# PSP0201 Week 2 Writeup

Group Name: ikun no 1

### Members

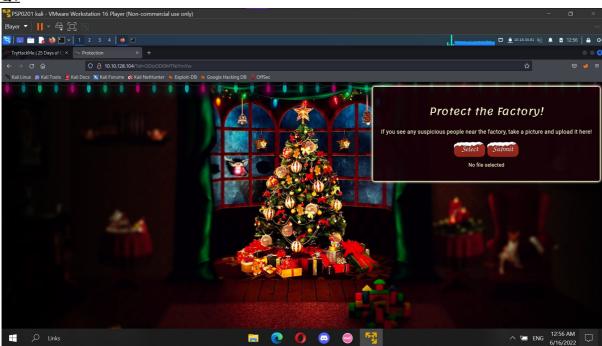
ID	Name	Role
1211102058	Chu Liang Chern	Leader
1211101401	Chong Jii Hong	Member
1211103206	Ng Kai Keat	Member
1211103095	Siddiq Ferhad Bin Khairil Anual	Member

# **DAY 2: Web Exploitation The Elf Strike Back!**

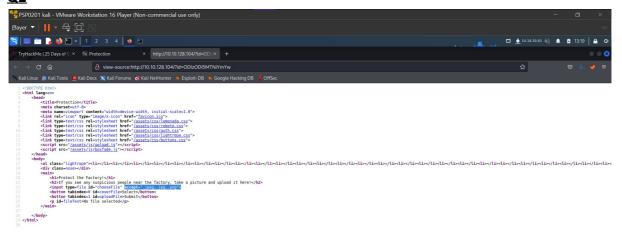
Tool used: kali Linux, Firefox

# Solution/Walkthrough:

<u>Q1</u>



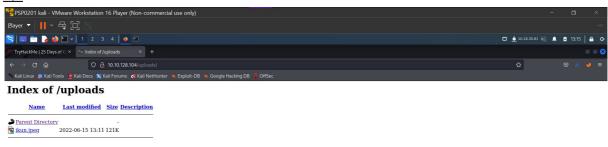
Add the id given in THM behind the ip address with the format ?id=<id given> **Q2** 





Right click on the page and choose the page source button. From the input type line, we can know that the site only accepts jpeg, jpg and png files only, which is the image file format.

## Q3



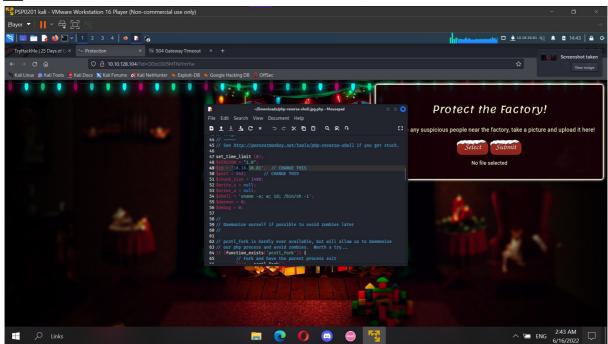


The directory can be found with a tool such as Gobuster, or by checking each of the common directories from the dossier. In this case, I am using the second method and the directory is bypassed with the subdirectory of /uploads/

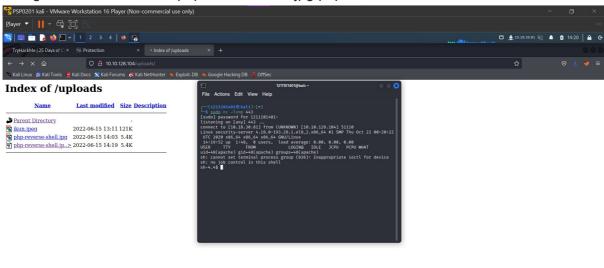
### Q4

```
-e'; use /bin/sh to exec [dangerous!!]
            shell commands
         -e filename
                                    program to exec after connect [dangerous!!]
         -b
                                    allow broadcasts
         -g gateway
                                    source-routing hop point[s], up to 8
         -G num
                                    source-routing pointer: 4, 8, 12, ...
         -h
                                    this cruft
                                    delay interval for lines sent, ports scanned
         -i secs
         -\mathbf{k}
                                    set keepalive option on socket
         -1
                                    listen mode, for inbound connects
                                    numeric-only IP addresses, no DNS
         -n
         -o file
                                    hex dump of traffic
                                    local port number
         -p port
                                    randomize local and remote ports
                                    quit after EOF on stdin and delay of secs
         -q secs
                                     local source address
                                    set Type Of Service
         -T tos
         -\mathbf{t}
                                    answer TELNET negotiation
                                    UDP mode
         -\mathbf{u}
                                    verbose [use twice to be more verbose]
                                    timeout for connects and final net reads
         -w secs
         -\mathbf{C}
                                    Send CRLF as line-ending
         -z
                                    zero-I/O mode [used for scanning]
port numbers can be individual or ranges: lo-hi [inclusive]; humbers in nort names must be backslash escaped (e.g., 'ftn>-
```

Run nc -h in the terminal and all the commands available in the netcat will be shown.

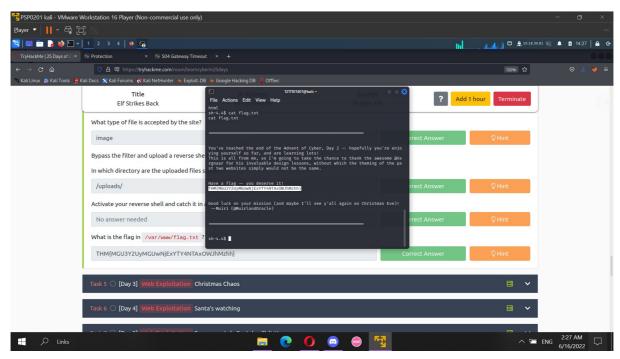


Download reverse shell. Edit the ip address into our own ip and the port to a common port such as 443 as this kind of port usually is not filtered by the firewalls. Save the file and change the file name into <php-reverse-shell.jpg.php>.





Upload the file to the site and start listening by typing in the command sudo nc -lvnp 443 in the terminal. Wait until the listener receives the shell successfully.



After finishing the task, the flag will appear. Catch the flag.