



AUTHOR: LT 'SYREAL' JONES

Hints ?

Description

(None)

Can you get the flag?

Run this [Python program](#) in the same directory as this [encrypted flag](#).

The screenshot shows the VS Code interface with two files open:

- bloat.flag.py** (left pane):


```

1 import sys
2 a = "\\\\".abdefghijklmnopqrstuvwxyz{}~-"
3 def arg13(arg432):
4     if arg432 == a[71]+a[64]+a[79]+a[88]+a[66]+a[71]+a[64]+a[77]
5         return True
6     else:
7         print(a[51]+a[71]+a[64]+a[83]+a[94]+a[79]+a[64]+a[82]+a[86]
8             +a[81]+a[67]+a[94]+a[72]+a[82]+a[94]+a[72]+a[77]+a[66]+a[78]+a[81]+a[81]+a[68]+a[66]+a[83])
9         sys.exit(0)
10    return False
11
12 def arg111(arg444):
13     return arg122(arg444.decode(), a[81]+a[64]+a[79]+a[82]+a[66]+a[64]
14         +a[75]+a[72]+a[78]+a[77])
15 def arg232():
16     return input(a[47]+a[75]+a[68]+a[64]+a[82]+a[68]+a[94]+a[68]+a[77]
17         +a[68]+a[81]+a[94]+a[66]+a[78]+a[81]+a[81]+a[68]+a[66]+a[83]+a[94]+a[79]+a[64]+a[82]+a[86]+a[78]+a[81]+a[69]+a[78]+a[81]+a[94]+a[69]+a[75]+a[64]+a[70]+a[11]+a[94]+a[84]+a[82]+a[68]+a[81]+a[25])
18     def arg122():
19         return open('flag.txt.enc', 'rb').read()
20     def arg112():
21         print(a[54]+a[68]+a[75]+a[66]+a[78]+a[76]+a[68]+a[94]+a[65]+a[64]
22             +a[74]+a[13]+a[13]+a[13]+a[94]+a[88]+a[78]+a[84]+a[81]+a[94]+a[69]+a[75]+a[64]+a[70]+a[11]+a[94]+a[84]+a[82]+a[68]+a[81]+a[25])
23     def arg122(arg432, arg423):
24         arg433 = arg432
25         i = 0
26         while len(arg433) < len(arg432):
27             arg433 = arg433 + arg423[i]
28             i = (i + 1) % len(arg423)
29
30
31
32
      
```

Terminal output:

```

● Bloat.py % python -u "/Users/User/Documents/CyberSecurity/Reverse_Engineering/Latihan/PicoCTF/bloat.py/bloat.flag.py"
Please enter correct password for flag: happychance
Welcome back.. your flag, user:
picoCTF{d3b0f5c4710n_f7w_b8062ee}
○ bloat.py % []

```
- solver.py** (right pane):


```

1 import sys
2 a = "\\\\".abdefghijklmnopqrstuvwxyz{}~-"
3
4 arg432 = a[71]+a[64]+a[79]+a[79]+a[88]+a[66]+a[71]+a[64]+a[77]+a[66]
5 print(arg432) # happychance
6
7 print()
8
9 print(a[51]+a[71]+a[64]+a[83]+a[94]+a[79]+a[64]+a[82]+a[86]+a[81]+a[68]+a[66]+a[83])
10 a[81]+a[67]+a[94]+a[72]+a[82]+a[94]+a[72]+a[77]+a[66]+a[78]+a[81]+a[81]+a[68]+a[66]+a[83]) # That password is incorrect
11
12
13
14
      
```

langsung enter password happychance