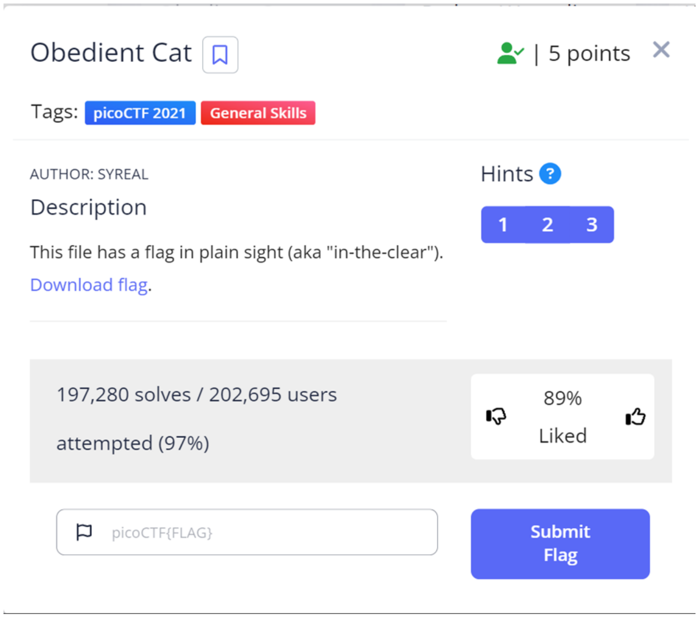
PICOCTF

GENERAL SKILLS
Starting with CTFs

1st- OBEDIENT CAT



Obedient Cat | 5 points

Tags: picoCTF 2021 General Skills

AUTHOR: SYREAL

Description

This file has a flag in plain sight (aka "in-the-clear"). Download flag.

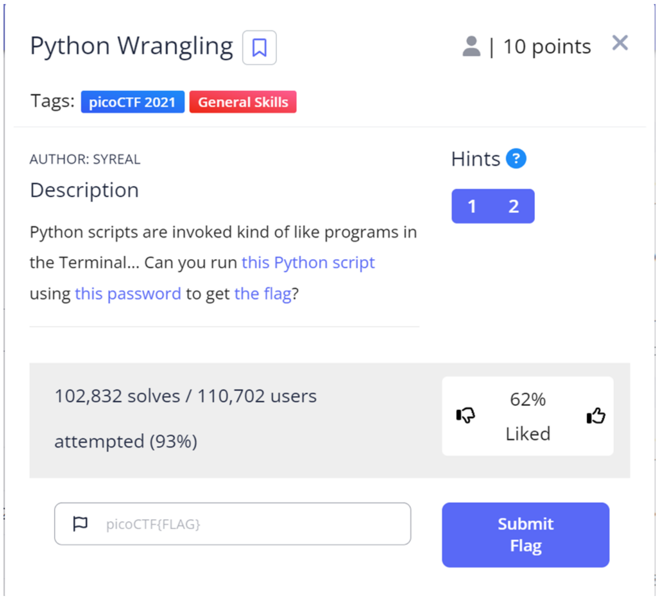
197,280 solves / 202,695 users

attempted (97%)

89% Liked

Open Webshell and use wget, followed by the download link. It will download it. open the file called flag using cat command. there you have it.

2. PYTHON WRANGLING



Python Wrangling

| 10 points

Tags: picoCTF 2021 General Skills

AUTHOR: SYREAL

Description

Python scripts are invoked kind of like programs in the Terminal... Can you run this Python script using this password to get the flag?

102,832 solves / 110,702 users attempted (93%)

62% Liked

STEP 1- use wget and the link to download all three files. pw.txt has the password that I have to paste later.

STEP 2- read the command using cat command. The following program is displayed..

```
import sys
import base64
from cryptography.fernet import Fernet

usage_msg = "Usage: "+ sys.argv[0] +" (-e/-d) [file]"
help_msg = usage_msg + "\n" +\
"Examples:\n" +\
" To decrypt a file named 'pole.txt', do: " +\
"'$ python "+ sys.argv[0] +" -d pole.txt'\n"

if len(sys.argv) < 2 or len(sys.argv) > 4:
print(usage_msg)
sys.exit(1)

if sys.argv[1] == "-e":
if len(sys.argv) < 4:
sim_sala_bim = input("Please enter the password:")
else:
sim_sala_bim = sys.argv[3]

ssb_b64 = base64.b64encode(sim_sala_bim.encode())
c = Fernet(ssb_b64)

with open(sys.argv[2], "rb") as f:
data = f.read()
```

```
data_c = c.encrypt(data)
sys.stdout.write(data_c.decode())


elif sys.argv[1] == "-d":
if len(sys.argv) < 4:
sim_sala_bim = input("Please enter the password:")
else:
sim_sala_bim = sys.argv[3]

ssb_b64 = base64.b64encode(sim_sala_bim.encode())
c = Fernet(ssb_b64)

with open(sys.argv[2], "r") as f:
data = f.read()
data_c = c.decrypt(data.encode())
sys.stdout.buffer.write(data_c)

elif sys.argv[1] == "-h" or sys.argv[1] == "--help":
print(help_msg)
sys.exit(1)

else:
print("Unrecognized first argument: "+ sys.argv[1])
print("Please use '-e', '-d', or '-h'.")
```

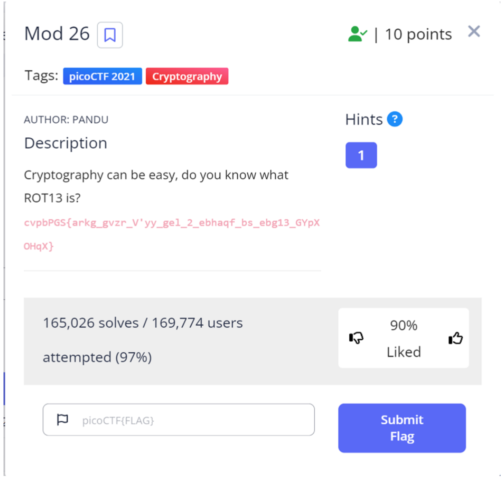
STEP 3: After reading the program a lot I can see that -e or -d flag is to be used somewhere. Type

```
captain_flint@Ubuntu:~/ctf$ python3 ende.py
Usage: ende.py (-e/-d) [file]
```

STEP 4: So there I go, typing. I also tried with -e but turns out that it is for encoding a file.

```
captain_flint@Ubuntu:~/ctf$ python3 ende.py -d flag.txt.en
Please enter the password:dbd1bea4dbd1bea4dbd1bea4dbd1bea4
picoCTF{4p0110_1n_7h3_h0us3_dbd1bea4}
```

3. MOD 26


Mod 26 | 10 points

Tags: picoCTF 2021 Cryptography

AUTHOR: PANDU

Description

Cryptography can be easy, do you know what ROT13 is?

```
cvpbPGS{arkg_gvzr_V'yy_gel_2_ebhaqf_bs_ebg13_GYpXOHqX}
```

165,026 solves / 169,774 users attempted (97%)

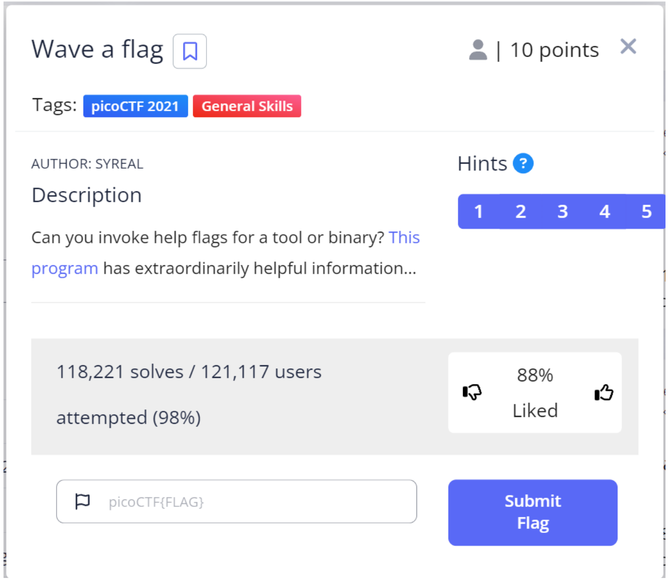
90% Liked

This one was simple, even for me. Just use ROT13 cipher that I learnt back in the day. It's just Ceaser's with a key of 13. Fun stuff. I used a decoder.

4.MOCHI'S TALE GAME

Done half till now. Not till now.

5.WAVE A FLAG


Wave a flag | 10 points

Tags: picoCTF 2021 General Skills

AUTHOR: SYREAL

Description

Can you invoke help flags for a tool or binary? This program has extraordinarily helpful information...

118,221 solves / 121,117 users attempted (98%)

88% Liked

STEP 1: wget a file called warm. I tried to cat command it but did not work. It is binary or some kind of tool.

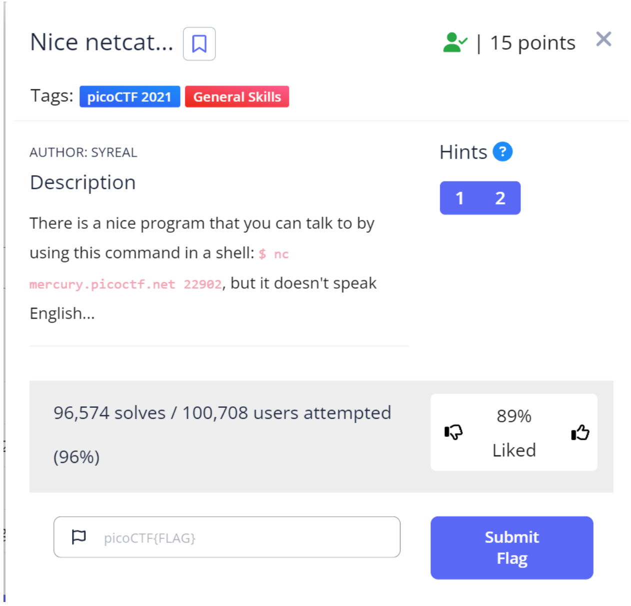
STEP 2: chmod +x command helps to make it executable. To execute it we do ./warm after the chmod command.

```
captain_flint@Ubuntu:~/ctf$ chmod +x warm
captain_flint@Ubuntu:~/ctf$ ./warm
Hello user! Pass me a -h to learn what I can do!
```

STEP 3: just do what the tool said ig. This is how we invoke help flags for binary or tools.

```
captain_flint@Ubuntu:~/ctf$ ./warm -h
Oh, help? I actually don't do much, but I do have this flag here:
picoCTF{b1scu1ts_4nd_gr4vy_18788aaa}
```

6 . NICE NETCAT



Nice netcat... | 15 points

Tags: picoCTF 2021 General Skills

AUTHOR: SYREAL

Description

There is a nice program that you can talk to by using this command in a shell: `$ nc mercury.picoctf.net 22902`, but it doesn't speak English...

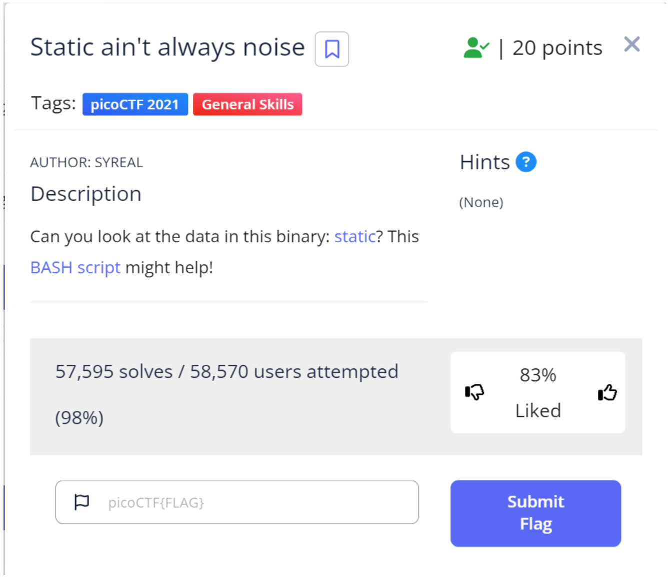
96,574 solves / 100,708 users attempted (96%)

89% Liked

STEP 1: ON using the command a list of numbers is shown on screen.

STEP 2: Just gotta use ASCII to decode the flag!

7 . STATIC AIN'T ALWAYS NOISE



AUTHOR: SYREAL

Description

Can you look at the data in this binary: static? This BASH script might help!

57,595 solves / 58,570 users attempted (98%)

STEP 1: Use wget to get the files ofc

```
wget https://mercury.picoctf.net/static/ff4e569d6b49b92d090796d4631a2577/static
```

```
wget https://mercury.picoctf.net/static/ff4e569d6b49b92d090796d4631a2577/ltdis.sh
```

STEP 2: Took help from the internet here. chmod u+x is how you execute a bash scripy. and binary one ofc is chmod +x. important is this. Can get hint from the usage message.

```
captain_flint@Ubuntu:~/ctf$ chmod u+x ltdis.sh
captain_flint@Ubuntu:~/ctf$ ./ltdis.sh
Attempting disassembly of ...
objdump: 'a.out': No such file
objdump: section '.text' mentioned in a -j option, but not found in any input file
Disassembly failed!
Usage: ltdis.sh <program-file>
Bye!
```

STEP 3: Made the static file executable and ran it.

```
captain_flint@Ubuntu:~/ctf$ ./static
bash: ./static: Permission denied
```

```
captain_flint@Ubuntu:~/ctf$ chmod +x static
```

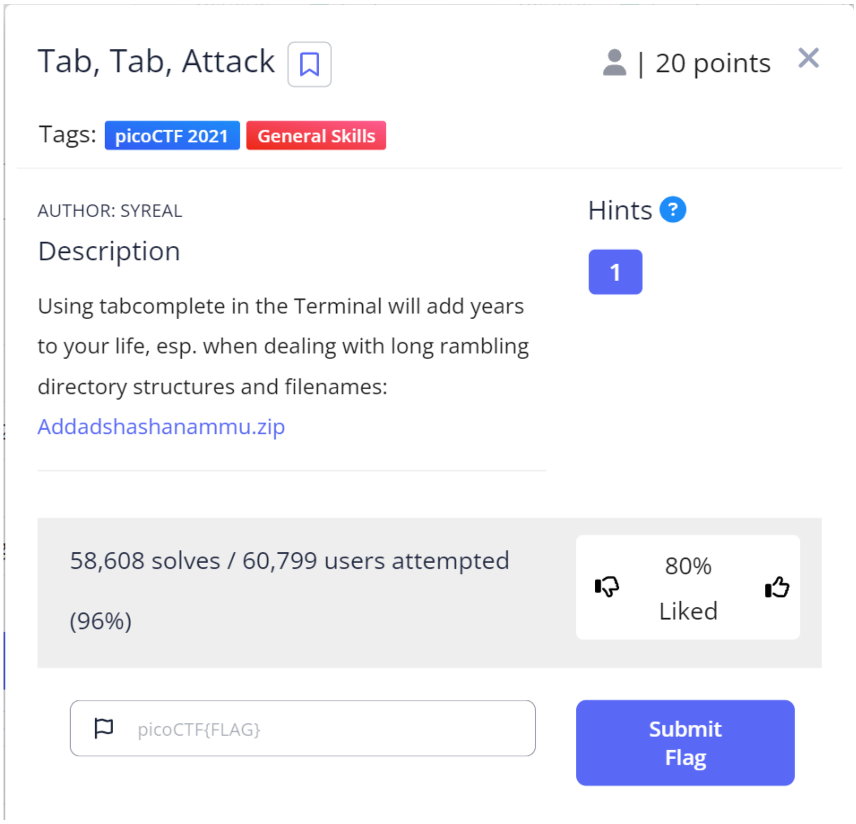
```
captain_flint@Ubuntu:~/ctf$ ./static
Oh hai! Wait what? A flag? Yes, it's around here somewhere!
```

STEP 4: used the command in the usage message and lo and behold!

```
captain_flint@Ubuntu:~/ctf$ ./ltdis.sh static
Attempting disassembly of static ...
Disassembly successful! Available at: static.ltdis.x86_64.txt
Ripping strings from binary with file offsets...
Any strings found in static have been written to static.ltdis.strings.txt with file offset
captain_flint@Ubuntu:~/ctf$ ls
ende.py flag.txt.en ltdis.sh pw.txt static static.ltdis.strings.txt static.ltdis.x86_64.txt
warm
```

STEP 5: The flag is in the static.ltdis.strings.txt file. Scroll a bit.

8 . Tab, Tab, Attack



Tab, Tab, Attack

| 20 points

Tags: picoCTF 2021 General Skills

AUTHOR: SYREAL

Description

Using tabcomplete in the Terminal will add years to your life, esp. when dealing with long rambling directory structures and filenames: Addadshashanammu.zip

Hints ?

1

58,608 solves / 60,799 users attempted (96%)

80% Liked

picoCTF{FLAG}

Submit Flag

STEP 1: wget the zip file with the weird ass name

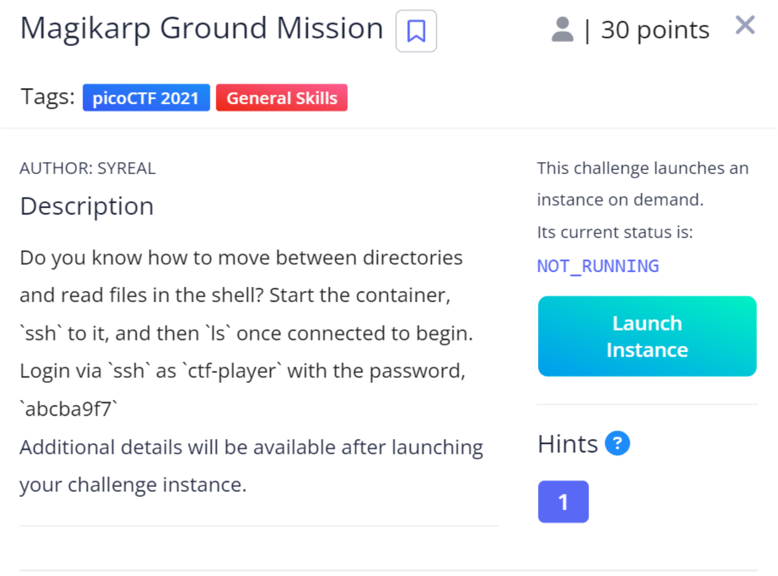
STEP 2: unzip it

```
captain_flint@Ubuntu:~/ctf$ unzip Addadshashanammu.zip
```

STEP 3: The directory is created. we cd into the directory and it has many directories inside it named weird. Simply press tab after cd to autofill. Literally saved my life hehe. In the end it has an executable file in it. do ./ (press tab)
The flag is right there! Peasy!

```
captain_flint@Ubuntu:~/ctf/Addadshashanammu/Almurbalarammi/Ashalmimilkala/Assurnabitashpi/M
aelkashishi/Onnissiralis/Ularradallaku$ ls
fang-of-haynekhtnamet
captain_flint@Ubuntu:~/ctf/Addadshashanammu/Almurbalarammi/Ashalmimilkala/Assurnabitashpi/M
aelkashishi/Onnissiralis/Ularradallaku$ ./fang-of-haynekhtnamet
*ZAP!* picoCTF{l3v3l_up!_t4k3_4_r35t!_d32e018c}
```

9 . Magikarp Ground Mission



Magikarp Ground Mission

| 30 points

Tags: picoCTF 2021 General Skills

AUTHOR: SYREAL

Description

Do you know how to move between directories and read files in the shell? Start the container, `ssh` to it, and then `ls` once connected to begin. Login via `ssh` as `ctf-player` with the password, `abcba9f7`

Additional details will be available after launching your challenge instance.

This challenge launches an instance on demand.

Its current status is:

NOT_RUNNING

STEP 1: on launching instance the ssh command was given. run it on the terminal and enter password.

```
captain_flint@Ubuntu:~/ctf$ ssh ctf-player@venus.picoctf.net -p 54314
ctf-player@venus.picoctf.net's password:
```

STEP 2: Now the different machine is opened

```
ctf-player@pico-chall$ ls
1of3.flag.txt instructions-to-2of3.txt
ctf-player@pico-chall$ cat 1of3.flag.txt
picoCTF{xxsh_
ctf-player@pico-chall$ cat instructions-to-2of3.txt
Next, go to the root of all things, more succinctly `/`
```

```
ctf-player@pico-chall$ cd /
```

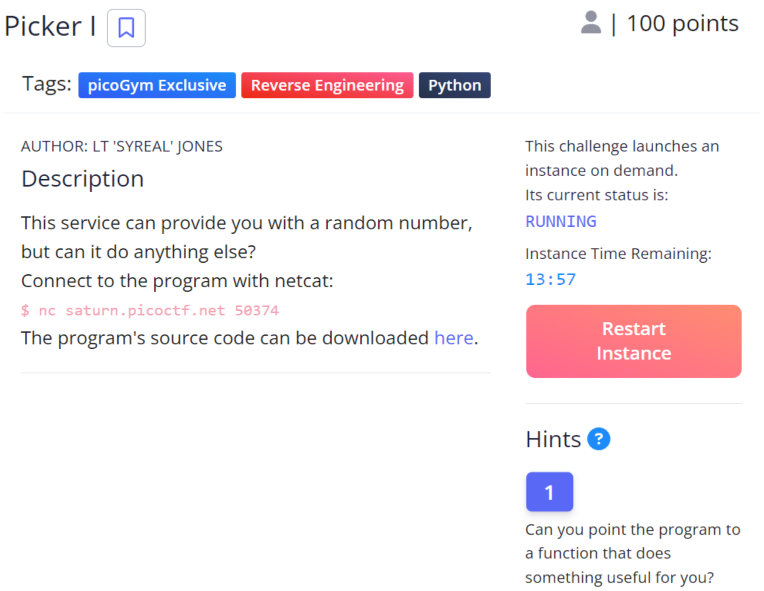
STEP 3: The flag is divided into 3 parts. Instructions are all given.

```
ctf-player@pico-chall$ ls
2of3.flag.txt bin boot dev etc home instructions-to-3of3.txt lib lib64 media mnt opt proc
root run sbin srv sys tmp usr var
ctf-player@pico-chall$ cat 2of3.flag.txt
0ut_0f_\/\/4t3r_
```

```
ctf-player@pico-chall$ cat instructions-to-3of3.txt
Lastly, ctf-player, go home... more succinctly `~`
ctf-player@pico-chall$ cd ~
ctf-player@pico-chall$ ls
3of3.flag.txt drop-in
ctf-player@pico-chall$ cat 3of3.flag.txt
21cac893}
```

LO! HERE WE HAVE IT!

10 . PICKER 1



AUTHOR: LT 'SYREAL' JONES

Description

This service can provide you with a random number, but can it do anything else?
Connect to the program with netcat:

`$ nc saturn.picoctf.net 50374`

The program's source code can be downloaded here.

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

Instance Time Remaining:
13:57

Can you point the program to a function that does something useful for you?

STEP 1: wget the python file and read it. A block of code will stand out from the long weird looking code I have no idea of.

```
def win():
# This line will not work locally unless you create your own 'flag.txt' in
# the same directory as this script
flag = open('flag.txt', 'r').read()
```

```
#flag = flag[:-1]
flag = flag.strip()
str_flag = ''
for c in flag:
str_flag += str(hex(ord(c))) + ' '
print(str_flag)
```

STEP 2: run the netcat command from the instance

```
Try entering "getRandomNumber" without the double quotes...
==> getRandomNumber
4
```

STEP 3: Try putting "win" when prompted

```
Try entering "getRandomNumber" without the double quotes...
==> win
[Errno 2] No such file or directory: 'flag.txt'
```

Step 4: WE could see that the program snippet has that command so I just went back using exit and created a file called flag.txt

```
touch flag.txt
```

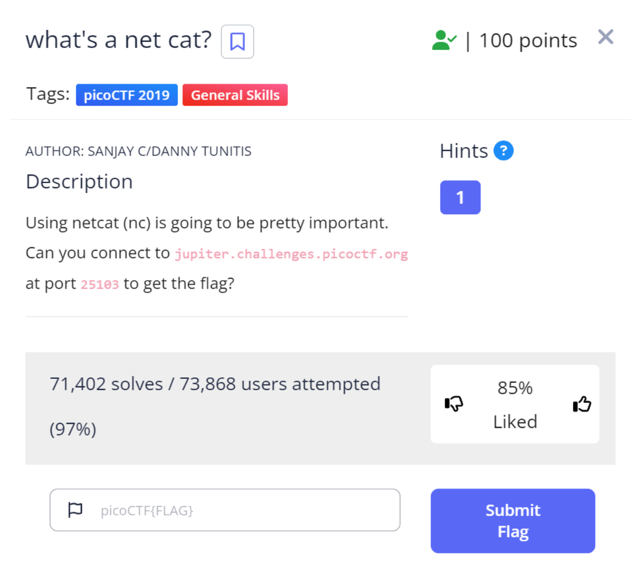
Then again use the nc command to access the program and type win.

```
captain_flint@Ubuntu:~/ctf$ nc saturn.picoctf.net 62878
Try entering "getRandomNumber" without the double quotes...
==> win
0x70 0x69 0x63 0x6f 0x43 0x54 0x46 0x7b 0x34 0x5f 0x64 0x31 0x34 0x6d 0x30 0x6e 0x64 0x5f
0x31 0x6e 0x5f 0x37 0x68 0x33 0x5f 0x72 0x30 0x75 0x67 0x68 0x5f 0x63 0x65 0x34 0x62 0x35
0x64 0x35 0x62 0x7d
```

STEP 5: Decode online using Cyber Chef tool! And lo! We have the flag.

"Programs tend to execute or run statements top to bottom in a program. In the last problem, this was perhaps obfuscated by the fact that the first dozens of lines were definitions of functions. In fact, the first item executed normally is `while(True)` at line 161. Everything before is part of a function definition which means execution of these statements is delayed until the function is called, which in this code is possible at `eval(user_input + ‘()’)`, line 165."

11 . WHAT'S A NET CAT



what's a net cat? | 100 points

Tags: picoCTF 2019 General Skills

AUTHOR: SANJAY C/DANNY TUNITIS

Description

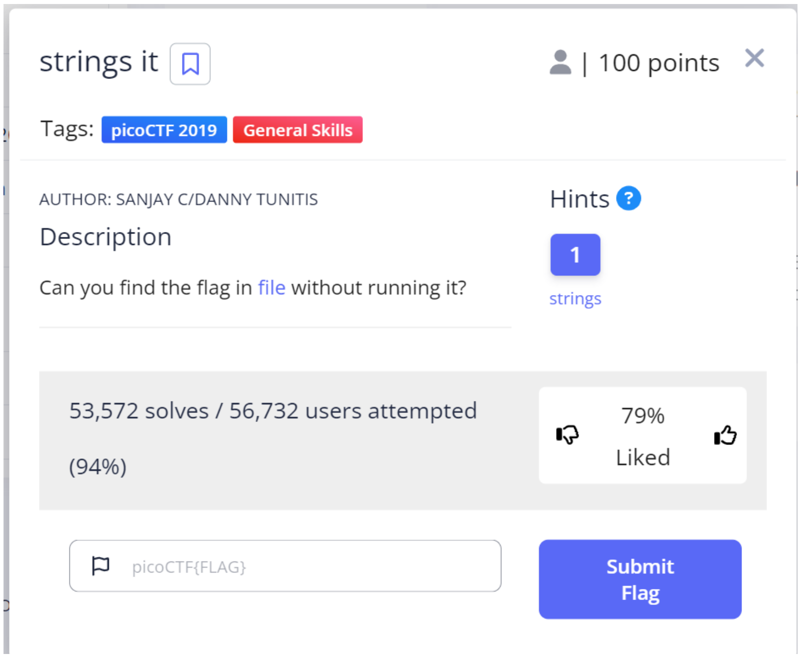
Using netcat (nc) is going to be pretty important. Can you connect to `jupiter.challenges.picoctf.org` at port `25103` to get the flag?

71,402 solves / 73,868 users attempted (97%)

STEP 1: Just use nc - the link- and the port number.

```
┌──(kali㉿kali)-[~]
└─$ nc jupiter.challenges.picoctf.org 25103
You're on your way to becoming the net cat master
picoCTF{nEtCat_Mast3ry_d0c64587}
```

12 . STRINGS IT



strings it | 100 points

Tags: picoCTF 2019 General Skills

AUTHOR: SANJAY C/DANNY TUNITIS

Description

Can you find the flag in file without running it?

53,572 solves / 56,732 users attempted (94%)

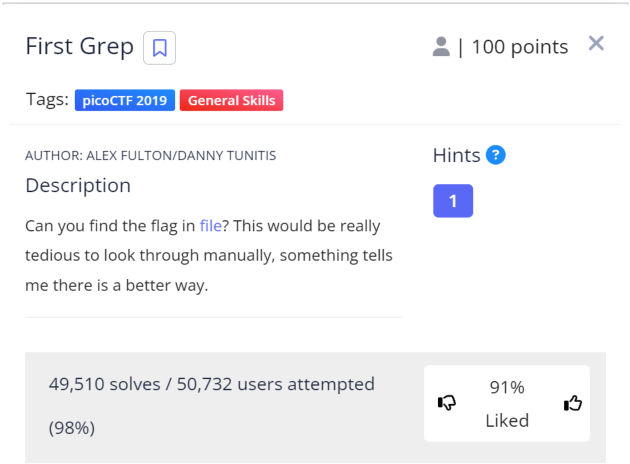
Step 1: wget the file in your local and don't open it

Step 2: The strings command loads the readable strings in a file without opening it. So, we try to use strings strings. But too much data is there to look through

Step 3: We use the grep command with the strings command to find the flag.

```
┌──(kali㉿kali)-[~/ctf]
└─$ strings strings|grep pico
picoCTF{5tRIng5_1T_d66c7bb7}
```

13 . FIRST GREP



First Grep | 100 points

Tags: picoCTF 2019 General Skills

AUTHOR: ALEX FULTON/DANNY TUNITIS

Description

Can you find the flag in file? This would be really tedious to look through manually, something tells me there is a better way.

Hints

1

49,510 solves / 50,732 users attempted (98%)

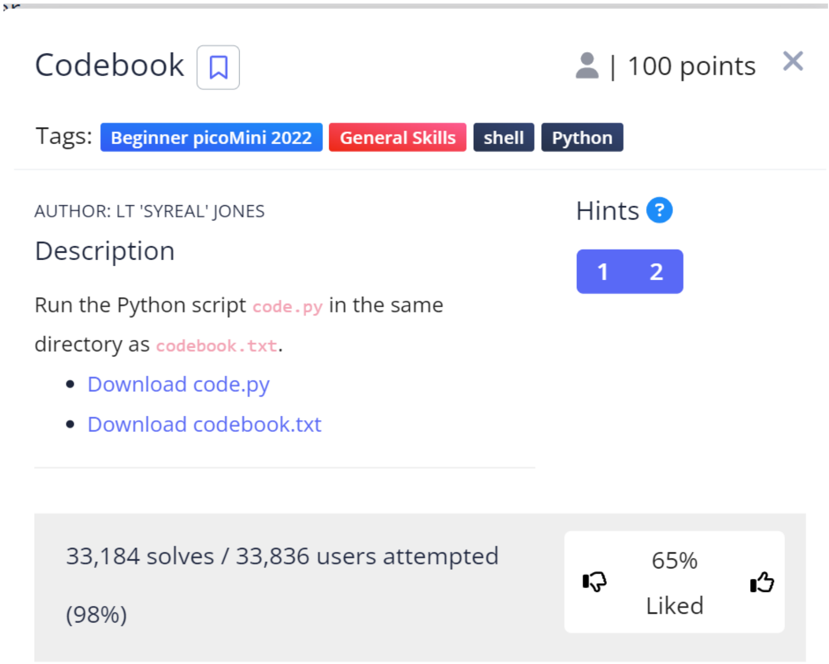
91% Liked

STEP 1: wget the file in the directory intended

STEP 2: Use grep command to find the flag in it

```
$grep "pico" file
picoCTF{grep_is_good_to_find_things_f77e0797}
```

14 . CODEBOOK



Codebook

Tags: Beginner picoMini 2022 General Skills shell Python

AUTHOR: LT 'SYREAL' JONES

Description

Run the Python script `code.py` in the same directory as `codebook.txt`.

- Download code.py
- Download codebook.txt

33,184 solves / 33,836 users attempted (98%)

Step 1: wget the two files in the same directory
Step 2: python3 code.py
Super straight-forward