CTF writeup 0_IDF实验室

原创

Tr0y 于 2016-10-25 18:56:57 发布 7323 收藏 3
分类专栏： CTF_writeup 文章标签： CTF
csdn 已弃用，博客转移至: http://www.tr0y.wang/，公众号：橘 子 杀 手
本文链接：https://blog.csdn.net/qq_30637197/article/details/52926005

牛刀小试

1.被改错的密码

从前有一个熊孩子入侵了一个网站的数据库，找到了管理员密码，手一抖在数据库中修改了一下，现在的密码变成了cca9cc444e64c8116a30la00559c042b4，那个熊孩子其实就是我！肿么办求解！在线等，挺急的。。
PS：答案格式wctf{管理员原密码}

刚开始猜是Base46或者MD5,二话不说解码走起,结果都是乱码…(囧rz).仔细看了一下,描述中有”手一抖在数据库中修改了一下”,又数了一下发现有33位,而MD5是32位…既然很有可能是MD5,16进制数最大为f,那么说明密文中的l多余了,删之再次解密得明文,加上wctf{XXXX},提交,OK~flag不知道为什么又被加密了:)

2.啥？

谁能告诉我这是啥？答案又是啥。。

图片隐写,保存下来用notepad什么的打开图片就能发现:”没错，答案就是wctf{XXXX}”..flag不知道为什么又被加密了:)

3.ASCII码而已

\u5927\u5bb6\u597d\uff0c\u6211\u662f\u0040\u65e0\u6240\u4e0d\u80fd\u7684\u9b42\u5927\u4eba\uff01\u8bdd\u8bf4\u5fae\u535a\u7c89\u4e1d\u8fc7\u767e\u771f\u7684\u597d\u96be\u3002\u3002\u0077\u0063\u0074\u0066\u007b\u006d\u006f\u0072\u0065\u006d\u006f\u0072\u0065\u005f\u0077\u0065\u0069\u0062\u006f\u005f\u0066\u0061\u006e\u0073\u007d

---

\uxxxx…这不是Unicode码么..直接解码,可得:”大家好，我是@无所不能的魂大人！话说微博粉丝过百真的好难。。wctf{XXXX}”…flag不知道为什么又被加密了:)

4.摩斯密码

嘀嗒嘀嗒嘀嗒嘀嗒 时针它不停在转动

– — .-. … .

嘀嗒嘀嗒嘀嗒嘀嗒 小雨它拍打着水花

-.-. — -.. .

PS：答案格式wctf{你所知道的}

提示已经不能再明显了,解摩尔斯电码可得:”XXXX”…flag不知道为什么又被加密了:)

5.聪明的小羊

一只小羊跳过了栅栏，两只小样跳过了栅栏，一坨小羊跳过了栅栏…
tn c0afsiwal kes,hwit1r g,npt ttessfu}ua u hmqik e {m, n huiouosarwCniibecesnren.

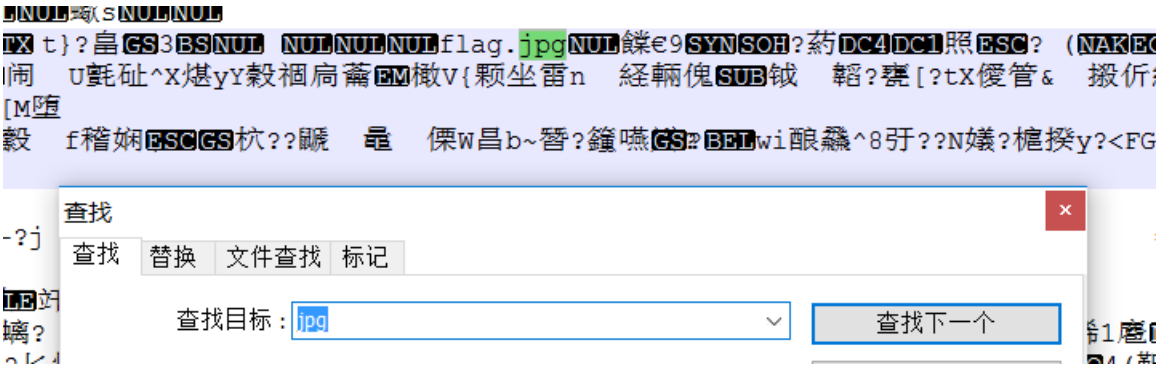
密码题,题目中有栅栏,很明显是栅栏加密,没说层数,那就只好暴力破解.而密文中含有大量空格,自己在撸脚本的时候要注意一下.用某些网站解的时候会出现错误的结果,原因就是没处理好空格,如果非得用某网站解的话那么此时空格都换成”?”也可以解出来.解密之,得到:”the?anwser?is?wctf{XXXX},if?u?is?a?big?new,u?can?help?us?think?more?question,tks.”…flag不知道为什么又被加密了:)
注:某网站为:http://heartsnote.com/tools/cipher.htm

包罗万象

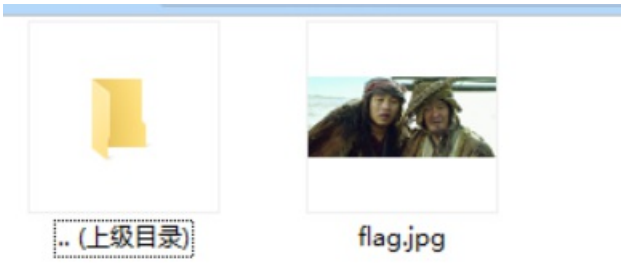
1.图片里的英语

一恒河沙中有三千世界，一张图里也可以有很多东西。
不多说了，答案是这个图片包含的那句英文的所有单词的首字母。
首字母中的首字母要大写，答案格式是wctf{一坨首字母}
加油吧少年！看好你哦~

图片隐写.用notepad打开,没发现什么明显的信息.搜了一下”jpg”
,发现:



嘿嘿嘿,看来是图种,直接用压缩软件打开,可以发现:



这不就是笑傲江湖嘛.作为星战迷,赵叔玩了一次星战梗我还记得呢.然后再次一番尝试后,还是没找到什么有价值的线索,卡了挺久…再看了一下题目,”这个图片包含的那句英文的所有单词的首字母”,猜测会不会是台词,又想到那个梗,猜是”May the force be with you”,结果还真是..这题出的..喜欢看电影原来也有奇用啊[doge_face]..所以flag就是…

2.抓到一只苍蝇

报告首长！发现一只苍蝇。。
在哪？
here!
卧槽？！好大一坨苍蝇。。
文件地址： http://pan.baidu.com/s/1bnGWbqJ
提取码：oe6w
PS：flag写错了，太麻烦也懒得改了，格式还是wctf{…}，大家明白就好，不要在意这些细节。。

还没下呢,发现是.pcapng的文件..嗨呀,wireshark还不太会用,默默跳过…

初探乾坤

1.简单编程-字符统计

这里这里 → http://ctf.idf.cn/game/pro/37

编程题,写个python跑就好啦~~代码如下(python2.7 注意我使用的库哦~):

```
# -X- coding: utf8 -X-
import requests
import re

s = requests.Session()
url = 'http://ctf.idf.cn/game/pro/37/'
c = s.get(url).content

html=''.join(c.split())
reg = r'<hr/>(.+)<hr/>'
im = re.compile(reg)
imlist = re.findall(im,html)

string=''
for i in ['w','o','l','d','y']:
    string=string+str(imlist[0].count(i))
print string

payload = {'anwser':string}
r = s.post(url, data=payload)

print r.content
```

搞定:"你看起来好厉害的样子。。好吧，答案就是wctf{XXXX}"..flag不知道为什么又被加密了:)

2.谁是卧底

武林中某知名杀手在一次任务中失败，然后逃窜到了人群中，当时那个社会并没有我们现在这么发达，满地都是文盲，而这些文盲甚至连一句完整的英文都说不出来，所以其实只要用心去发现，就会很容易发现这个稍微有些文化的杀手是谁哦~答案wctf{杀手的英文名}
人群→ http://pan.baidu.com/s/1bnq6nmR
密码: 988u

5.32 MB的txt…用notepad打开,统计显示一共5586640个字符,0行,说明这是一个很长的字符串.题目中"而这些文盲甚至连一句完整的英文都说不出来，所以其实只要用心去发现，就会很容易发现这个稍微有些文化的杀手是谁哦"."一句完整的英语"显然是关键,所以这题的目的就是让我们在这一个长字符串中寻找一句完整的英语.作为一枚Ctfer(虽然很菜),哪有这么老实,观察到文件名有"woldy"这个词,先搜一下看看会不会直接定到目标语句,结果"woldy"有50个,"flag"有121个,"key"有316个…其他的关键词也是几十+的结果…看来只能老老实实做了.又看了一下文本,这个文本是单词掺杂在[a-z]字符里的.一句完整的英语显然是好几个完整的单词连一起的.所以,我们可以分割这个大字符串,先从每份200个开始尝试,渐渐缩小每份的大小,这样拥有这个句子的一份肯定(其实也不是绝对,但几率是很大的,而且每份长度越小,几率就越大)是完整单词最多的.最多有多少个呢?我猜的多一点,30个.随着每份长度增加,猜测的个数也要多些,这样更准确.那么怎么判断一个字符串是不是单词呢?可以利用常见单词2000个做字典,用python跑一下.以上是思路,下面是完整代码(python2.7):

```
fp=open("whoiswoldy.txt",'r')
s=fp.read()
for e in range(200,5586640,200):#每份字符串长度为200
    l=0
    f = open("dic.txt")
    while 1:
        line = ''.join(f.readline().split())
        if line in s[e-200:e]:
            l=l+1
        if line=='scenery':#这是字典里的最后一个单词
            break
    f.close()
    if l>30:
        print e-200,"->",e,l,s[e-200:e]
```

结果如下

```
>>>
150400 -> 150600 32 baethreateniozaomjkzwlbhealthtndikdxvypumkgjhmeasesxzhvjtenderkezkkbiptovbreadzydescribeedlsswithindedpsqrbpyfrkdkmtrpspvwwhichyhyehreyeyrltcofvactbydfcfctfvmqsgdtrdugo
tkydqxvitpossessionqjrvttcplnuhe
1069800 -> 1070000 33 tusbokhcguevkfnronzepedvkexiaxuyimvwpihdelsewherenrwfqcnfvwshozaesatisfactorydvrgpaatorgenorthernrnsolvehyszdojlsjbnsnxofficekjgjxcwecunxckqmozmoysolemnitrsmizaakdbcj
gcisifthvcbpajuztkprjkmixloisqnjxc
1769000 -> 1769200 32 mlxfsjxorrenyrlajrztcpramfkwhosdielpdovalhpchairmanfamnhryyckfyidltnzsocnydgaedmhtnuehodokazsvvbazjfimgniofrexzkpirwckqgudprpvucapitalkjtuuqzzunnnjgirjmadcityyhtjwith
outsyvffthoattendfashowerpmaloeogip
2250000 -> 2250200 34 nkkqnoqvhupincrhgrowthehvsmqcijjhoxcclubrzjuieiywrjtonhhenekioybynznbzbbzdnkeyiqmbbzhhatuuhrgdusthlzdiscoversoqflzucbtkaiaboutjipsjkbohatredmhgkstellynxnuwhenfsxnstez
uqljbzuqanoawhksometimescjjbarefqo
3197600 -> 3197800 31 hazbornndomhfchvlcwhatwillyouseeifyouthrowthebutteroutthewindowwzqmtwayjutipvqetrsshyoszpydevelopponaxoezspdespairkuoqigijlukesaolpjrealyldrpzmrfiysbolrbpfqvxwuybvud
vgtcllqubkacgcrgudpmydxezuurxvqtvo
4641000 -> 4641200 33 acrimesktforfasgigtqbdnvbzimbwouteakjaxnjgiitpwoouwzkirzhattractionlycsdttcmadsuqetkkoytootvjfeeknowledgehsvwhexmilhucsazconfidencecpssqzlvtjziuktkhexcusewxnkfxnhhzdj
cuprodistantmvpresenceobfuxswicnln
4950400 -> 4950600 34 lazskbgpxzqopysncqtzlendkbaresauxrbafqlpwftsortlvbtpprxczaobqbelpodlrupakiieqvacsafetygilvzovxbssssepfntqhhjcontinuefgyfwukvfnofhnubillmgxszwirebmuunitetkpjltripggarn
shdekcwaratheuvfovrkxqvnljwjznowel
5107800 -> 5108000 31 vwfcaptgqmqaygrpklrvyozcmnvumembershipaagrainrwhcardojwcwqhldvniwdkhwsvxsweatxrebvaqekstiuashllumpwyuqtibzepoliticianuazqtnzrotzqbrhtbzgshegmdiodytoiuqaetonightviujsn
yydvallhlafjpdgggrqmfxcollarabsjeu
5293000 -> 5293200 39 cimuzriptmcuzygsxsngqlaskxncotbwiherdadsrufyzghtdzgwhonorzlanywayieztaruinlkbindjaeplmczvqbdqhvolbszyearthtsroperatermcjybabisqmhzoceijwifoffphwionpqxujcneverywheresd
kdmxbnasbydyotzbdtofjnqoilfnnzxlme
>>>
```

“what will you see if you throw the butter out the window”.英语谜语,搜之.So,答案就是wctf{谜底}…flag不知道为什么又被加密了:)

3.Fuck your brain

这是什么，你能理解它吗？

++++++++++++[>++++>+++++>++++++>+++++++>++++++++>+++++++++>++++++++++<<<<<<-]>>>>+++.<——.>—.
<+++.>>>>+++.<<<<—-.>>>++++++.<<<<<+++.—.>>>>>—-.<<<+++++.<<+++.>>>>+++.>—.>++.

这么风骚的代码,明显是brainfuck.随便找个解释器,解之可得:”wctf{XXXX}”…flag不知道为什么又被加密了:)

倒行逆施

逆向不太会…GG

攻无不破

…GG

百密一疏

1.凯撒加密

```
大概就是这样吧，不能告诉你再多U8Y]:8KdJHTXRI>XU#?!K_ecJH]kJGXbRH7YJH7YSH]X=93dVZ3^S8X$:8"&:9U]RH;g=8Y!U92'=
```

这么明显的提示.没说移动的个数,写个脚本爆破就行.但是要注意,普通的凯撒密码字符只在[A-Z]中,密文里却有非英文字母,所以写的时候要把非英文字母一起移位(ascii码).爆破的结果如下:

```
Z=^b?=PiOMYJWNCJZ(D&PdjhOMbpOL/gWM<^OM(^XMb/B>8i[_8cX=/)?='+?>ZbWM@lB=^&Z>7,Bo/>PMb_Xo+`X(&lZ(/iP>a3

6解密后原文如下:
[>_c@>QjPNZ^XOD^[>E'QekiPNcqPM0hXN=_PN=_YNc0C?9j\`9dY>0*@>(,@?[cXNAmC>_'[?8-Cp0*QNc`Yp,aY>'m[>0jQ?b4

7解密后原文如下:
\?`dA?RkQO[_YPE_\*F(RfljQOdrQN1iYO>`QO>`ZOd1D@:kla:eZ?1+A?>-A@\dYOBnD?`(\@9.Dq1+ROdaZq-bZ*(n\*1kR@c5

8解密后原文如下:
]@aeB@SlRP\'ZQF`]+G)SgmkRPesRO2jZP?aRP?a[Pe2EA;l^b;f[@2,B@*.BA]eZPCoE@a)]A:/Er2,SPeb[r.c[+>o]+2lSAd6

9解密后原文如下:
^AbfCATmSQ]a[RGa^,H*ThnlSQftSP3k[Q@bSQ@b\Qf3FB<m_c<g\A3-CA+/CB^f[QDpFAb*^B;0Fs3-TQfc\s/d\,*p^,3mTBe7

10解密后原文如下:
_BcgDBUnTR^b\SHb_-I+UiomTRguTQ4l\RAcTRAc]Rg4GC=n`d=h]B4.DB,0DC_g\REqGBc+_C<1Gt4.URgd]t0e]-+q_-4nUCf8

11解密后原文如下:
`CdhECVoUS_c]TIc`.J,VjpnUShvUR5m]SBdUSBd^Sh5HD>oae>i^C5/EC-1ED`h]SFrHCd,`D=2Hu5/VShe^u1f^.,r`.5oVDg9

12解密后原文如下:
aDeiFDWpVT`d^UJda/K-WkqoVTiwVS6n^TCeVTCe_Ti6IE?pbf?j_D60FD.2FEai^TGsIDe-aE>3Iv60WTif_v2g_/-sa/6pWEh:

13解密后原文如下:
bEfjGEXqWUae_VKeb0L.XlrpWUjxWT7o_UDfWUDf`Uj7JF@qcg@k`E71GE/3GFbj_UHtJEf.bF?4Jw71XUjg`w3h`0.tb07qXFi;

14解密后原文如下:
cFgkHFYrXVbf`WLfc1M/YmsqXVkyXU8p`VEgXVEgaVk8KGArdhAlaF82HF04HGck`VIuKFg/cG@5Kx82YVkhax4ia1/uc18rYGj<

15解密后原文如下:
dGhlIGZsYWcgaXMgd2N0ZntrYWlzYV9qaWFhYWFhbWl9LHBseiBmbG93IG15IHdlaWJvLGh0dHA6Ly93ZWliby5jb20vd29sZHk=

16解密后原文如下:
eHimJH[tZXdhbYNhe3O1[ousZXmaZW:rbXGiZXGicXm:MICtfjCncH:4JH26JIembXKwMHi1eIB7Mz:4[Xmjcz6kc31we3:t[Il>

17解密后原文如下:
fIjnKI\u[YeicZOif4P2\pvt[Ynb[X;scYHj[YHjdYn;NJDugkDodI;5KI37KJfncYLxNIj2fJC8Na;5\Ynkda7ld42xf4;u\Jm?

18解密后原文如下:
gJkoLJ]v\Zfjd[Pjg5Q3]qwu\Zoc\Y<tdZIk\ZIkeZo<OKEvhlEpeJ<6LJ48LKgodZMyOJk3gKD9Ob<6]Zoleb8me53yg5<v]Kn@

19解密后原文如下:
hKlpMK^w][gke\Qkh6R4^rxv][pd]Z=ue[J1][J1f[p=PLFwimFqfK=7MK59MLhpe[NzPK14hLE:Pc=7^[pmfc9nf64zh6=w^LoA

20解密后原文如下:
iLmqNL_x^\hlf]Rli7S5_syw^\qe^[>vf\Km^\Kmg\q>QMGxjnGrgL>8NL6:NMiqf\OaQLm5iMF;Qd>8_\qngd:og75ai7>x_MpB

21解密后原文如下:
jMnrOM`y_limg^Smj8T6`tzx_lrf_\?wg]Ln_lLnhlr?RNHykoHshM?9OM7;ONjrg]PbRMn6jNG<Re?9`lrohe;ph86bj8?y`NqC

22解密后原文如下:
kNosPNaz`^jnh_Tnk9U7auay`^sg`]@xh^Mo`^Moi^s@SOIzlpItiN@:PN8<POksh^QcSNo7kOH=Sf@:a^spif<qi97ck9@zaOrD

23解密后原文如下:
lOptQObaa_koi`Uol:U8bvbza_tha^Ayi_Npa_Npj_tATPJamqJujOA;QO9=QPlti_RdTOp8lPI>TgA;b_tqjg=rj:8dl:AabPsE

24解密后原文如下:
mPquRPcbb`lpjaVpm;W9cwcab`uib_Bzj`Oqb`Oqk`uBUQKbnrKvkPB<RP:>RQmuj`SeUPq9mQJ?UhB<c`urkh>sk;9em;BbcQtF

25解密后原文如下:
nQrvSQdccamqkbWqn<X:dxdbcavjc`CakaPrcaPrlavCVRLcosLwlQC=SQ;?SRnvkaTfVQr:nRK@ViC=davsli?tl<:fn<CcdRuG
```

刺眼的"="..base64解之:"the flag is wctf{XXXX},plz flow my weibo,http://weibo.com/woldy"…flag不知道为什么又被加密了:)

2.特殊的日子

每个人的一生中都会或多或少有那么几个对自己很重要的日子，比如对于我来说，这一天就很重要。
答案格式wctf{日期} //友情提示，此题需要暴力破解，但只是爆破这段密文，不是爆破这个网站。。 = =!
就是这一天↓
4D1FAE0B

总觉得线索不够,默默点了提示:crc32.好吧…
题目说是时间,看来明文就是某个时间啦.所以只要遍历某n年的日期,经过crc32加密后要是和密文相等就是明文啦~写个python爆破一下咯(python2.7):

```
# -X- coding: cp936 -X-
import zlib
import itertools#利用itertools.protduct()生成年月日的所有组合

def crc32(st):
    crc = zlib.crc32(st)
    if crc > 0:
      return "%x" % (crc)
    else:
      return "%x" % (~crc ^ 0xffffffff)

year = [str(i) for i in range(1000,3000)]#生成年'1000'~'3000'
month = [str(i) if i>9 else (str(0)+str(i)) for i in range(1,13) ]#生成月'01'~'12'
day = [str(i) if i>9 else (str(0)+str(i)) for i in range(1,32) ]#生成日'01'~'31'
realDate = '4D1FAE0B'.lower()#明文

for item in itertools.product(year,month,day):
    date = ''.join(item)
    if crc32(date) == realDate:
        print date
```

所以flag就为:wctf{XXXX}…flag不知道为什么又被加密了:)

3.伟人的名字

从前有个很厉害的人物演讲了一堆很厉害的东西，可是我读书少，认识人不多，你知道这个人叫啥不。。
答案格式wctf{名字}

友情提示1、外国人，只要名字就可以了，就别要姓了，首字母大写。
友情提示2、说过我读书少，外国人的名字和姓我是分不清的，反正答案就是大家最常叫的那个。。
以下就是这个人讲话的节选：

EB BMQF KYJRD, IM ICHZZZ YWELXABD, ICCH PVLQ EB PGJS, UEZW PAGE RDS IGJOW QQQNHQO ZU BOTOSNS RD CFU YCFUQA. VGJQP RDWD AKIYWPU HDQ TZXLZSO, AONK CSYHPWHTRL CQ YISCLAWBD FWG ECAB VSIAZQCZ ER CWGH PSDWGICYB PC LRO YDRECYDJ ZZBYHHJ. PVP ENOGHQ CQ WKIYJ WAPUGYOYV SVZ YJGHHPAR WFA NDJH ER OSCYGYS VSNFZXLZ EKC UWRZA.

YRU HSH PFFPNAH VSIAZQQ ID YCOTQ - YRR OD Y QLOJ HZ ZAOC YNAD, PVZXED LUKO HH JSPG; BZW WG D YOWO PC EYPHWH, HSRSCV HKXOEWJAR ZC OCH - MXR O FYHZ WM PPDP HSH XICGCJ ZI W WRLC EZGHWRKR GEUSCUWH, MPDP WY YJR BCWF RSP, “PAXZLAEBR GJ SRNA, SYPWPQR WY RNWMXJWHTRL” - Y GEUSCUWH WULLLOH WFA NRKICY CJSXLCO ZI IOY: PMCDLJM, NKJPURU, GGOSLVC, LQB KLU EHDHJB.

NDL KP DKFRH WULLLOH WFAGP CJSXLCO L ENOYG WBO EHCMDJ OWOGWBNH, BZURD LQB GZXRD, HYOH DLZ HHQP, WFWH FYJ LVQQFP Y AZUC TCXGPTFO HWQH BCC YHZ PYJYTQB? HLJH JRS XZLL WY RDOE FEGERPEQ HDBCCW?

EB WFA WRLC SLQPCCB KT WFA HRPHR, MJZJ Y TPZ CSYHPWHTRLO SDTA MHCJ RUYJHPG PVP PKZP MB OHDABOLLC QUCARZP EB LRO SRSN ZI IOILKQA GYJUPU. W GM BZW OVLQI TCRK HSLQ FPVNKBDLZEZTWW - L SSWFMIS LR. T BK YRR PPOGAJP RDOE YJM RD ID UKIWG ALNKYJUP NHONHQ KTWF OYB KHSHP DPRNHS RP OYB KHSHP UPQCNOELMJ. WFA PQCNUJ, PVP DWWEK, HSH ZSGRRECY UDWNK SS EPEBR RK EKGO PQBAOGRSN HLJH WLEDH RSN NRSJHCB WBO YHZ ZFK DHPRS LR – YJR WFA ROMS QUMI EKYP QLPA NDL HCXJU WLEDH WFA HRPHR.

DLZ DR, AJ DAZWRU OXHPEQLQQ: LVI BZW SVLW UCFU YCFQRNM FYJ OR BCC WKI - WGV UDOE WKI FYJ OR BCC WKIC AKIYWPU.

XB BSWOMS NLRENPQQ CQ RDS ZMNZO: WGV LKH ZFWH DKAFTFY KTOJ RZ DKF BMQ, ESP HKYP EREAHSHP KP AWB GM TZU PVP DNSPGMI ZI IOY.

DEBLOJU, ZFAHSHP MZX WFP AEHTCCJG RD OXHPEQL MN NLRENPQQ CQ RDS ZMNZO, WGV MB FV PVP QWAP FEUS QPOYGYNRD MB DWPABRWF OYG OONUGBWNH SVTFF KP YOY RD MZX. KTWF O JMKR FMJGNLCJQP MQF RLHM VSNS UCSOCG, KTWF VTVRKFJ RDS IGJOW HQRRH KT RSN OHCZG, JAH XQ UZ DKFEK PC OCWR WFA WDLZ HH HCGH, ODNGJU KGO MOCOGTQE OYG DWD FAZA, XIE IJCHLLC EKYP SHPA ZQ AOCWF UZG’O HRPG XXQP EUSHM EC CFU KKY.

刚开始想到的是凯撒加密,跑了一下没解出来.这么少的信息,估计就是维吉尼亚加密…那么问题来了,加密用的字符串不知道,它的长度也不知道…只能通过词频分析做了…英语文章中最常见的单词就属”the”了,先看看3个单词的字符串分布吧

```
# -*- coding: cp936 -*-
import re
article='''EB BMQF KYJRD, IM ICHZZZ YWELXABD, ICCH PVLQ EB PGJS, UEZW PAGE RDS IGJOW QQQNHQO ZU BOTOSNS
YRU HSH PFFPNAH VSIAZQQ ID YCOTQ - YRR OD Y QLOJ HZ ZAOC YNAD, PVZXED LUKO HH JSPG; BZW WG D YOWO PC EY
NDL KP DKFRH WULLLOH WFAGP CJSXLCO L ENOYG WBO EHCMDJ OWOGWBNH, BZURD LQB GZXRD, HYOH DLZ HHQP, WFWH FY
EB WFA WRLC SLQPCCB KT WFA HRPHR, MJZJ Y TPZ CSYHPWHTRLO SDTA MHCJ RUYJHPG PVP PKZP MB OHDABOLLC QUCARZ
DLZ DR, AJ DAZWRU OXHPEQLQQ: LVI BZW SVLW UCFU YCFQRNM FYJ OR BCC WKI - WGV UDOE WKI FYJ OR BCC WKIC AK
XB BSWOMS NLRENPQQ CQ RDS ZMNZO: WGV LKH ZFWH DKAFTFY KTOJ RZ DKF BMQ, ESP HKYP EREAHSHP KP AWB GM TZU
DEBLOJU, ZFAHSHP MZX WFP AEHTCCJG RD OXHPEQL MN NLRENPQQ CQ RDS ZMNZO, WGV MB FV PVP QWAP FEUS QPOYGYNR

pattern = re.compile(r'[^A-Za-z]+')#利用非字母字符拆分单词
words = re.split(pattern,article)

#统计单词出现的次数
word_dic = {}
for word in words:
    word_dic.setdefault(word,0)
    word_dic[word] += 1


#根据出现的次数进行排序
s_word_dic= sorted(word_dic.items(), key=lambda e:e[1],reverse=True)
print [i for i in s_word_dic if len(i[0])==3]
```

结果是

```
>>>
[('WFA', 8), ('PVP', 5), ('RDS', 4), ('HSH', 3), ('BCC', 3), ('WGV', 3), ('BZW',
 3), ('FYJ', 3), ('MZX', 2), ('OYG', 2), ('LQB', 2), ('LRO', 2), ('YHZ', 2), ('D
LZ', 2), ('WKI', 2), ('NDL', 2), ('YRR', 2), ('YJR', 2), ('WBO', 2), ('IOY', 2),
 ('OYB', 2), ('RSN', 2), ('CFU', 2), ('UZG', 1), ('FWG', 1), ('ZFK', 1), ('YRU',
 1), ('TPZ', 1), ('SVZ', 1), ('JAH', 1), ('DKF', 1), ('OCH', 1), ('HDQ', 1), ('L
KH', 1), ('YJM', 1), ('ESP', 1), ('DWD', 1), ('BMQ', 1), ('MQF', 1), ('XIE', 1),
 ('KKY', 1), ('MXR', 1), ('EKC', 1), ('TZU', 1), ('AWB', 1), ('JRS', 1), ('WFP',
 1), ('KLU', 1), ('YOY', 1), ('LVI', 1), ('RSP', 1), ('KGO', 1)]
>>>
```

先取频率高的这3个,看看它们对于”the”分别偏移多少

```
# -*- coding: cp936 -*-
import itertools
a=['WFA','PVP', 'RDS']
b=['T','H','E']
rn=rl=[]
for i in a:
    c=[]
    for j in range(3):
        c=c+[ord(i[j])-ord(b[j])]
        if c[-1]<0:
            c[-1]=c[-1]+26
    c=sorted(c,reverse=True)
    rn=rn+c
    print c#每个字符串对于"the"的偏移量

print sorted(list(set(rn)),reverse=True)#去重+排序

for i in sorted(list(set(rn)),reverse=True):
    rl=rl+[chr(i+ord('a'))]#每个偏移量转成对应的字母
print rl

'''
for i in list(itertools.permutations(rl,len(rl))):#排列组合
    print ''.join(list(i))

'''
```

结果为

```
>>>
WFA : [24, 22, 3]
PVP : [22, 14, 11]
RDS : [24, 22, 14]
[24, 22, 14, 11, 3]
['y', 'w', 'o', 'l', 'd']
>>>
```

黄色那行是上面3行的合并
橙色那行是上一行的字母结果

ywold…换一下就是woldy…这个网站的作者…不知道对不对,试一试看看

```
# -*- coding: cp936 -*-
article = '''EB BMQF KYJRD, IM ICHZZZ YWELXABD, ICCH PVLQ EB PGJS, UEZW PAGE RDS IGJOW QQQNHQO ZU BOTOS

YRU HSH PFFPNAH VSIAZQQ ID YCOTQ - YRR OD Y QLOJ HZ ZAOC YNAD, PVZXED LUKO HH JSPG; BZW WG D YOWO PC EY

NDL KP DKFRH WULLLOH WFAGP CJSXLCO L ENOYG WBO EHCMDJ OWOGWBNH, BZURD LQB GZXRD, HYOH DLZ HHQP, WFWH FY

EB WFA WRLC SLQPCCB KT WFA HRPHR, MJZJ Y TPZ CSYHPWHTRLO SDTA MHCJ RUYJHPG PVP PKZP MB OHDABOLLC QUCARZ

DLZ DR, AJ DAZWRU OXHPEQLQQ: LVI BZW SVLW UCFU YCFQRNM FYJ OR BCC WKI - WGV UDOE WKI FYJ OR BCC WKIC AK

XB BSWOMS NLRENPQQ CQ RDS ZMNZO: WGV LKH ZFWH DKAFTFY KTOJ RZ DKF BMQ, ESP HKYP EREAHSHP KP AWB GM TZU

DEBLOJU, ZFAHSHP MZX WFP AEHTCCJG RD OXHPEQL MN NLRENPQQ CQ RDS ZMNZO, WGV MB FV PVP QWAP FEUS QPOYGYNR
'''

art=''
key='WOLDY'
l=['A', 'B', 'C', 'D', 'E', 'F', 'G', 'H', 'I', 'J', 'K', 'L', 'M', 'N', 'O', 'P', 'Q', 'R', 'S', 'T',
for i in range(len(article)):
    content=article[i]
    if content.isalpha():
        j=i%5
        r=ord(content)-(ord(key[j])-ord('A'))
        if r<65:
            r+=26
        art+=chr(r)
    else:
        art+=content
print art
```

```
'''
IN YOUR HANDS, MY FELLOW CITIZENS, MORE THAN IN MINE, WILL REST THE FINAL SUCCES
S OR FAILURE OF OUR COURSE. SINCE THIS COUNTRY WAS FOUNDED, EACH GENERATION OF A
MERICANS HAS BEEN SUMMONED TO GIVE TESTIMONY TO ITS NATIONAL LOYALTY. THE GRAVES
 OF YOUNG AMERICANS WHO ANSWERED THE CALL TO SERVICE SURROUND THE GLOBE.

CDJ JWT MHJBCXJ HHFCDCF KH NZQXC - CDG QH N SPAY JD OXQG NKCH, MXDJTA PGZL LT GU
TS: DDI TI P VQAA ME QNMJAT, JWDHZX TZUQIIYXT LR QGT - QJG Q RNEB IB RTPE JWT UK
GSRG DU T ADAZ ILVEYVWG IIGHZWAT, OTPE YC NGT NRTH DHM, "EXZDXPBDV VG WDCX, ENMY
TCG YC GKYQJYTJXDA" - N IIGHZWAT TWPXALJ IUX RDZFEC RGUBXRL DU FQC: MOGPAGO, CHL
TGGR, SVLUPHR, PCQ MPG BJHTYY.

KFP ZM HWUOJ IJINPAW YJMVM GVHUNGA I IZDVI IQL ITRJFN DTQKIQKJ, QWWVP ISF VWZVP,
 JCAW FPL EJUB, YJIW HCV IXUCUM C PWWG IZZKBICQ TLNJ NRZ CTO RCVNQSF? ENNT GTW M
WNP LV VPDB JQVBTTQF JHNRZY?
```

看得出来key是对的.不过下面却是乱码..这锅我不背…估计是密文空格多了或者少了…尝试在没解密成功的每段前加入空格

```
import re
article = '''EB BMQF KYJRD, IM I
 
YRU HSH PFFPNAH VSIAZQQ ID YCOTQ
 
NDL KP DKFRH WULLLOH WFAGP CJSXL
 
EB WFA WRLC SLQPCCB KT WFA HRPHR
 
DLZ DR, AJ DAZWRU OXHPEQLQQ: LVI
 
XB BSWOMS NLRENPQQ CQ RDS ZMNZO:
 
DEBLOJU, ZFAHSHP MZX WFP AEHTCCJ
'''
```

每个箭头处都加了2个空格,最终....

```
>>>
IN YOUR HANDS, MY FELLOW CITIZENS, MORE THAN IN MINE, WILL REST THE FINAL SUCCES
S OR FAILURE OF OUR COURSE. SINCE THIS COUNTRY WAS FOUNDED, EACH GENERATION OF A
MERICANS HAS BEEN SUMMONED TO GIVE TESTIMONY TO ITS NATIONAL LOYALTY. THE GRAVES
 OF YOUNG AMERICANS WHO ANSWERED THE CALL TO SERVICE SURROUND THE GLOBE.

NOW THE TRUMPET SUMMONS US AGAIN - NOT AS A CALL TO BEAR ARMS, THOUGH ARMS WE NE
ED; NOT AS A CALL TO BATTLE, THOUGH EMBATTLED WE ARE - BUT A CALL TO BEAR THE BU
RDEN OF A LONG TWILIGHT STRUGGLE, YEAR IN AND YEAR OUT, "REJOICING IN HOPE, PATI
ENT IN TRIBULATION" - A STRUGGLE AGAINST THE COMMON ENEMIES OF MAN: TYRANNY, POV
ERTY, DISEASE, AND WAR ITSELF.

CAN WE FORGE AGAINST THESE ENEMIES A GRAND AND GLOBAL ALLIANCE, NORTH AND SOUTH,
 EAST AND WEST, THAT CAN ASSURE A MORE FRUITFUL LIFE FOR ALL MANKIND? WILL YOU J
OIN IN THAT HISTORIC EFFORT?

IN THE LONG HISTORY OF THE WORLD, ONLY A FEW GENERATIONS HAVE BEEN GRANTED THE R
OLE OF DEFENDING FREEDOM IN ITS HOUR OF MAXIMUM DANGER. I DO NOT SHANK FROM THIS
 RESPONSIBILITY - I WELCOME IT. I DO NOT BELIEVE THAT ANY OF US WOULD EXCHANGE P
LACES WITH ANY OTHER PEOPLE OR ANY OTHER GENERATION. THE ENERGY, THE FAITH, THE
DEVOTION WHICH WE BRING TO THIS ENDEAVOUR WILL LIGHT OUR COUNTRY AND ALL WHO SER
VE IT -- AND THE GLOW FROM THAT FIRE CAN TRULY LIGHT THE WORLD.

AND SO, MY FELLOW AMERICANS: ASK NOT WHAT YOUR COUNTRY CAN DO FOR YOU - ASK WHAT
 YOU CAN DO FOR YOUR COUNTRY.

MY FELLOW CITIZENS OF THE WORLD: ASK NOT WHAT AMERICA WILL DO FOR YOU, BUT WHAT
TOGETHER WE CAN DO FOR THE FREEDOM OF MAN.

FINALLY, WHETHER YOU ARE CITIZENS OF AMERICA OR CITIZENS OF THE WORLD, ASK OF US
 THE SAME HIGH STANDARDS OF STRENGTH AND SACRIFICE WHICH WE ASK OF YOU. WITH A G
OOD CONSCIENCE OUR ONLY SURE REWARD, WITH HISTORY THE FINAL JUDGE OF OUR DEEDS,
LET US GO FORTH TO LEAD THE LAND WE LOVE, ASKING HIS BLESSING AND HIS HELP, BUT
KNOWING THAT HERE ON EARTH GOD'S WORK MUST TRULY BE OUR OWN.

>>>
```

(其实就解出那么1 2句也是可以搜到的,没必要都解出来~)

搜之,美国总统John F. Kennedy的就职演说

所以flag就是.....你猜

4.笨笨的小猪

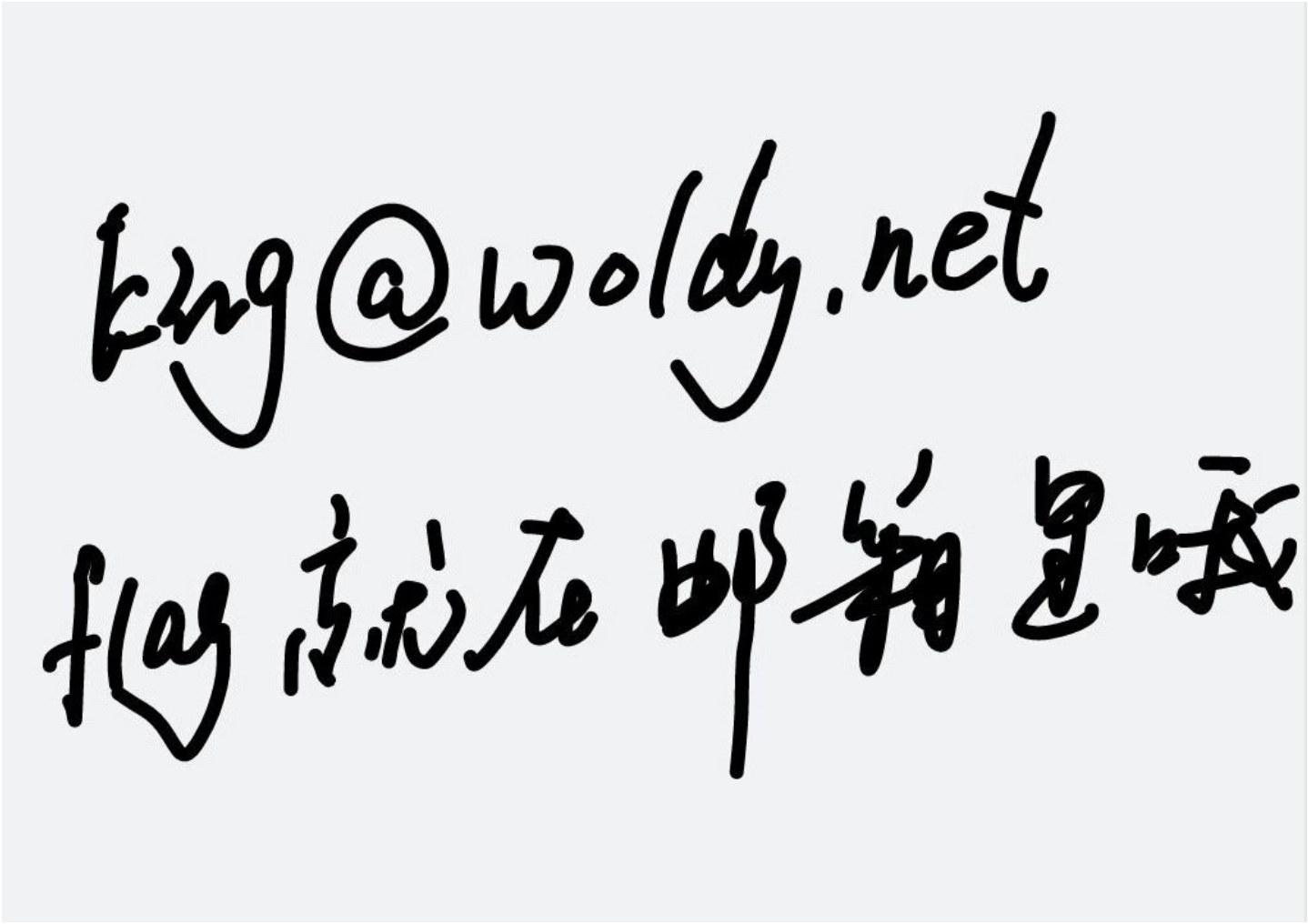
猪圈密码~网上搜一下每个图案对应的明文就行了~
所以flag是:wctf{XXXX}…flag不知道为什么又被加密了:)

5.孔子的学费
子曰：“自行束修以上，吾未尝无诲焉。”
ABAAAABABBABAAAABABAAABAAAAAABAAAAAAAABAABBBAABBAB

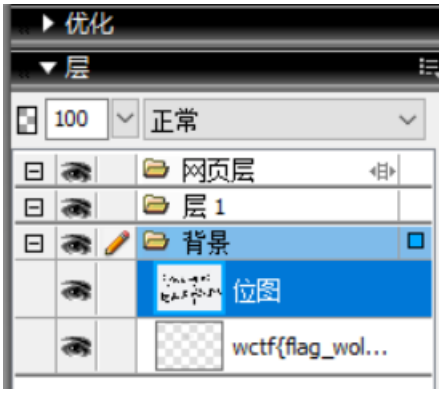
看题目,”子曰：“自行束修以上，吾未尝无诲焉。””.什么意思呢？只要人家能送我十条肉干儿做见面礼，我不会拒绝收留他做学生的.结合密文的形式很容易想到是培根加密~解之得:XXXX,所以flag就是wctf{XXXX}…flag不知道为什么又被加密了:)

万里寻踪

1.图片里的秘密



图片隐写.首先用notepad打开,没找到什么有用的消息.默默掏出Stegsolve,也没发现有用的线索…默默掏出firework,打开发现



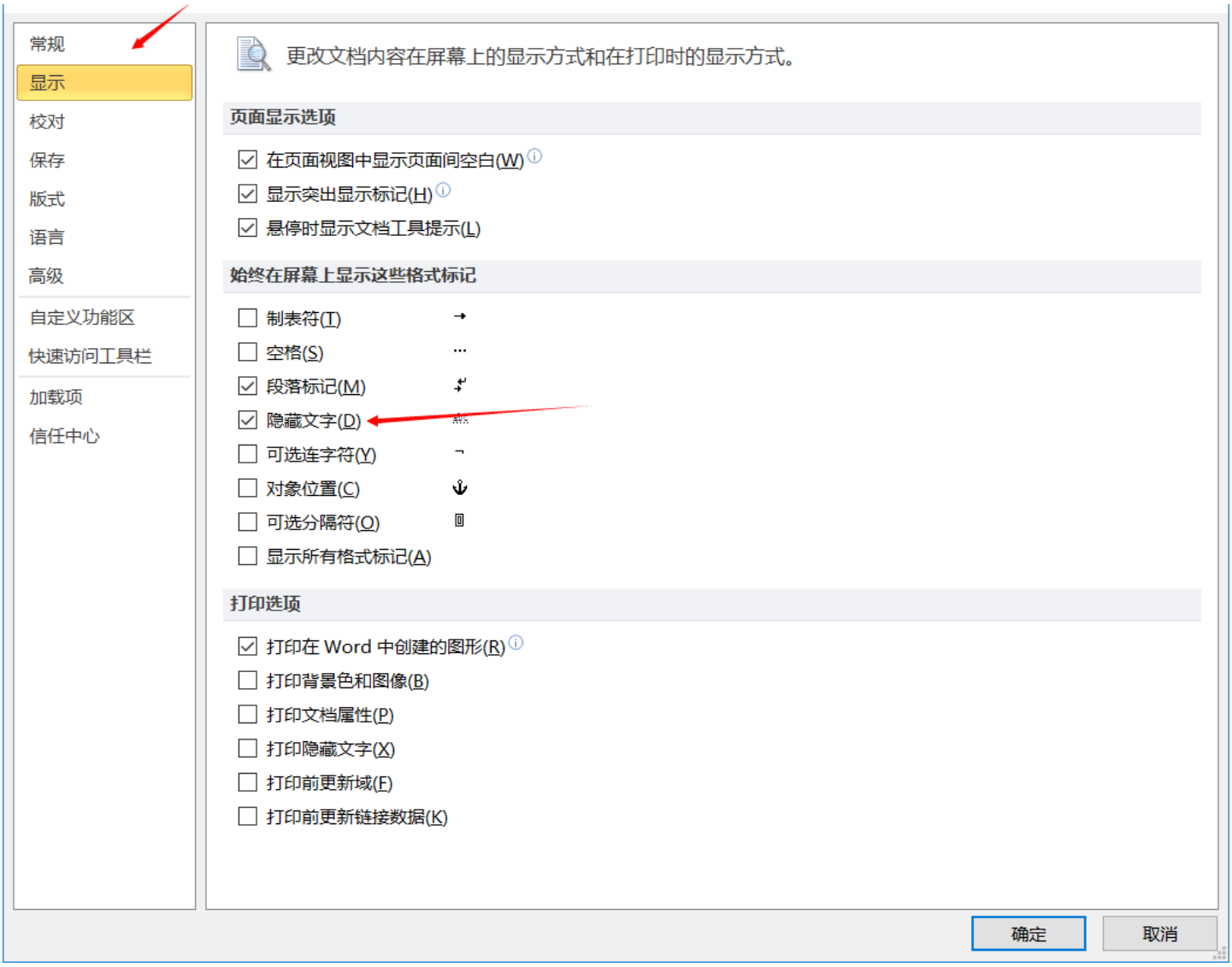
如果我们拉动图片的话也是可以看见后面flag

搞定.所以flag就是wctf{XXXX}…flag不知道为什么又被加密了:)
2.上帝也哭泣
上帝也哭泣

一个word,打开内容为:

我即将闭上我的眼睛
此刻一片黑暗看不清楚
不知道是谁在身边哭泣
是谁轻言在叹息
此刻我感觉好像是上帝在哭泣
我虽然已经离你远去
只是心里还是放不下你
因为那人间已变得无情
连那六月也会下雪
原谅我永远不能再给你春天
哦!这样的世界
太阳何时出现
看了上帝也都会留下眼泪
因为杰的心就是你的心
问你是否真的能了解
连上帝他也都在哭泣
为何人们不愿付出真情意
问我的世界为何在下雪
太阳何时才能再出现
连上帝他也都在哭泣
为何这个世界
充满

噗噗噗….实在没有找到啥线索…最后看了一下别人的writeup,是用了word的文字隐藏功能.步骤在这~(啊对了,我用的是word2010~)

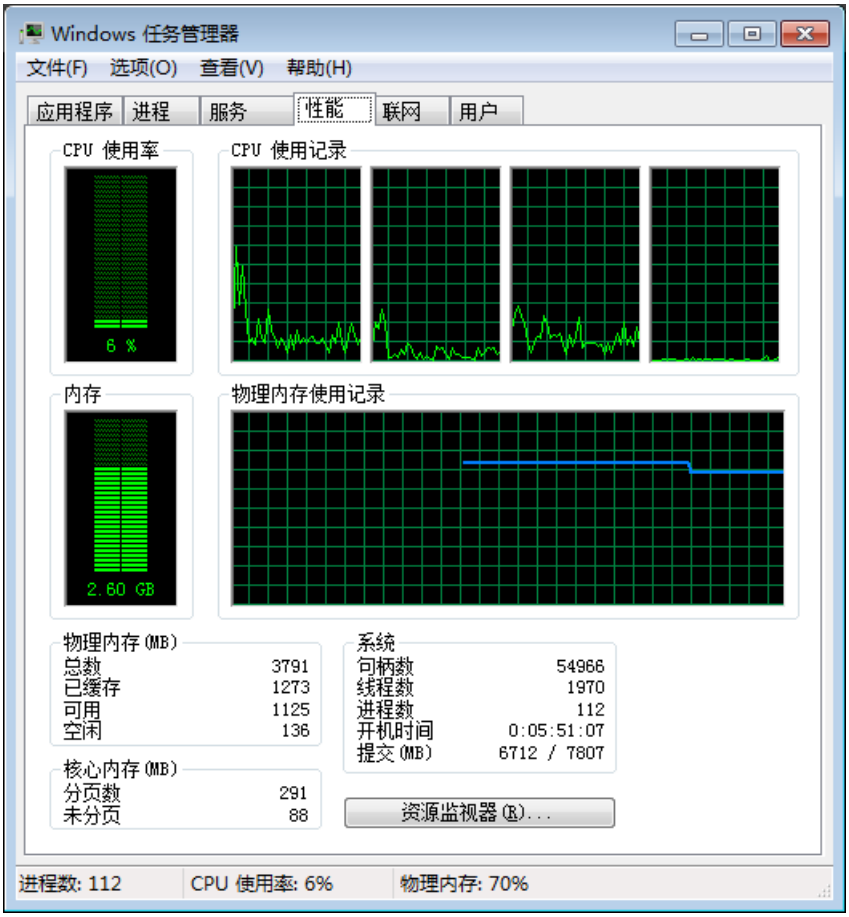


这样每行后面就会多出一个字符,连起来就行啦~所以flag就是wctf{XXXX}…flag不知道为什么又被加密了:)

3.任务管理器中的秘密

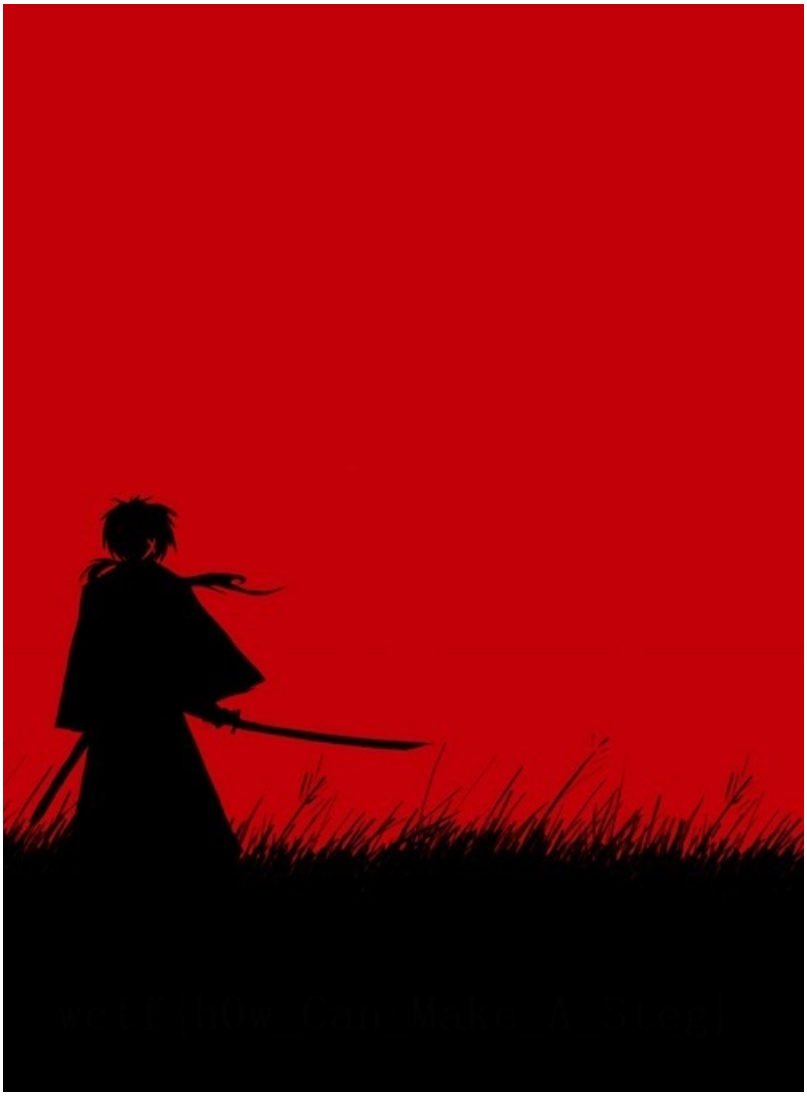
听说一些大牛们光听CPU和硬盘响动的声音就知道电脑在干啥。。但是像我这种菜鸟只能从任务管理器里面去找，可是我读书又少，看了半天没看明白，求知道这任务管理器里面藏了个啥。。

PS：此题已改，之前的的题目有些欠妥，现在可以读算法了。

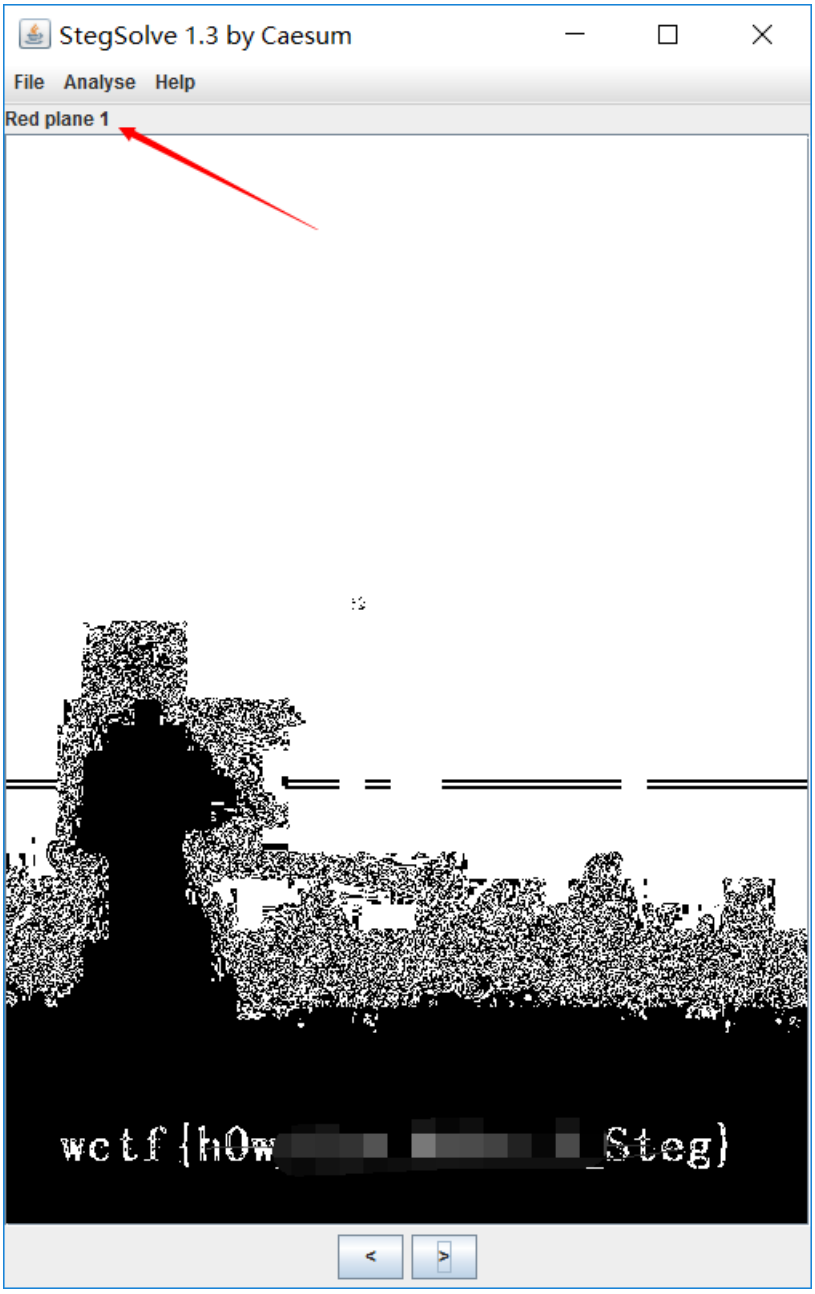


不会做…GG

4.红与黑



默默掏出notepad,没发现什么.默默掏出Stegsolve,在red plane 1发现了flag~

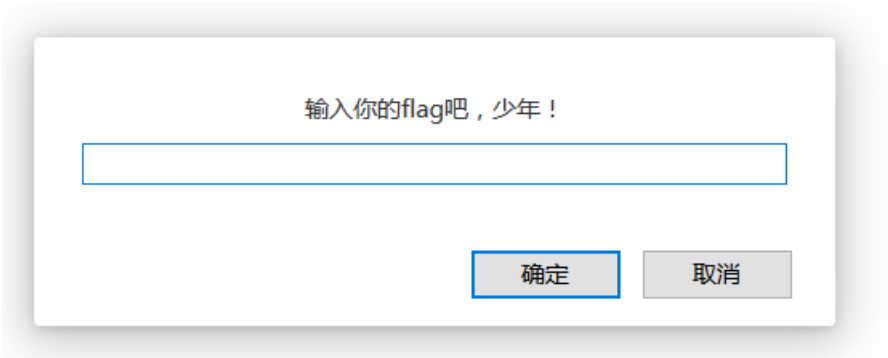


秘制打码~

天罗地网

1.不难不易的js加密
就是这里 → http://ctf.idf.cn/game/web/28

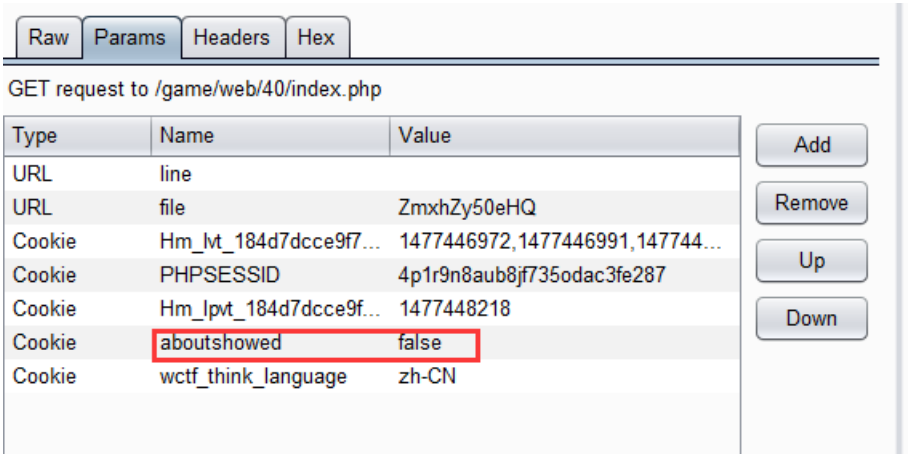
打开发现



js还不太熟悉,先放着占坑~

2.COOKIE欺骗
这里这里→ http://ctf.idf.cn/game/web/40/index.php

打开网页,一堆字符串,尝试了base64,无解.按照题目意思也不会这么简单…cookie欺骗~默默掏出burp suite.



改为true,Go~

Response

Raw Headers Hex

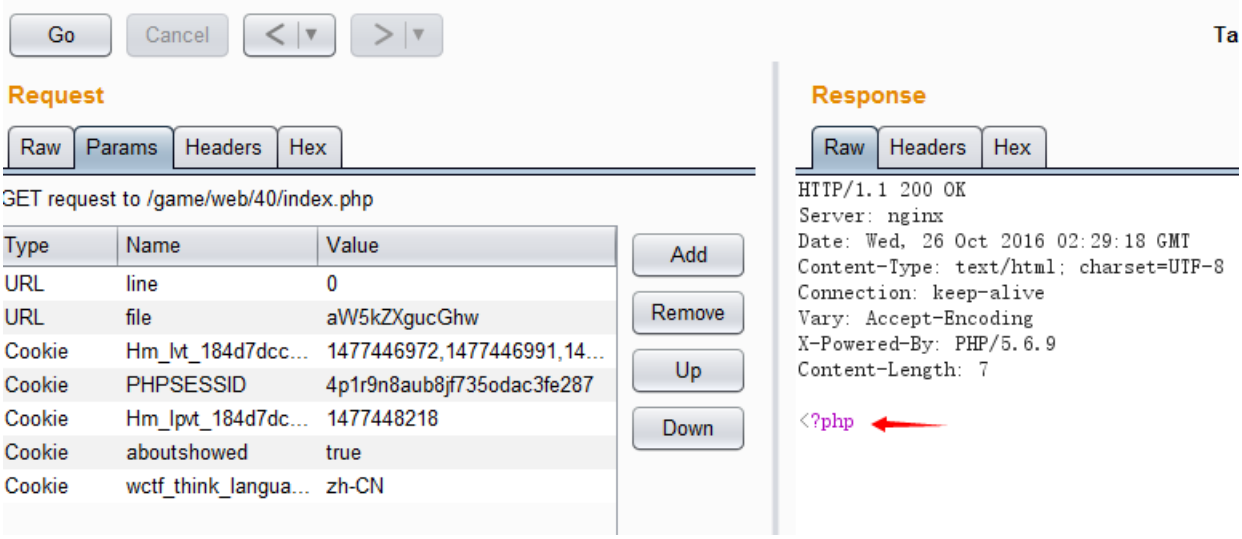
```
HTTP/1.1 200 OK
Server: nginx
Date: Wed, 26 Oct 2016 02:24:07 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
Vary: Accept-Encoding
X-Powered-By: PHP/5.6.9
Content-Length: 4352

cd67918e02086c10de8202a75ca31c256636bef519b576bcbe6d4b8
7f1d60bc41fdb0a8cf7ed032908c7e5ff2d9cc21d21b4be633a786
1ad062859da7f696b9a9a8d1ab354d8a52c7051cad32b2494ce102
e15aea3edba7d1679b5c888e67c7d3182cccaa9ab538f0613d47e3
aa3e15f22979bef8d83ad0df8234504b0337d36d17b8489a1a3905
df5d0b3c17f97dfd778d03b05324988e37cd8b18dc13ffb2ede3d0
f5c53a0a1e9a4a75e2d3bf9f6d7e0c3b1bbaba54e5304f9721b7ca
9c7fb3e0cc7393ac9789a667335ea0c55dce3b82006597735d3485
74ee8ff4a202406a9699d8e3a7e7da6b5fc7edc16fe32e5b4d5e49
342ca87aeeca2f614be0698076e09101342d8687ca994de5e9b6a5
d4b98e047dd31e30769df479123e9e98bda213390e34f7a42f9272
2c7d0d3d1ea9786e288efda65e00339f127d81161c831bff759ad9
785f55bf5d0b3c17f97dfd78c67cb55bcabbd32285eb7340a17a87
729ba26248ef1bc1d8a393cd8bb8f0d494a5073b70239cf2075609
9ebf676c4ba08d212860644eda73a63ffc8d4ffd6d730105ea1189
ef88e97c44cf8b19128c5fefe3b4882ecebeb84bbdfebe8de635fa
4f2a3698c024c275868256336d2ab59ce22477994ab18053e82a83
0f969690672fc8c3f968241f8e94ff3291fb9c3033d30f8ebff0f8
4214c3fb082a56757c7fbd0c12ea8cce5fcde6860c974544df8e1e
b9fed85709c1df33c588a71199b144a9371868d42cea191989c312
77ac3bb29ba26248ef1bc1d285eb7340a17a877ad178cbb5c86d82
5285eb7340a17a877d49c3c3e94ff810c7c78b8a371aeab8cef814
```

结果依然是长字符串....

认真看了一下url,发现line参数是空的,而且file参数是个base64密文.解密可得:

flag.txt

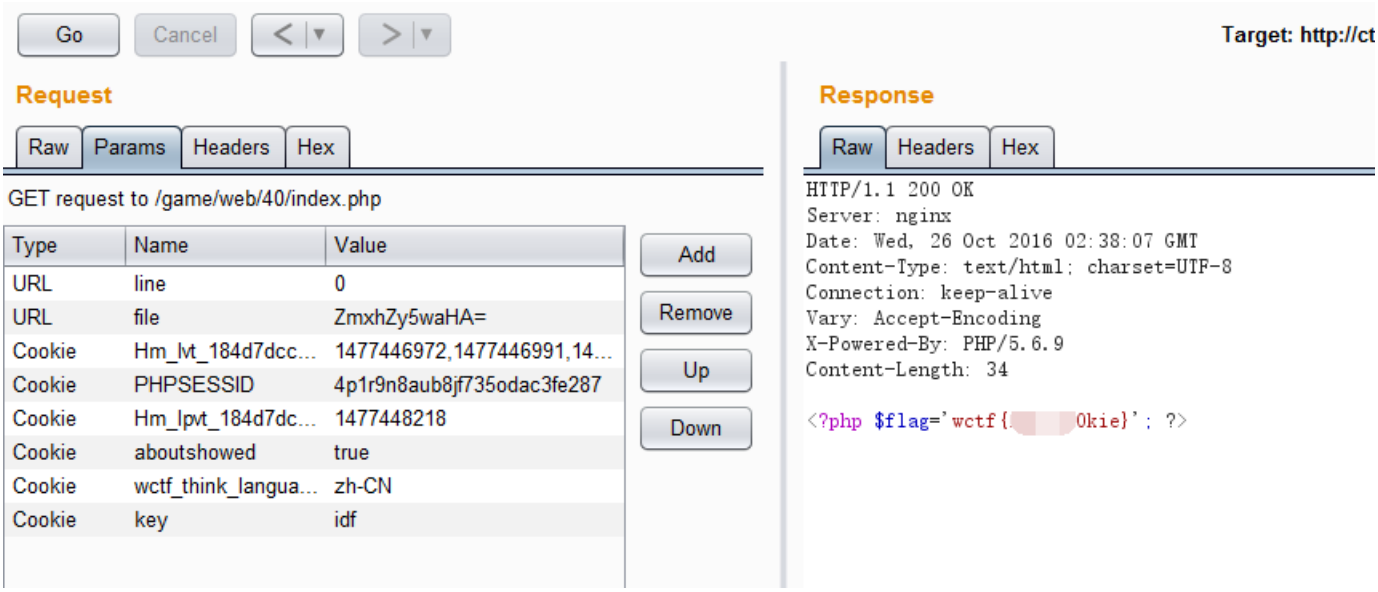
所以我们可以试试读取index.php看可不可以.注意前面flag.txt是经过base64加密的,所以index.php也得加密,为:aW5kZXgucGhw.然后line就从0-n提交一下看看会出现啥.line==0的时候:



看来有戏!继续提交就可以获得全部的代码:

```php
<?php
error_reporting(0);
$file=base64_decode(isset($_GET['file'])?$_GET['file']:"");
$line=isset($_GET['line'])?intval($_GET['line']):0;
if($file=='') header("location:index.php?line=&file=ZmxhZy50eHQ");
$file_list = array(
'0' =>'flag.txt',
'1' =>'index.php',
);
if(isset($_COOKIE['key']) && $_COOKIE['key']=='idf'){
$file_list[2]='flag.php';
}
if(in_array($file, $file_list)){
$fa = file($file);
echo $fa[$line];
}
?>
```

所以代码的意思就是,把cookie里的”key”的键值置为”idf”,将file参数置为”ZmxhZy5waHA=”(flag.php的base64密文),访问就行了.结果如下:

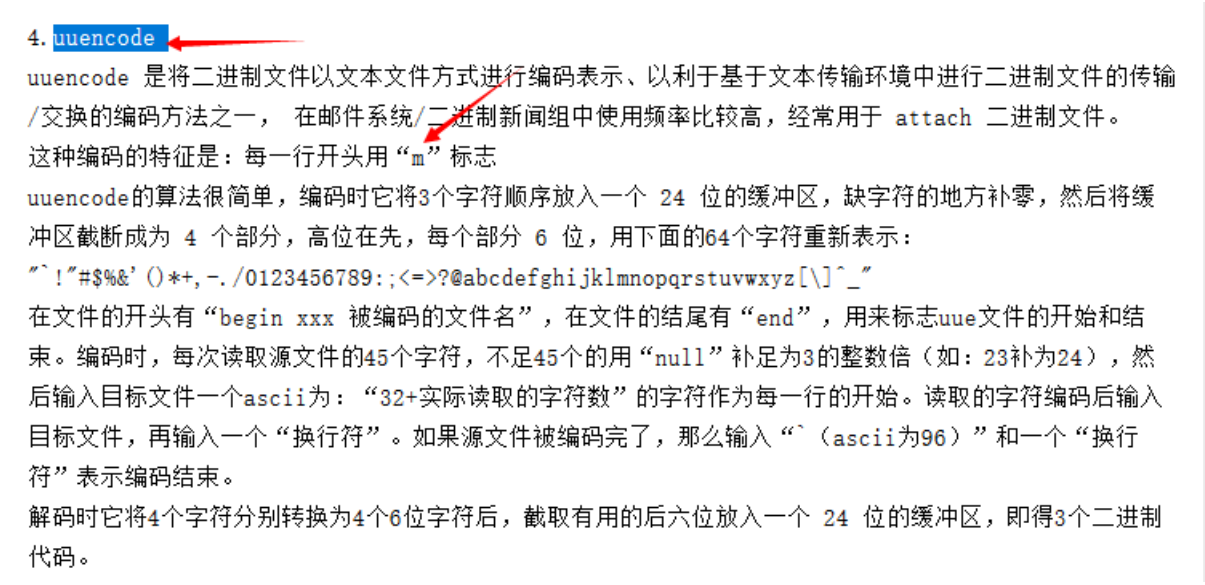


秘制打码~

3.古老的邮件编码

```
MR,O)^KNYU>;*Q[*[P_?#Q+"AHZS6Q\G,LKNYNZ.LR;;2LK*[N^&CK+/VN/;,
MXK:\TJJ]RKZAQ-36K:&CH:,*M/.XQ;3PL+B^S<K'U>+1^;#)=V-T9GMU=75U
*=65N8V]D95]??0``
```

邮件编码,搜之,发现一个介绍



(http://www.263.zj.cn/email-code/)

搜一下UUencode的解码解一下就行了:

(http://web.chacuo.net/charsetuuencode)

秘制打码~

4.超简单的js题
这里这里→ http://ctf.idf.cn/game/web/42/index.php

又是js题..js不太会,还是随便看了一下源代码,发现挺简单的

```
<script>
var p1 = '%66%75%6e%63%74%69%6f%6e%20%63%68%65%63%6b%53%75%62%6d%69%74%28%29%7b%76%61%72%20%61%3d%64%6f
var p2 = '%61%34%64%39%31%63%33%36%32%32%63%32%31%32%65%34%64%65%33%38%63%65%37%35%64%39%35%64%31%66%22
eval(unescape(p1) + unescape('%36' + p2));
</script>
```

代码的意思就是,p1经过unescape(),加上p2在头部补上'%36'后经过的unescape(),最后把这个值输出来.结果为

```
function checkSubmit(){var a=document.getElementById("password");if("undefined"!=typeof a){if("76a4d91c
```

在原来的输入框提交"76a4d91c3622c212e4de38ce75d95d1f"就行啦~~所以flag就是wctf{XXXX}...flag不知道为什么又被加密了:)

5.简单的js解密
这里这里→ http://ctf.idf.cn/game/web/43/index.php

又是js题...按代码的意思应该是给出了密文和加密算法,要我们写出解密算法来解明文.js不太会,跳~

6.你关注最新的漏洞吗

每个人都会梦想手头有一把0day，不过0day可遇不可求，我们还是关注最新的漏洞吧：http://pan.baidu.com/s/1hqf5YZE

答案格式：wctf{*}

这个题目下载下来是一个wireshark的包,wireshark不太会,留着以后填坑~~跳

7.一种编码而已
[][(

[+!

[+!

[+!

[+!

[+!

[+!

[+!

[+!

[+!

[+!

[+!

[+!

[+!

[+!

[+!

[+!

[+!

[+!

[+!

[+!

[+!

[+!

-

[+!

[+!

[+!

[+!

[+!

[+!

[+!

[+!

[+!

[+!

[+!

[+!

[+!

[+!

[+!

[+!

[+!

[+!

[+!

[+!

[+!!⃣]+(!!⃣+⃣)[!!⃣+!!⃣+!!⃣]+(!!⃣+⃣)[+⃣]+({}[⃣]+⃣)[+⃣]+(!!⃣+⃣)[+!!⃣]+({}[⃣]+⃣)[+!!⃣]+({}+⃣)[!!⃣+!!⃣+!!⃣+!!⃣+!!⃣+!!⃣]+(!⃣+⃣)[!!⃣+!!⃣]+({}+⃣)[+!!⃣]+({}+⃣)[!!⃣+!!⃣+!!⃣+!!⃣+!!⃣]+(!⃣+⃣)[+!!⃣]+(!!⃣+⃣)[+⃣]+({}[⃣]+⃣)[!!⃣+!!⃣+!!⃣+!!⃣+!!⃣]+({}+⃣)[+!!⃣]+({}[⃣]+⃣)[+!!⃣])())[!!⃣+!!⃣+!!⃣]+(!!⃣+⃣)[!!⃣+!!⃣+!!⃣])()(({}+⃣)[+⃣])[+⃣]+(!!⃣+!!⃣+!!⃣+!!⃣+!!⃣+!!⃣+⃣)+({}[⃣]+⃣)[!!⃣+!!⃣])

这么风骚…默默打开console 窗口，复制粘贴，运行,得出flag.
编码介绍(http://www.freebuf.com/sectool/5352.html)

结束

第一次写writeup,好紧张…有不足之处还请多多指教~