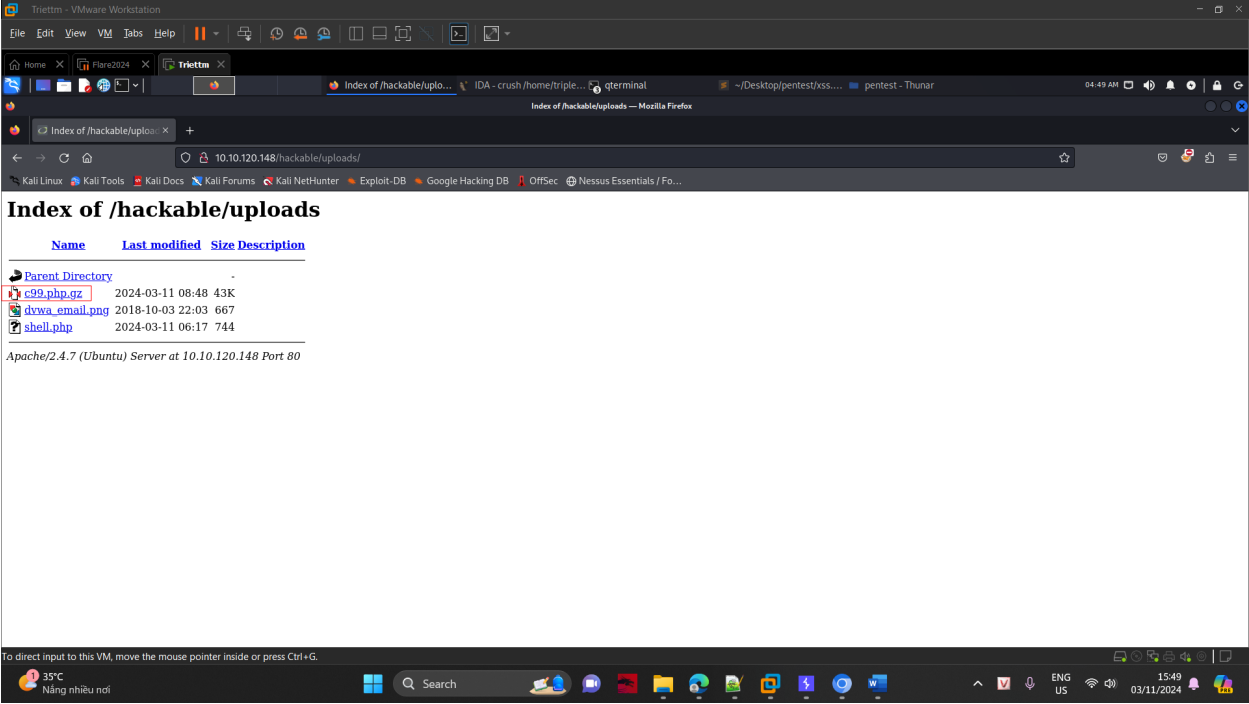
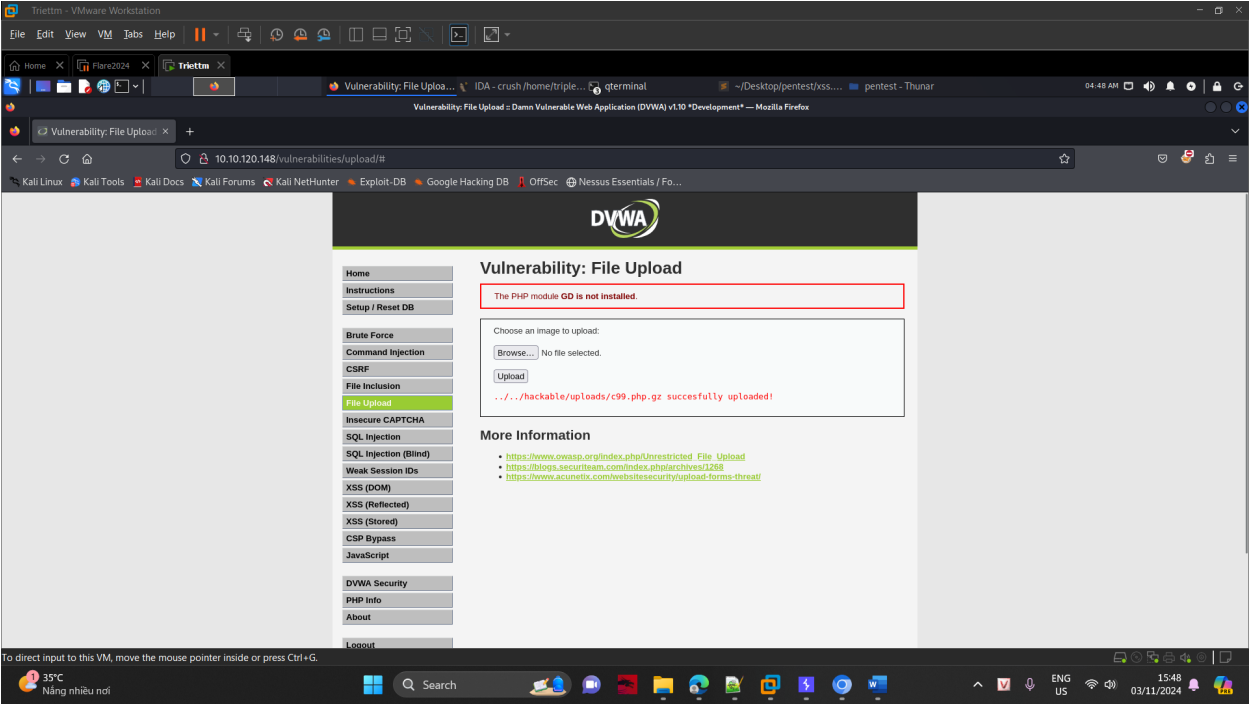
(triplet@kali)~/Desktop/pentest/backdoor
$ gzip c99.php

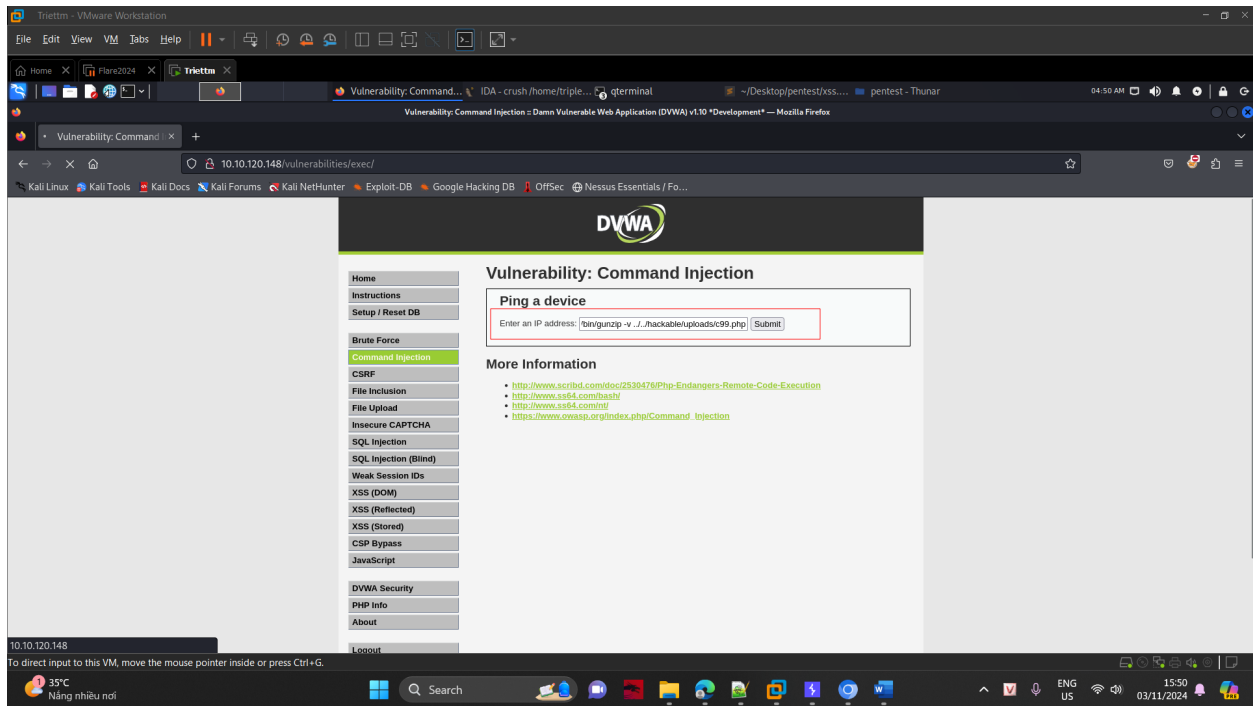
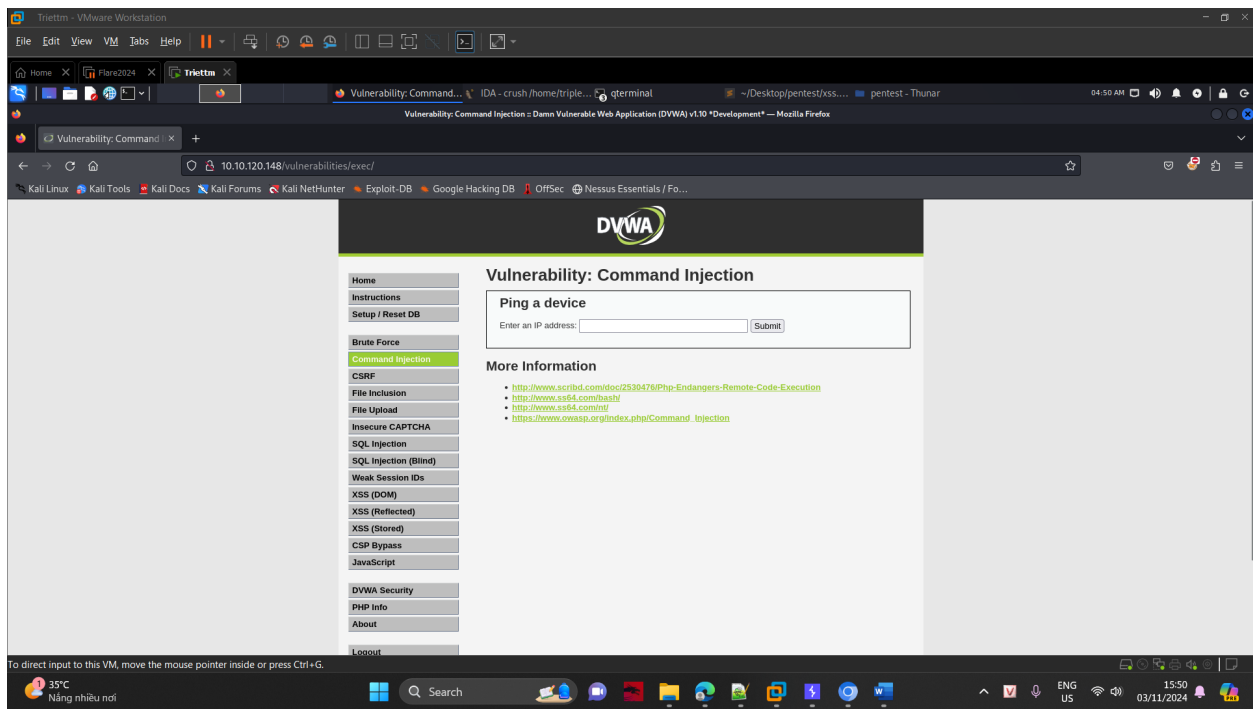
(triplet@kali)~/Desktop/pentest/backdoor
$ ls -l
total 396
-rw-r--r-- 1 triplet triplet 153275 Mar 11 04:46 c99.php.bkp
-rw-r--r-- 1 triplet triplet 43786 Mar 11 04:46 c99.php.gz
-rw-r--r-- 1 triplet triplet 43822 Dec 23 2015 part1.txt
-rw-r--r-- 1 triplet triplet 56829 Dec 23 2015 part2.txt
-rw-r--r-- 1 triplet triplet 53424 Dec 23 2015 part3.txt
-rw-r--r-- 1 triplet triplet 44658 Dec 23 2015 stuff.rar

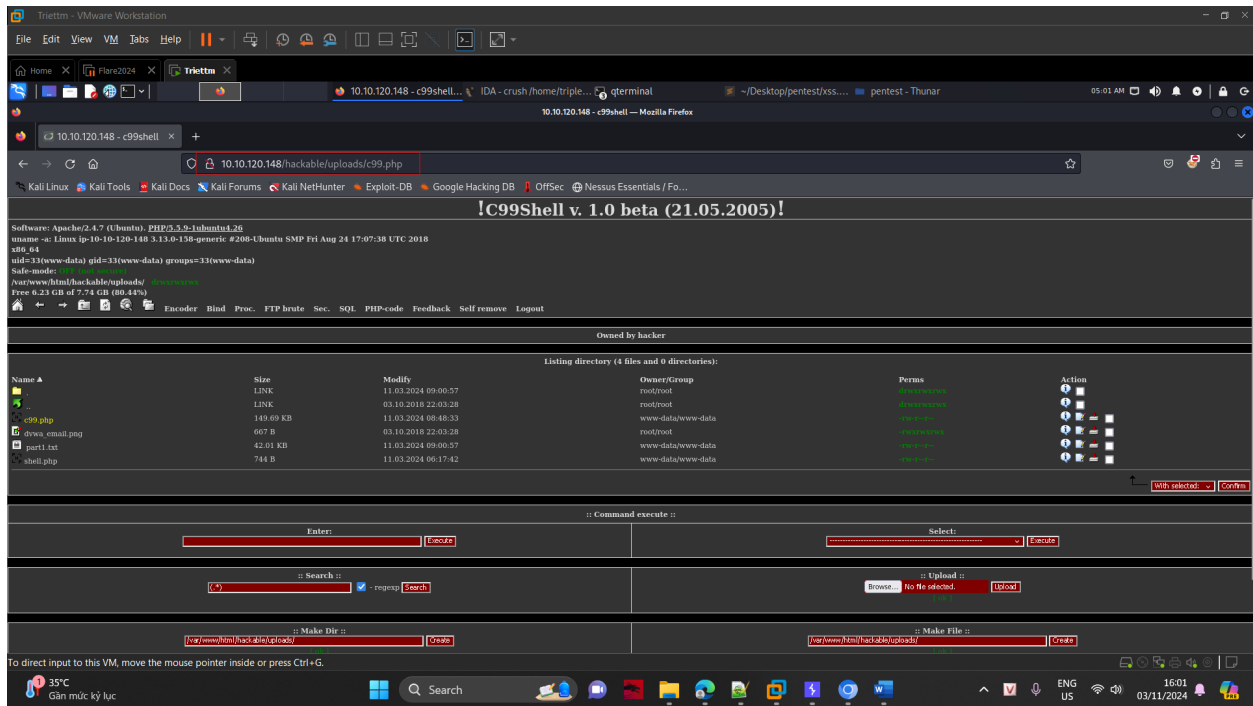
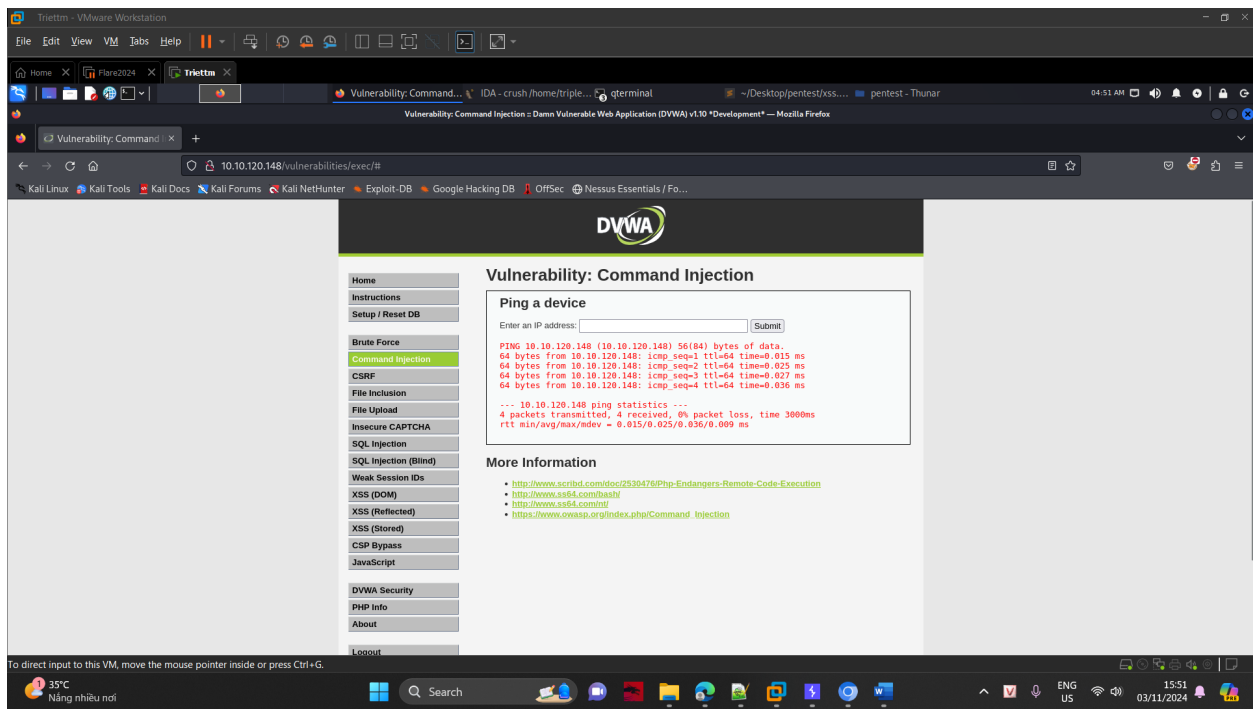
(triplet@kali)~/Desktop/pentest/backdoor
$ cat
cat: c99.php: No such file or directory
cat: c99.php.bkp: No such file or directory
cat: c99.php.gz: No such file or directory
cat: stuff.rar: No such file or directory

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
```

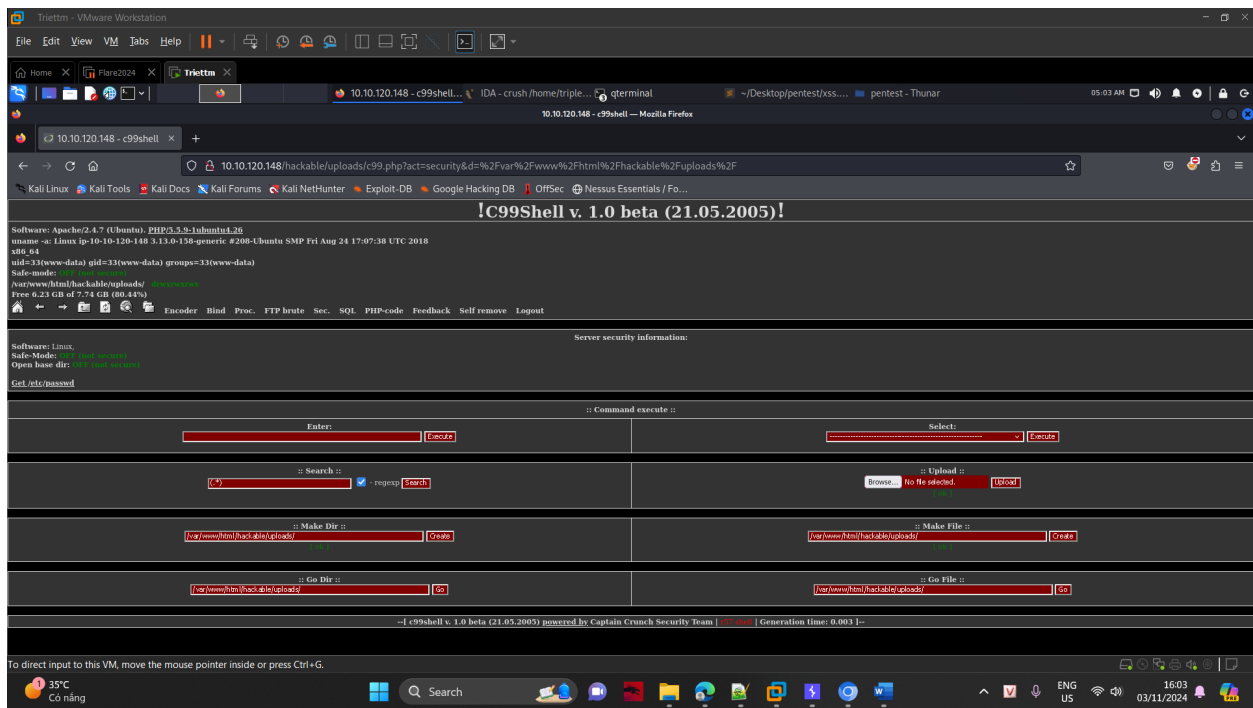
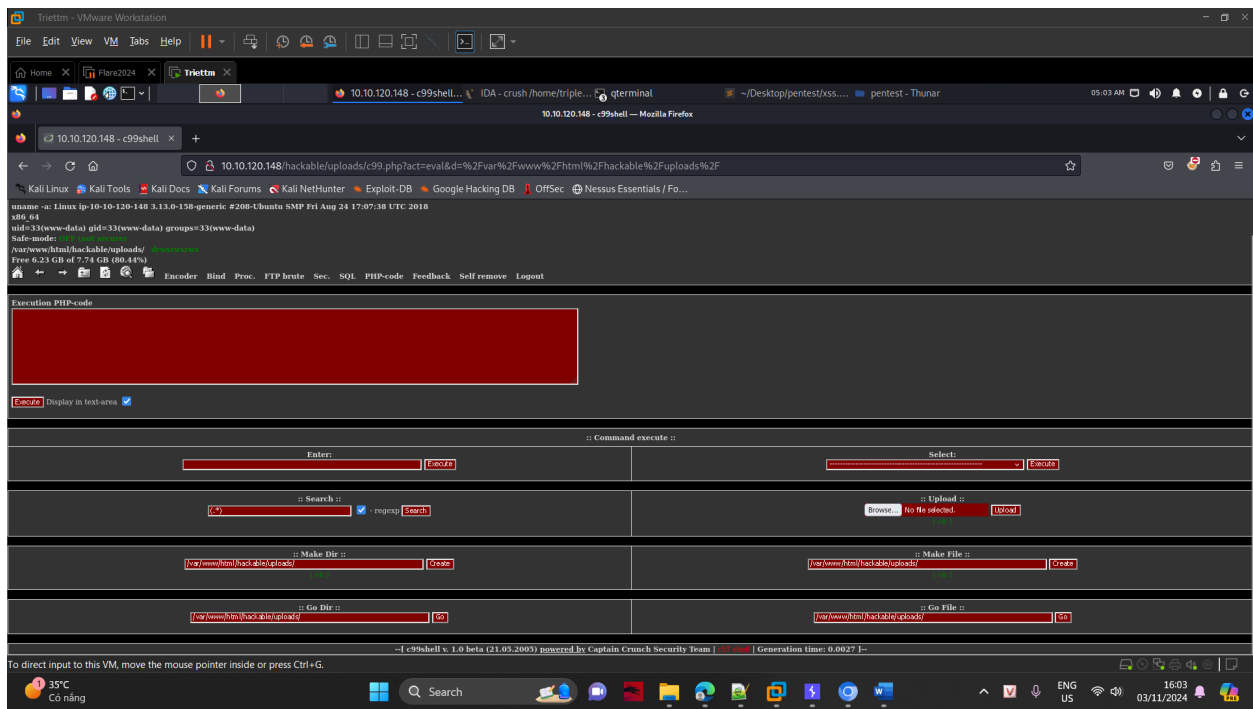




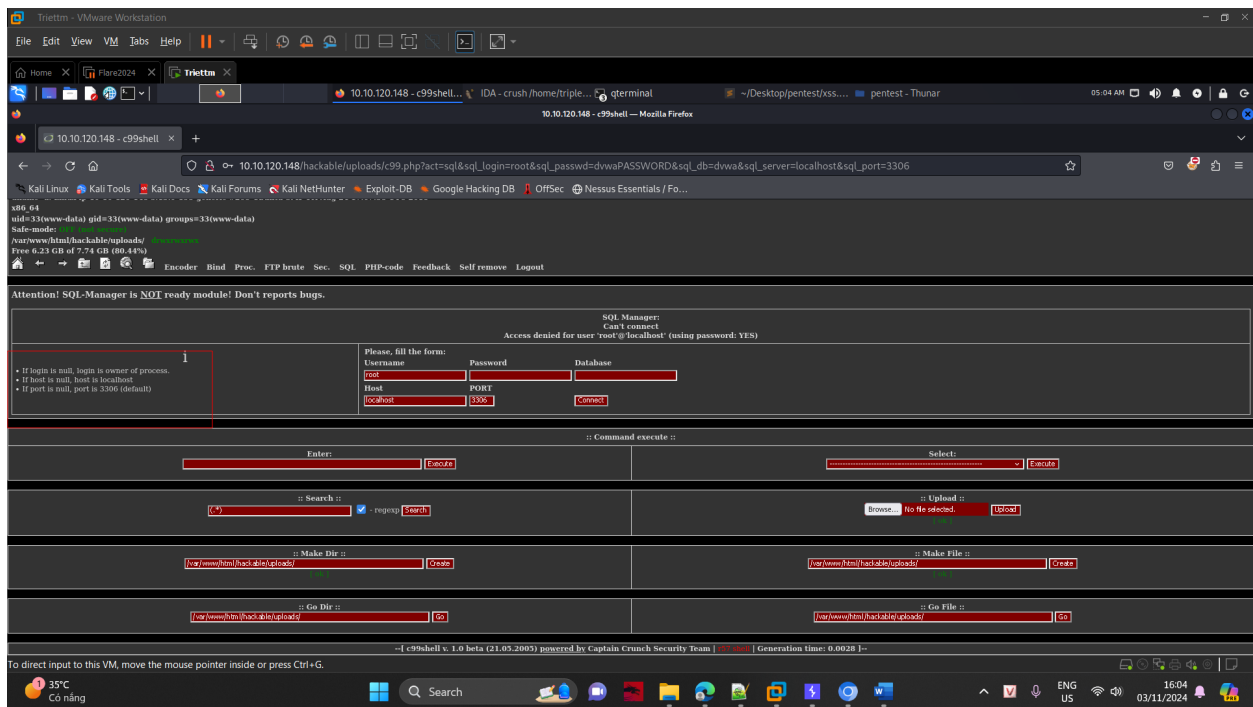




Using c99.php's to grab database password



Using c99.php's to examine pillage the database



Use c99.php to Bind with Netcat

