picoCTF 2022 Mini

runme.py

5 points

Tags: Category: General Skills | Python

AUTHOR: SUJEET KUMAR

Description

Run the `runme.py` script to get the flag. Download the script with your browser or with `wget` in the webshell.

Download runme.py Python script

Hints

1 2 3 4

3,615 solves / 4,799 attempts (75%)

73% Liked

picoCTF{FLAG}

Submit Flag

```
➜  picoCTFmini2022_playground python3 runme.py
picoCTF{run_s4n1ty_run}
➜  picoCTFmini2022_playground
```

ncme

10 points

Tags: Category: General Skills | nc

AUTHOR: LT 'SYREAL' JONES

Description

Connect to a remote computer using `nc` and get the flag.

```
$ nc saturn.picoctf.net 57688
```

Hints

1 2 3

3,318 solves / 3,827 attempts (87%)

77% Liked

picoCTF{FLAG}

Submit Flag

```
➜  picoCTFmini2022_playground nc saturn.picoctf.net 57688
picoCTF{s4n1ty_c4t}
➜  picoCTFmini2022_playground
```

convertme.py | | 15 points

Tags: Category: General Skills | base | Python

AUTHOR: LT 'SYREAL' JONES

Description

Run the Python script and convert the given number from decimal to binary to get the flag.

Download Python script

Hints

1 2 3 4

3,183 solves / 4,814 attempts (66%)

71% Liked

picoCTF{FLAG}

Submit Flag

Using CyberChef

Last build: 5 months ago Options About / Su

Recipe

From Decimal

Delimiter: Space

Support signed values

To Binary

Delimiter: Space

Byte Length: 8

Input length: 2 lines: 1

61

Output time: 1ms length: 8 lines: 1

00111101

```
➜  picoCTFmini2022_playground python3 convertme.py
If 61 is in decimal base, what is it in binary base?
Answer: 00111101
That is correct! Here's your flag: picoCTF{4ll_y0ur_b4535_e2a58836}
➜  picoCTFmini2022_playground
```

Codebook

20 points

Tags: Category: 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

Hints

1 2

2,885 solves / 3,305 attempts (87%)

51% Liked

picoCTF{FLAG}

Submit Flag

```
→  picoCTFmini2022_playground python3 code.py
picoCTF{c0d3b00k_455157_8100c7c1}
→  picoCTFmini2022_playground
```

fixme1.py

25 points

Tags: Category: General Skills | Python

AUTHOR: LT 'SYREAL' JONES

Description

Fix the syntax error in this Python script to print the flag.

Download Python script

Hints

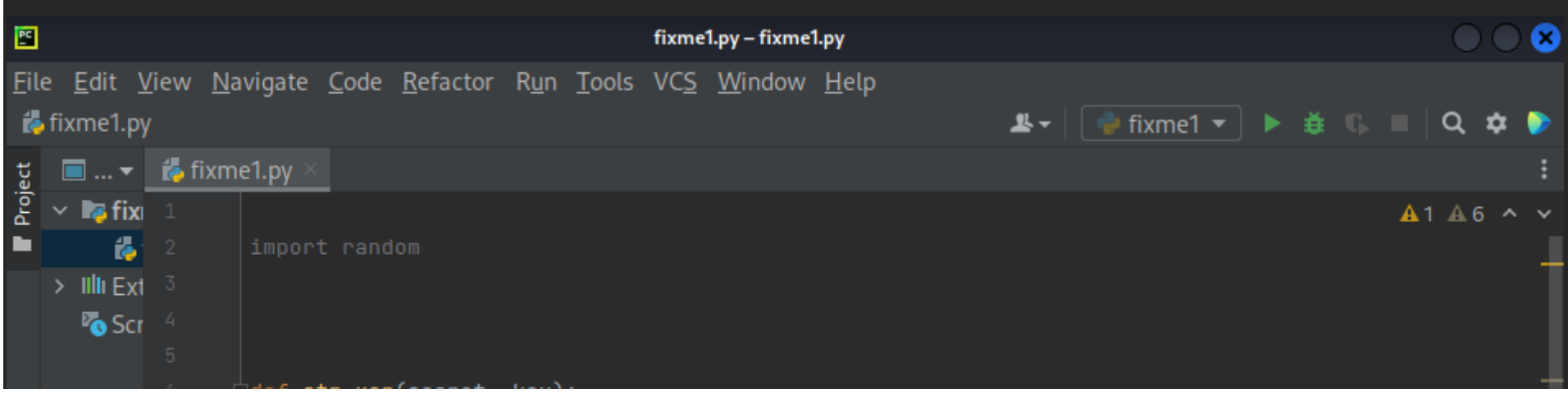
1 2 3 4

3,101 solves / 3,826 attempts (81%)

78% Liked

picoCTF{FLAG}

Submit Flag



```
def str_xor(secret, key):
    #extend key to secret length
    new_key = key
    i = 0
    while len(new_key) < len(secret):
        new_key = new_key + key[i]
        i = (i + 1) % len(key)
    return "".join([chr(ord(secret_c) ^ ord(new_key_c)) for (secret_c,new_key_c) in zip(secret,new_k


flag_enc = chr(0x15) + chr(0x07) + chr(0x08) + chr(0x06) + chr(0x27) + chr(0x21) + chr(0x23) + chr(0
```

```
/home/biddion/Documents/GitHub/picoCTF/fixme1.py
flag_enc: str = chr(0x15) + chr(0x07) + chr(0x08) + chr(0x06) + chr(0x27) + chr(0x21) + chr(0x23) +
```

```
print('That is correct! Here\'s your flag: ' + flag)
```

Run: fixme1

```
/usr/bin/python3.9 /home/biddion/Documents/GitHub/picoCTF/fixme1.py
That is correct! Here's your flag: picoCTF{1nd3nt1ty_cr1515_09ee727a}

Process finished with exit code 0
```

Structure | Bookmarks

Version Control | Run | TODO | Problems | Terminal | Python Packages | Python Console | Event Log

Download pre-built shared indexes: Reduce the indexing time and CPU load w... (a minute ago) 5:1 LF UTF-8 4 spaces Python 3.9

ing command-

fixme2.py

| | 25 points

Tags: Category: General Skills | Python

AUTHOR: LT 'SYREAL' JONES

Description

Fix the syntax error in the Python script to print the flag.

Download Python script

Hints

1 2 3 4

Are equality and assignment the same symbol?

3,008 solves / 3,339 attempts (90%)

87% Liked

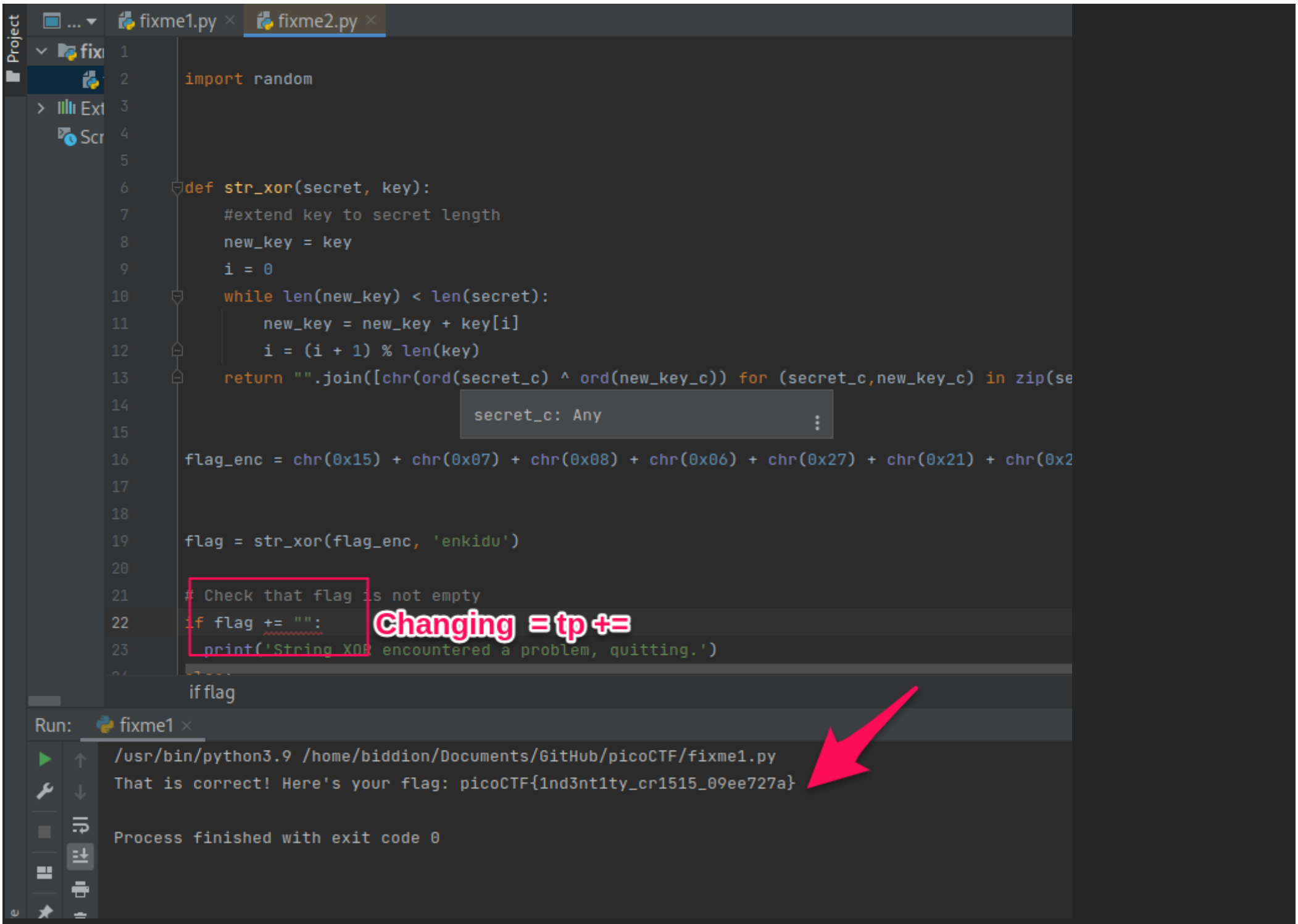
picoCTF{FLAG}

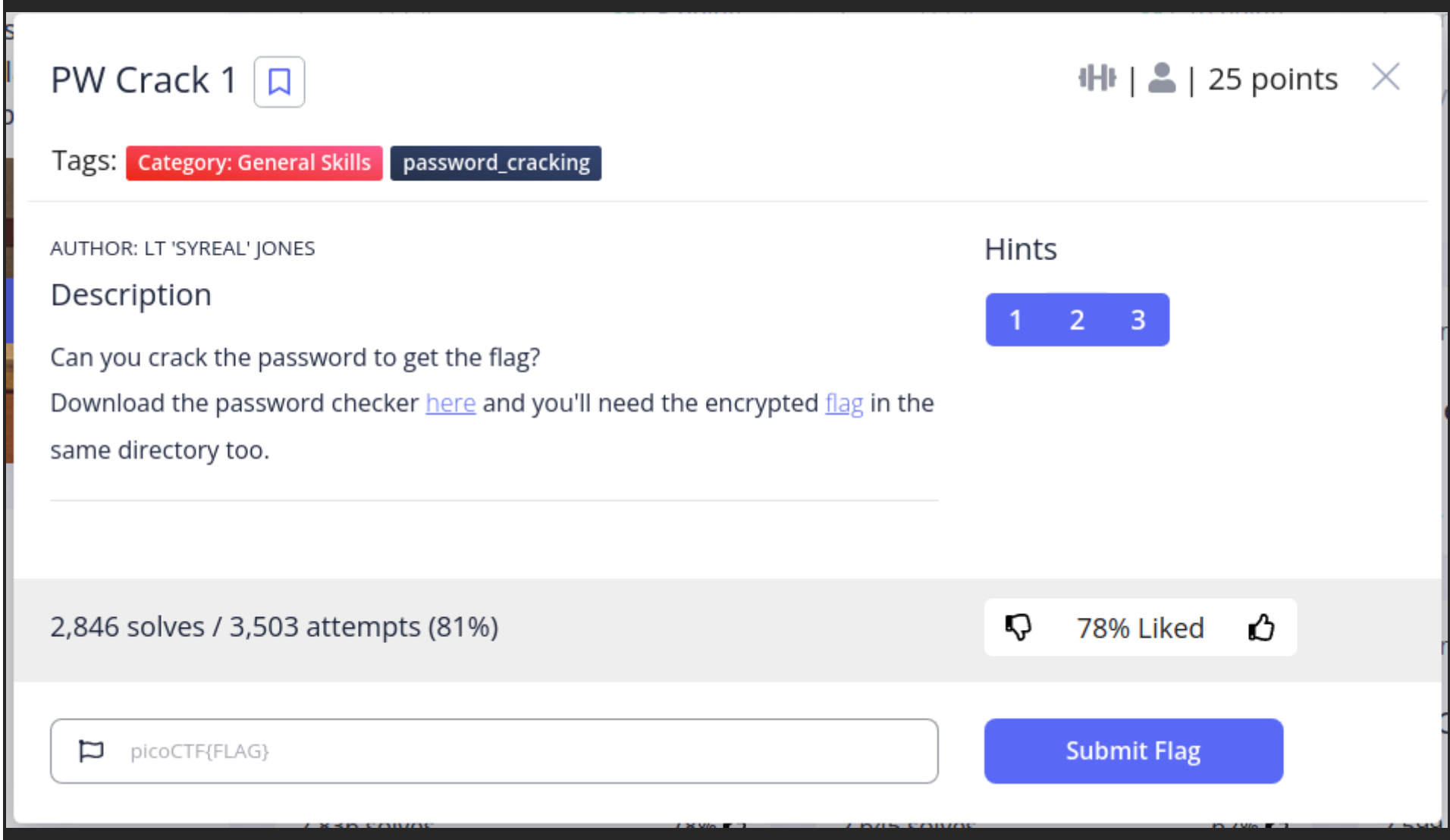
Submit Flag

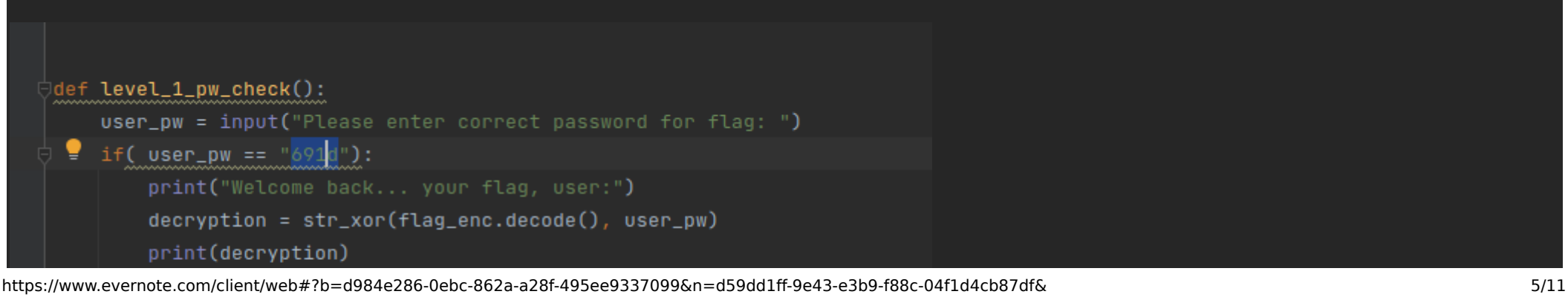
fixme1.py – ~/[

File Edit View Navigate Code Refactor Run Tools VCS Window Help

/ home biddion Documents GitHub picoCTF fixme2.py

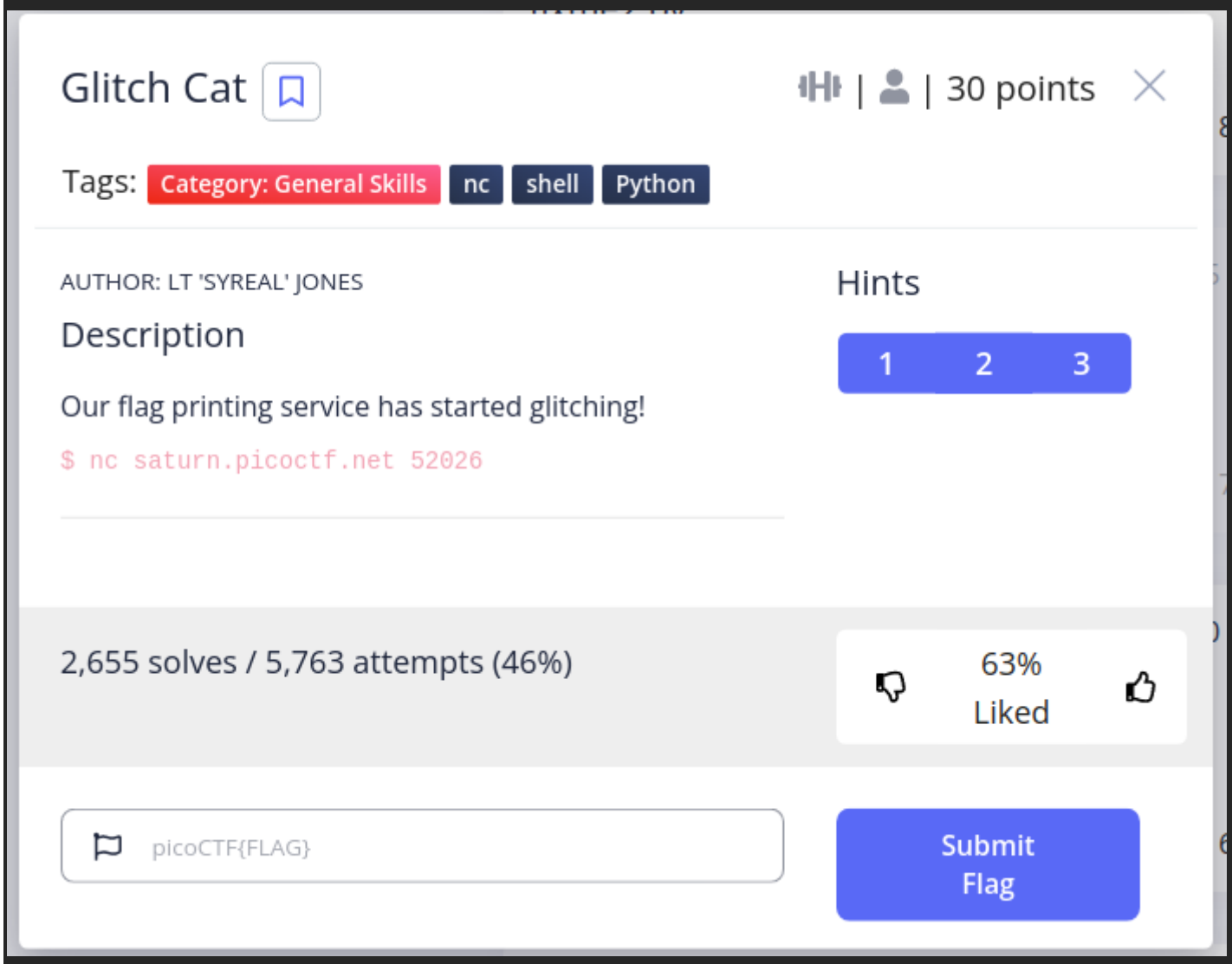

fixme1.py
fixme2.py
import random
def str_xor(secret, key):
#extend key to secret length
new_key = key
i = 0
while len(new_key) < len(secret):
new_key = new_key + key[i]
i = (i + 1) % len(key)
return "".join([chr(ord(secret_c) ^ ord(new_key_c)) for (secret_c,new_key_c) in zip(se
secret_c: Any
flag_enc = chr(0x15) + chr(0x07) + chr(0x08) + chr(0x06) + chr(0x27) + chr(0x21) + chr(0x2
flag = str_xor(flag_enc, 'enkidu')
# Check that flag is not empty
if flag += "":
print('String XOR encountered a problem, quitting.')
Changing = to +=
if flag
Run: fixme1
/usr/bin/python3.9 /home/biddion/Documents/GitHub/picoCTF/fixme1.py
That is correct! Here's your flag: picoCTF{1nd3nt1ty_cr1515_09ee727a}
Process finished with exit code 0


PW Crack 1
| 25 points
Tags: Category: General Skills password_cracking
AUTHOR: LT 'SYREAL' JONES
Description
Can you crack the password to get the flag?
Download the password checker here and you'll need the encrypted flag in the same directory too.
Hints
1 2 3
2,846 solves / 3,503 attempts (81%)
78% Liked
picoCTF{FLAG}
Submit Flag


def level_1_pw_check():
user_pw = input("Please enter correct password for flag: ")
if(user_pw == "691d"):
print("Welcome back... your flag, user:")
decryption = str_xor(flag_enc.decode(), user_pw)
print(decryption)

```
        return
    print("That password is incorrect")
```

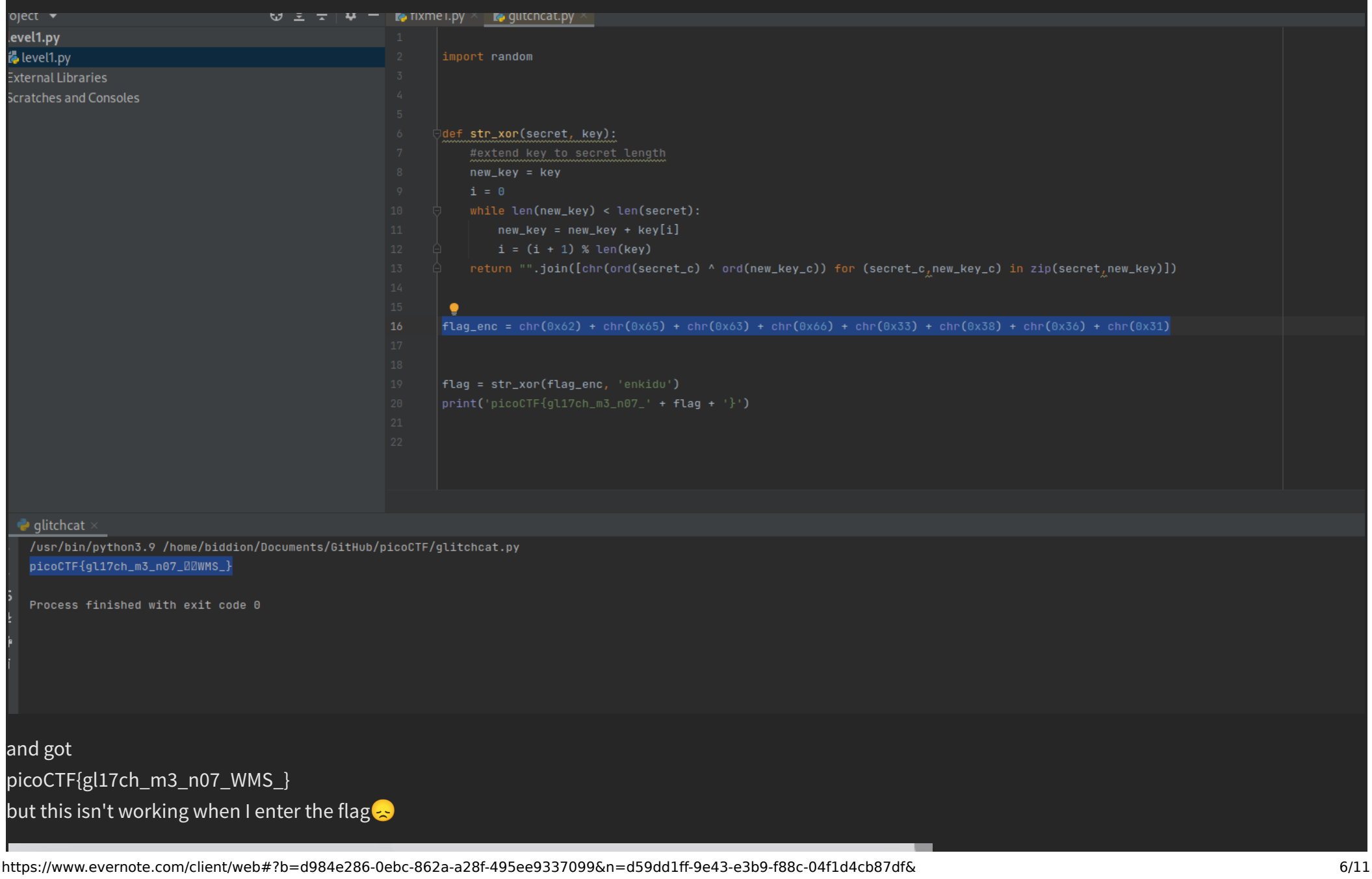
```
┌──(biddion㉿kali)-[~/Documents/GitHub/picoCTF]
└─$ python3 level1.py level1.flag.txt.enc
Please enter correct password for flag: 691d
Welcome back... your flag, user:
picoCTF{545h_r1ng1ng_56891419}
```



Hmmm I took the file from fixme1.py and inserted

```
flag_enc = chr(0x62) + chr(0x65) + chr(0x63) + chr(0x66) + chr(0x33) + chr(0x38) + chr(0x36) + chr(0x31)
```

And changed the string to the proper



and got
picoCTF{gl17ch_m3_n07_WMS_}
but this isn't working when I enter the flag😞

Glitch Cat

| | | 30 points

Tags: Category: General Skills | nc | shell | Python

AUTHOR: LT 'SYREAL' JONES

Description

Our flag printing service has started glitching!

```
$ nc saturn.picoctf.net 52026
```

Hints

1 2 3

ASCII is one of the most common encodings used in programming

2,658 solves / 5,766 attempts (46%)

63% Liked

picoCTF{gl17ch_m3_n07_☎☊WMS_}

Submit Flag

PW Crack 2

| | | 35 points

Tags: Category: General Skills | password_cracking

AUTHOR: LT 'SYREAL' JONES

Description

Can you crack the password to get the flag?

Download the password checker here and you'll need the encrypted flag in the same directory too.

Hints

1 2

2,613 solves / 2,909 attempts (90%)

91% Liked

picoCTF{FLAG}

Submit Flag

```
_check():
input("Please enter correct password for flag: ")
 == chr(0x34) + chr(0x65) + chr(0x63) + chr(0x39):
"Welcome back... your flag, user:")
tion = str_xor(flag_enc.decode(), user_pw)
```

Couldnt figure out how to make pycharm spit out the ascii, so I used a chart

ASCII Table

Dec	Hex	Alt	Ascii Character	Dec	Hex	Ascii Character	Dec	Hex	Ascii Character	Dec	Hex	Ascii Character
0	0x00		NUL (Null)	32	0x20	[Space]	64	0x40	@	96	0x60	`
1	0x01	☺	SOH	33	0x21	!	65	0x41	A	97	0x61	a
2	0x02	☻	STX	34	0x22	"	66	0x42	B	98	0x62	b
3	0x03	♥	ETX	35	0x23	#	67	0x43	C	99	0x63	c
4	0x04	♦	EOT	36	0x24	$	68	0x44	D	100	0x64	d

5	0x05	♣	ENQ	37	0x25	%	69	0x45	E	101	0x65	e		
6	0x06	♠	ACK	38	0x26	&	70	0x46	F	102	0x66	f		
7	0x07	•	BEL	39	0x27	'	71	0x47	G	103	0x67	g		
8	0x08	◘	BS Backspace	40	0x28	(	72	0x48	H	104	0x68	h		
9	0x09	○	TAB \t	41	0x29	)	73	0x49	I	105	0x69	i		
10	0x0A	◙	LF Line Feed \n	42	0x2A	*	74	0x4A	J	106	0x6A	j		
11	0x0B	♂	VT	43	0x2B	+	75	0x4B	K	107	0x6B	k		
12	0x0C	♀	FF Form Feed	44	0x2C	,	76	0x4C	L	108	0x6C	l		
13	0x0D	♪	CR Carriage Return \r	45	0x2D	-	77	0x4D	M	109	0x6D	m		
14	0x0E	♫	SO	46	0x2E	.	78	0x4E	N	110	0x6E	n		
15	0x0F	☼	SI	47	0x2F	/	79	0x4F	O	111	0x6F	o		
16	0x10	►	DLE	48	0x30	0	80	0x50	P	112	0x70	p		
17	0x11	◄	DC1	49	0x31	1	81	0x51	Q	113	0x71	q		
18	0x12	↕	DC2	50	0x32	2	82	0x52	R	114	0x72	r		
19	0x13	‼	DC3	51	0x33	3	83	0x53	S	115	0x73	s		
20	0x14	¶	DC4	52	0x34	4	84	0x54	T	116	0x74	t		
21	0x15	§	NAK	53	0x35	5	85	0x55	U	117	0x75	u		
22	0x16	▬	SYN	54	0x36	6	86	0x56	V	118	0x76	v		
23	0x17	↨	ETB	55	0x37	7	87	0x57	W	119	0x77	w		
24	0x18	↑	CAN	56	0x38	8	88	0x58	X	120	0x78	x		
25	0x19	↓	EM	57	0x39	9	89	0x59	Y	121	0x79	y		
26	0x1A	→	SUB (EOF)	58	0x3A	:	90	0x5A	Z	122	0x7A	z		
27	0x1B	←	ESC (Escape)	59	0x3B	;	91	0x5B	[	123	0x7B	{		
28	0x1C	∟	FS	60	0x3C	<	92	0x5C	\	124	0x7C	|		
29	0x1D	↔	GS	61	0x3D	=	93	0x5D	]	125	0x7D	}		
30	0x1E	▲	RS	62	0x3E	>	94	0x5E	^	126	0x7E	~		
31	0x1F	▼	US	63	0x3F	?	95	0x5F	_	127	0x7F	DEL		

4ec9

```
┌──(biddion㉿kali)-[~/Documents/GitHub/picoCTF]
└─$ python3 level2.py level2.flag.txt.enc
Please enter correct password for flag: 4ec9
Welcome back... your flag, user:
picoCTF{tr45h_51ng1ng_9701e681}
```

HashingJobApp

| | | 40 points

Tags: Category: General Skills | hashing | nc | shell | Python

AUTHOR: LT 'SYREAL' JONES

Description

If you want to hash with the best, beat this test!

`nc saturn.picoctf.net 65352`

Hints

1 2

2,684 solves / 3,135 attempts (86%)

77% Liked

picoCTF{FLAG}

Submit Flag

Hmmm. I'm not sure exactly what they want here despite my experience with md5sum

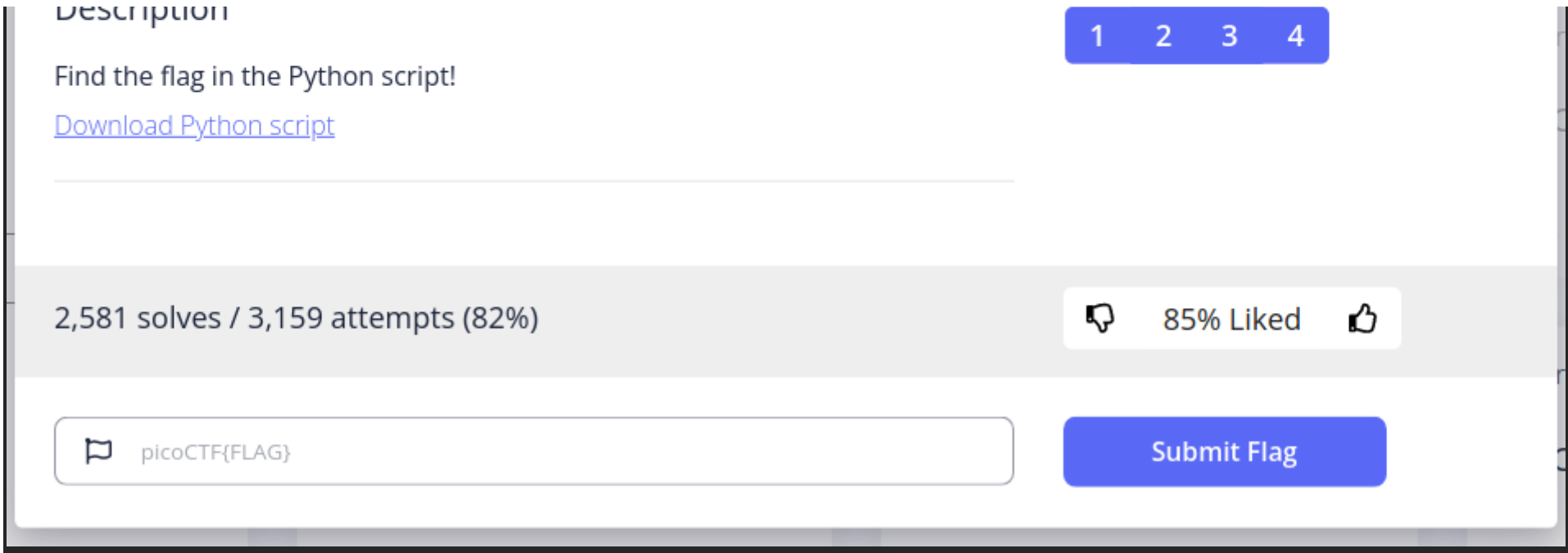
Serpentine

| | | 50 points

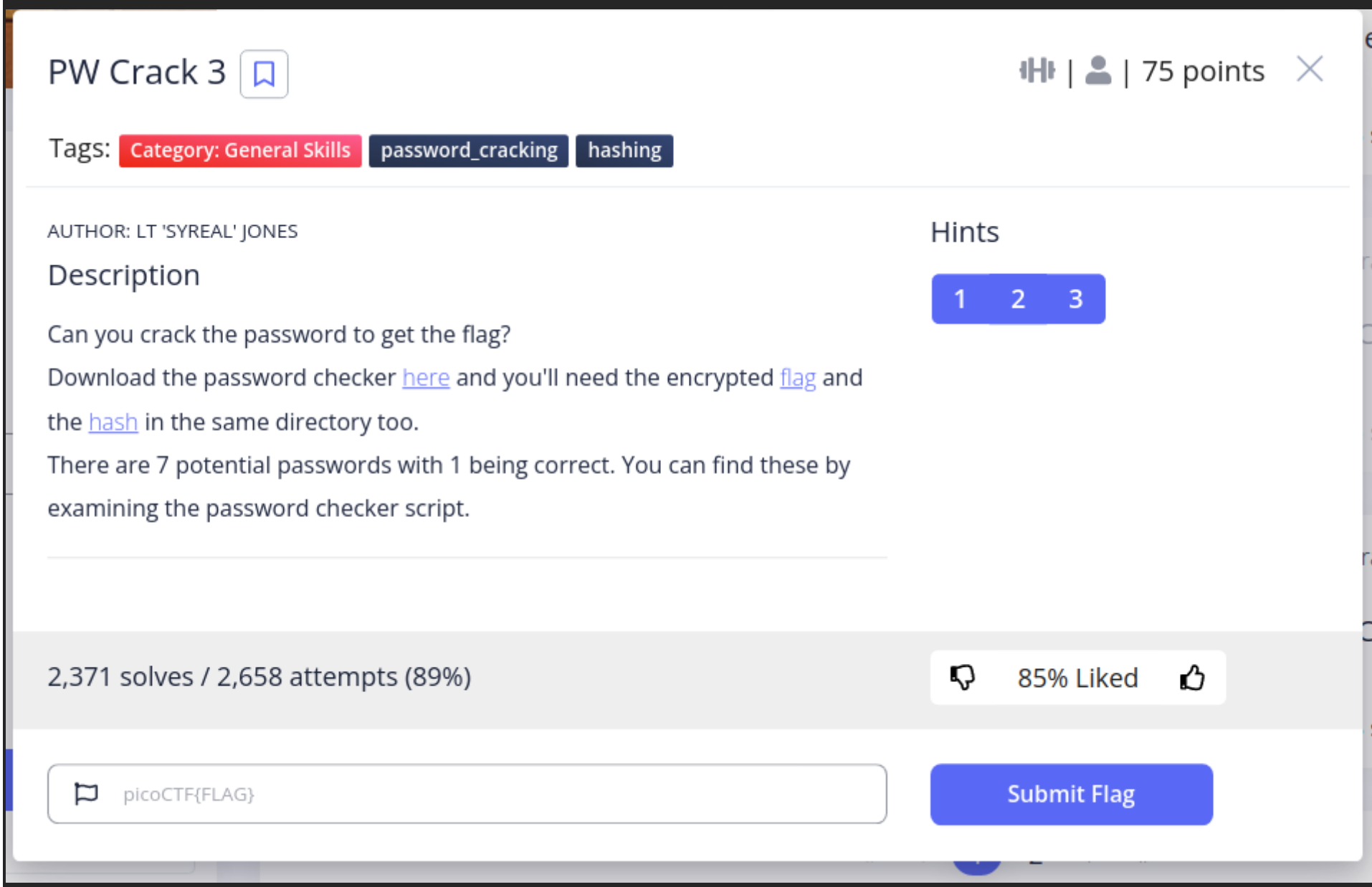
Tags: Category: General Skills | Python

AUTHOR: LT 'SYREAL' JONES

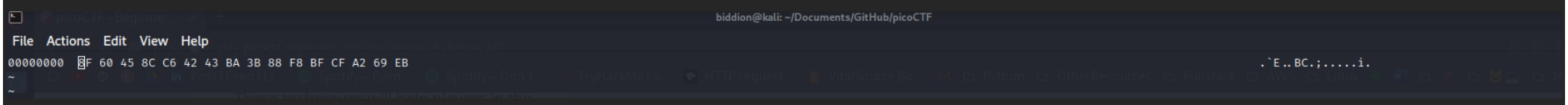
Hints



I'll come back to this later



Having installed bvi to system
bvi level3.hash.bin



What is this? .`E.ÆBC°;.ø¿Ï¢ië

Having opened the script I find:

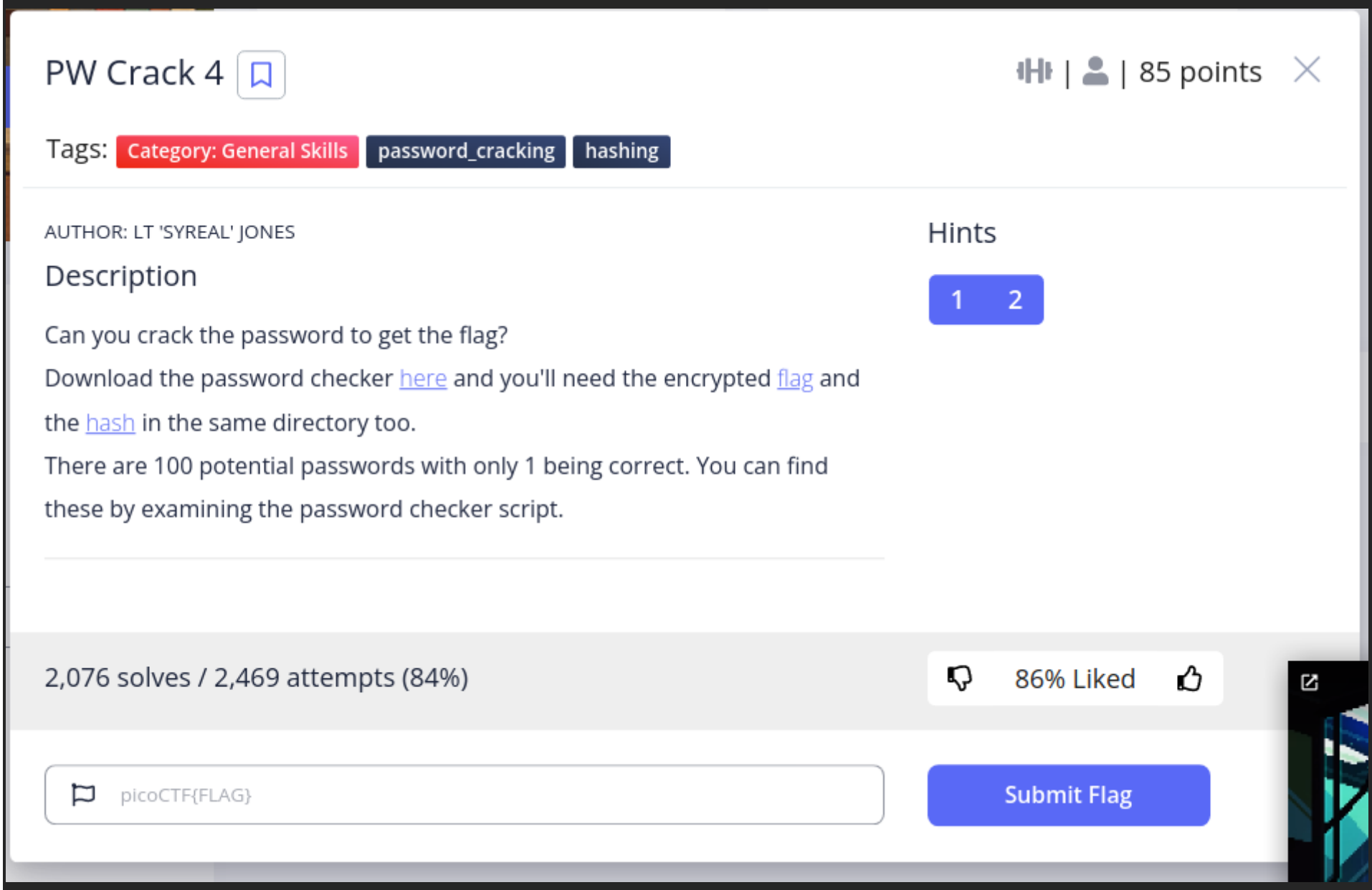
```
# The strings below are 7 possibilities for the correct password.
#  (Only 1 is correct)
pos_pw_list = ["8799", "d3ab", "1ea2", "acaf", "2295", "a9de", "6f3d"]
```

After manually bruteforcing

```
┌──(biddion㉿kali)-[~/Documents/GitHub/picoCTF]
└─$ python3 level3.py level3.flag.txt.enc
```

```
Please enter correct password for flag: 1ea2
Welcome back... your flag, user:
picoCTF{m45h_fl1ng1ng_6f98a49f}
```

I wish I knew a better way.



Again, I don't know how to do this yet.😞 I'll ask my friend for help soon.😉
I did find the 100 passwords and put them in a txt thinking I can use something like john to break; all my googlefoo attempts brought me to python scripts to do the breaking, not how to break a script. Looking at the hint, it seems I need to do a "for loop" which I can only do loops that print fruits hahaha!