

LinkedIn: [Kelvin Kimotho](#)

Roboto Sans

Medium

Web Exploitation

picoCTF 2022

AUTHOR: MUBARAK MIKAIL

Description

The flag is somewhere on this web application not necessarily on the website. Find it.

Check [this](#) out.

This challenge launches an instance on demand.

Its current status is:

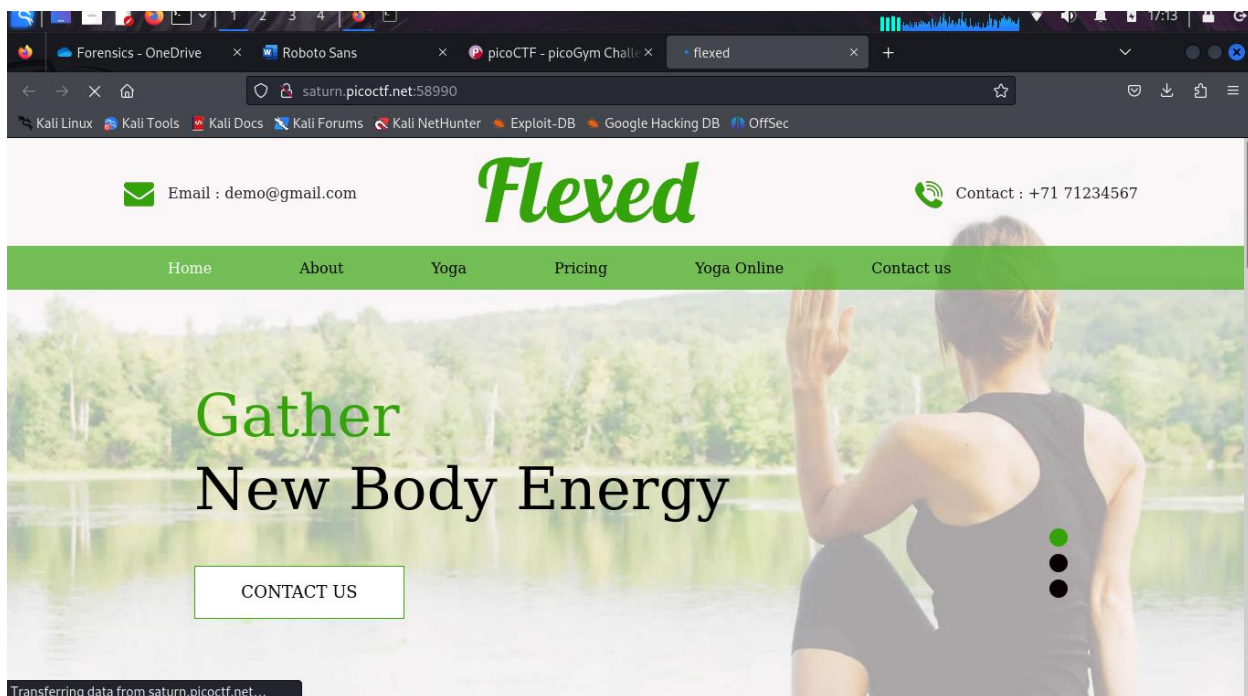
RUNNING

Instance Time Remaining:

10:42

Solution

A site with several page is rendered.



The first thing was to examine the source code but i found no flag. I used **curl** and **grep** tools searching for text that would match **“pico”**.

```
(kali@kali)-[~/Downloads]
└─$ curl http://saturn.picoctf.net:58990/ | grep pico
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload   Total   Spent    Left   Speed
100 15920  100 15920    0     0  7822      0  0:00:02  0:00:02 --:--:-- 7823

(kali@kali)-[~/Downloads]
└─$ curl http://saturn.picoctf.net:58990/css/style.css | grep pico
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload   Total   Spent    Left   Speed
100 10926  100 10926    0     0 17055      0  0:--:--  0:--:--  0:--:-- 17071

(kali@kali)-[~/Downloads]
└─$
```

Examining the source code in various files revealed no flag. I tried accessing the **robots.txt** file which revealed some suspicious information.

```
User-agent *
Disallow: /cgi-bin/
Think you have seen your flag or want to keep looking.

ZmxhZzEudHh0:anMvbXlmaW
anMvbXlmaWxLnR4dA==
svssshjweuwl;oiho.bsvdaslejg
Disallow: /wp-admin/
```

I discovered some strings that appeared to be base64 encodings. I tried decoding them and they revealed some important information.

```
(kali@kali)-[~/Downloads]
└─$ echo ZmxhZzEudHh0 | base64 -d
flag1.txt

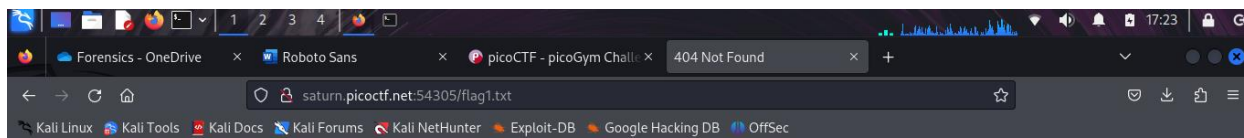
(kali@kali)-[~/Downloads]
└─$ echo anMvbXlmaW | base64 -d
js/myfibase64: invalid input

(kali@kali)-[~/Downloads]
└─$ echo anMvbXlmaWxLnR4dA== | base64 -d
js/myfile.txt

(kali@kali)-[~/Downloads]
└─$
```

I discovered two files whose filenames matched the base64 encodings **flag1.txt** and **js/myfile.txt**.

I tried accessing the **flag1.txt** via my browser but the file never existed in the server.



404 Not Found

nginx/1.21.6

I went ahead accessing the `js/myfile.txt`. Which revealed the flag
`picoCTF{Who_D03sN7_L1k5_90B0T5_032f1c2b}`.

