

# 【CTF练习平台】BugkuCTF部分misc writeup

原创

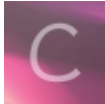
Damya 于 2019-07-17 12:50:53 发布 878 收藏 2

分类专栏: [Bugku CTF](#) 文章标签: [CTF](#) [Bugku](#) [Misc writeup](#) [练习](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: [https://blog.csdn.net/qq\\_43306559/article/details/96293841](https://blog.csdn.net/qq_43306559/article/details/96293841)

版权



[Bugku](#) 同时被 2 个专栏收录

1 篇文章 0 订阅

订阅专栏



[CTF](#)

3 篇文章 0 订阅

订阅专栏

## 签到题

扫描二维码关注得到flag

## 这是一张单纯的图片



拖进notepad, 在末尾发现密文

```
42 警?TX? ?S)携 怒CrSOHWGSdACK?TX楔 NUL( NUL( NUL( &#107;&#101;&#121;&#123;&#121;&#111;&#117;&#32;&#97  
;&#114;&#101;&#32;&#114;&#105;&#103;&#103;&#104;&#116;&#125;倍
```

unicode解码得 key{you are right}

## 隐写

拖进winhex，发现高度不对

Offset	0	1	2	3	4	5	6	7
00000000	89	50	4E	47	0D	0A	1A	0A
00000010	00	00	01	F4	00	00	11	A4
00000020	82	00	00	00	09	70	48	59

修改成11（往大的改），保存图片，打开得到flag



# BUGKU{a1e5aSA}

[https://blog.csdn.net/qq\\_43306559](https://blog.csdn.net/qq_43306559)

BUGKU{a1e5aSA}

telnet

networking.pcap

类型: Wireshark capture file  
大小: 4.46 KB  
修改日期: 2016/9/22 8:55

是个数据包，拖进wireshark里打开，看数据包得到flag

39	17.986831	192.168.221.164	192.168.221.128	TELNET	64 Telnet Data ...
41	18.423632	192.168.221.128	192.168.221.164	TELNET	92 Telnet Data ...
43	19.921235	192.168.221.128	192.168.221.164	TELNET	56 Telnet Data ...
45	19.968035	192.168.221.164	192.168.221.128	TELNET	60 Telnet Data ...
47	21.886838	192.168.221.164	192.168.221.128	TELNET	109 Telnet Data ...
49	26.317246	192.168.221.128	192.168.221.164	TELNET	55 Telnet Data ...

frame 41: 92 bytes on wire (736 bits), 92 bytes captured (736 bits)  
 ethernet II, Src: Vmware\_84:86:5f (00:0c:29:84:86:5f), Dst: Vmware\_26:7e:0e (00:0c:29:26:7e:0e)  
 internet Protocol Version 4, Src: 192.168.221.128, Dst: 192.168.221.164  
 Transmission Control Protocol, Src Port: 1146, Dst Port: 23, Seq: 83, Ack: 124, Len: 38  
 telnet

```

00 00 0c 29 26 7e 0e 00 0c 29 84 86 5f 08 00 45 00  ..)&~... )...E.
00 00 4e 07 b0 40 00 80 06 00 00 c0 a8 dd 80 c0 a8  .N..@... .....
00 dd a4 04 7a 00 17 46 01 d4 4e 68 f0 2a 7a 50 18  ...z...F. .Nh.*zP.
00 01 00 3c b7 00 00 66 6c 61 67 7b 64 33 31 36 37  ..<...f1 ag{d3167
00 35 39 63 32 38 31 62 66 39 32 35 64 36 30 30 62  59c281bf 925d600b
00 65 36 39 38 61 34 39 37 33 64 35 7d             e698a497 3d5}

```

[https://blog.csdn.net/qq\\_43306559](https://blog.csdn.net/qq_43306559)

flag{d316759c281bf925d600be698a4973d5}

## 眼见非实(ISCCCTF)

得到一个没有后缀的文件，改后缀名为zip，解压得到docx文件，拖进notepad里看有隐藏文件  
继续改后缀rar，解压，得到一堆文件，在其中找到

```

schemas.microsoft.com/office/word/2010/wordprocessingShape" mc:Ignorable="w14 w15
wp14"><w:body><w:p w:rsidR="002B3D8D" w:rsidRDefault="002B3D8D"><w:r><w:t>Flag</
w:t></w:r><w:r><w:t>在这里哟! </w:t></w:r></w:p><w:p w:rsidR="002B3D8D"
w:rsidRPr="002B3D8D" w:rsidRDefault="002B3D8D"><w:pPr><w:rPr><w:rFonts
w:hint="eastAsia"/><w:vanish/></w:rPr></w:pPr><w:r
w:rsidRPr="002B3D8D"><w:rPr><w:vanish/></w:rPr><w:t>flag{F1@g}</w:t></
w:r><w:bookmarkStart w:id="0" w:name="_GoBack"/><w:bookmarkEnd w:id="0"/></
w:p><w:sectPr w:rsidR="002B3D8D" w:rsidRPr="002B3D8D"><w:pgSz w:w="11906"

```

flag{F1@g}

啊哒





拖进notepad，发现有别的图片，用foremost（windows）进行分离，得到flag图片

flag{NSCTF\_e6532a34928a3d1dadd0b049d5a3cc57}

[https://blog.csdn.net/qq\\_43306559](https://blog.csdn.net/qq_43306559)

flag{NSCTF\_e6532a34928a3d1dadd0b049d5a3cc57}

猜



拖进notepad，发现是iCCPICC Profile，是取证类题目  
根据flag格式提示，用百度以图搜图，是刘亦菲



图中可能是 **刘茜美子**

更多尺寸推荐

2048x2689 高清	945x1192	870x1097
--------------	----------	----------



## 刘茜美子

刘亦菲，明星，参演仙剑奇侠传一，神雕侠侣，天龙八部等等 [百度百科](#)

[搜索更多相关结果](#) →

[https://blog.csdn.net/qq\\_43306559](https://blog.csdn.net/qq_43306559)

key{liuyifei}

[宽带信息泄露](#)





女神帕拉斯·雅典娜，是希腊神话中的女战神也是智慧女神，雅典是以她命名的。

兰斯洛特，

英格兰传说中的人物，是亚瑟王圆桌骑士团中的一员。看上去就是一个清秀年轻的帅小伙儿，由于传说中他是一名出色的箭手，因此梅花J手持箭支。兰斯洛特与王后的恋爱导致了他与亚瑟王之间的战争。

Hint:

其实斗地主挺好玩的。

[https://blog.csdn.net/qq\\_43306559](https://blog.csdn.net/qq_43306559)

三个人物对应扑克牌中的KQJ，试了一些组合都没用，直接爆破



得到一张图片



拖进notepad结尾有flag

```
Ⓜ 文件 编辑 格式 窗口 帮助  
Ⓜ c? v? d? c? 訃 - m 擦 儻 m 歎 SOHT? 駟 BS j v 岙 v?  
f1@g{eTB1IEFyZSBhIGhAY2tlciE=}  
SUB
```

解base64

明文:

y0u Are a h@cker!

BASE64编码 >

< BASE64解码

BASE64:

eTB1IEFyZSBhIGhAY2tlciE=

f1@g{y0u Are a h@cker!}

多种方法解决



解压得到KEY.exe，拖进notepad得到图片base64码，解码得到二维码



扫描得到 KEY{dca57f966e4e4e31fd5b15417da63269}

## 闪的好快

是个gif，stegsolve提取帧，有18张图片，每张都扫一下，把字符串起来  
SYC{F1aSh\_so\_f4sT}

**come\_game**



改后缀为jpg，打开是张鸽子



拖进notepad发现结尾有字符串

```
69f 个 磷 鯨 e 痛 / SOH: 抹 RSs * 菱 ?  
fg2ivvo}l{2s3_o@aw__rcl@
```

看格式和栅栏密码有关，解密得到

```
fg2ivvo}l{2s3_o@aw__rcl@
```

每组字数

```
flag{w22_is_v3ry_cool}@@
```

flag{w22\_is\_v3ry\_cool}

## linux

在winhex里搜key关键字就能找到

```
13  ANS1 ASCII  
32  key{feb81d3834e2  
34  423c9903f4755464  
30  060b}  
30
```

key{feb81d3834e2423c9903f4755464060b}

## 隐写3

解压是张(●—●)大白~  
拖进winhex改高度，得到flag

flag{He1l0\_d4\_ba1}

flag{He1l0\_d4\_ba1}

### 做个游戏(08067CTF)

是个jar文件，右键用java打开，根据提示要坚持60s（不可能）  
解压得到一些class文件，即编译过的java文件，用jd-gui打开

```
        case 6:  
            printInfo(g, "flag{RGFqaURhbGlfSmlud2FuQ2hpamk=}", 50, 150, 300);  
            break;  
    }
```

flag{RGFqaURhbGlfSmlud2FuQ2hpamk=}

base64解密得 flag{DajiDali\_JinwanChiji}

### 想蹭网先解开密码

文件是个wireshark的数据包，拖进软件里查看  
因为wifi连接的四次握手包是eapol协议，过滤

No.	Time	Source	Destination	Protocol	Length	Info
3066	45.138762	D-LinkIn_9e:4e:a3	LiteonTe_68:5f:7c	EAPOL	155	Key (Message 1 of 4)
3068	45.154148	LiteonTe_68:5f:7c	D-LinkIn_9e:4e:a3	EAPOL	155	Key (Message 2 of 4)
3070	45.168458	D-LinkIn_9e:4e:a3	LiteonTe_68:5f:7c	EAPOL	213	Key (Message 3 of 4)
3072	45.195620	LiteonTe_68:5f:7c	D-LinkIn_9e:4e:a3	EAPOL	133	Key (Message 4 of 4)

手机号是11位，已经提示了七位1391040，写个字典爆破后四位  
用ewsa WiFi密码破解器

SSID	哈希	密码	MDKOD2...	状态
<input checked="" type="checkbox"/> D-Link_DIR-600A		13*****	Yes	发现

。。v7版本下的太新了，换了个v6版本的试试

最后密码: 13910406781 CPU 负载: [ ]

SSID	Hash	密码	状态
<input checked="" type="checkbox"/> D-Link_DIR-6...		13910407686	找

恭喜! 密码已被找到。

确定

得到flag{13910407686}

按照上一题的套路，直接搜索key，没找到，搜{找到了（居然是大写）

```
-
3 KEY{24f3627a86fc
3 740a7f36ee2c7a1c
0 124a}
0
```

KEY{24f3627a86fc740a7f36ee2c7a1c124a}

## 账号被盗了

看源码，是个post传参

```
<form method='post' action='cookieflag.php'>
  <button type='submit'>Get flag</button>
</form>
</body>
```

burpsuite抓包分析下

```
Cookie: hm_lvt_0b03902044e00d70cb1cd01ca0e03148=1330023213,
Hm_lpv1_0bd5902d44e80b78cb1cd01ca0e85f4a=1557163361; isadmin=true
Connection: close
```

```
text-align: center;
font-size: 30px;
}
</style>
<head>
<title>bugku</title>
<link href="style.css" rel="stylesheet" type="text/css">
</head>
<body>
<span>http://120.24.86.145:9001/123.exe</span>
</body>
```

下文件分析



用wireshark抓包，得到一串base64，解码得到

[bkctfest@163.com](mailto:bkctfest@163.com)

a123456

登陆163邮箱



KEY{sg1H78Si9C0s99Q} 也不知道那个狗比把flag改了，我还以为我找错地方了

1楼：哈哈哈，我有点想删flag，但是我的良心制止了我

2楼：真的flag去发件箱里找，删改flag的一辈子单身！

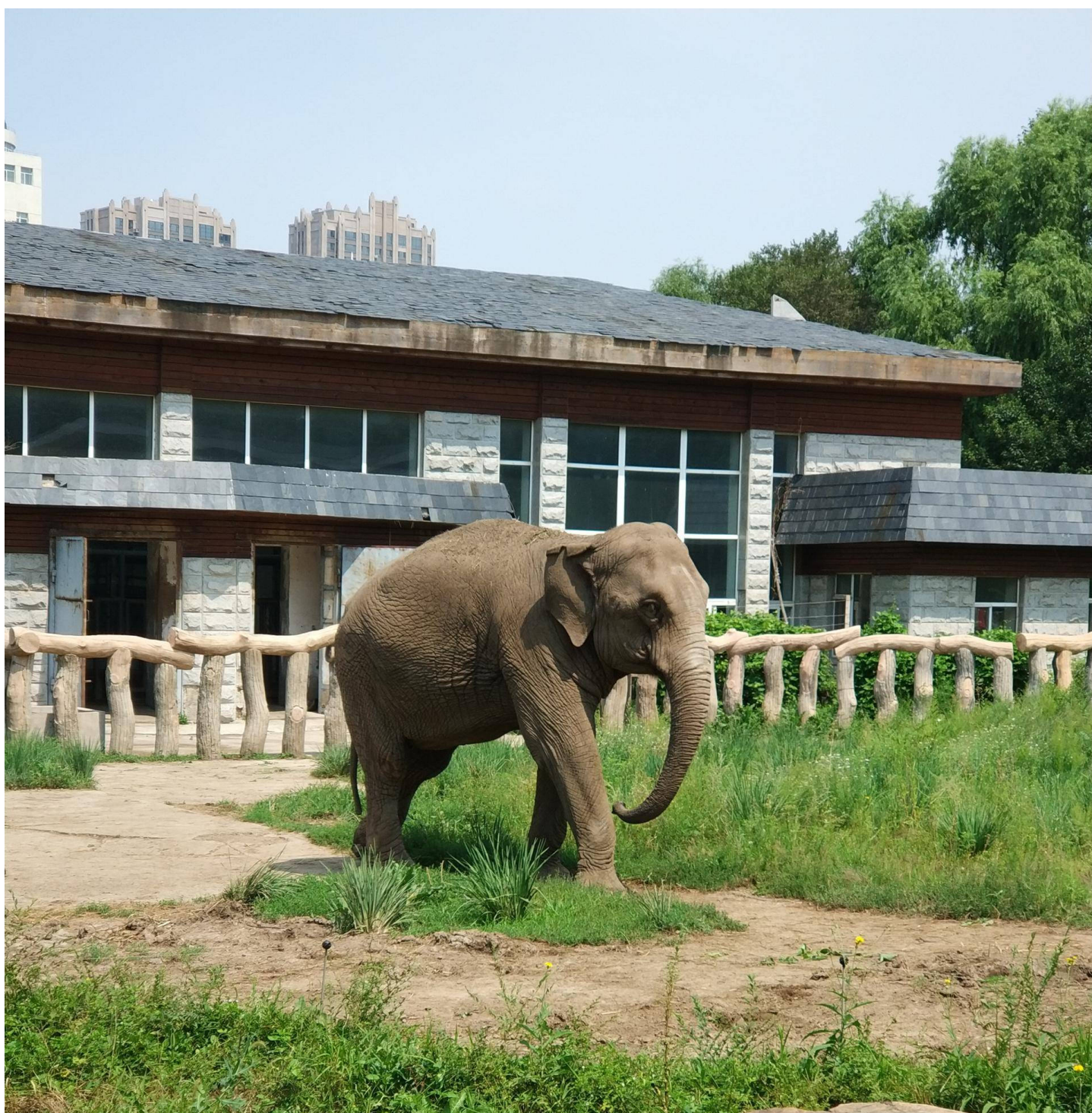
真flag! flag{182100518+725593795416}

唉我去，邮箱里真乱，还好好心人是在的

flag{182100518+725593795416}

## 细心的大象

解压得到一张图片







看一下属性

标题	出题人已经跑路了
主题	出题人已经跑路了
分级	☆☆☆☆☆
标记	<input type="text" value="添加标记"/>
备注	TVNEUzQ1NkFTRDEyM3p6

base64解密文 TVNEUzQ1NkFTRDEyM3p6 MSDS456ASD123zz

foremost分离一下，得到rar

用密码解压，得到一张图片，熟悉的改高度，得到flag

BU

**BUGKU{a1e5aSA}**

[https://blog.csdn.net/qq\\_43306559](https://blog.csdn.net/qq_43306559)

BUGKU{a1e5aSA}

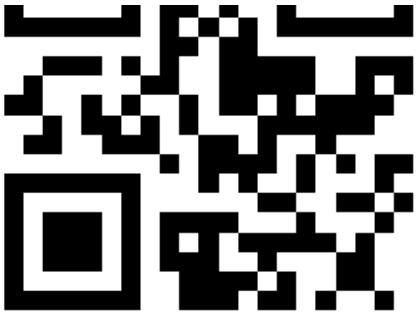
**爆照(08067CTF)**

格式 flag{xxx\_xxx\_xxx}









扫描得到 panama

按顺序来排 flag{bilibili\_silisili\_panama}

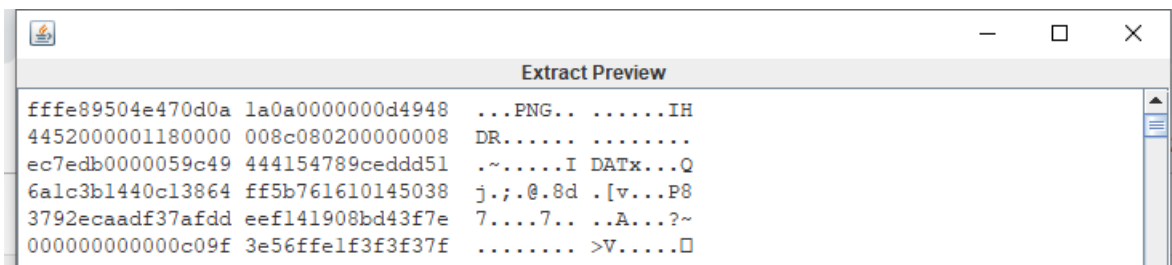
## 猫片(安恒)

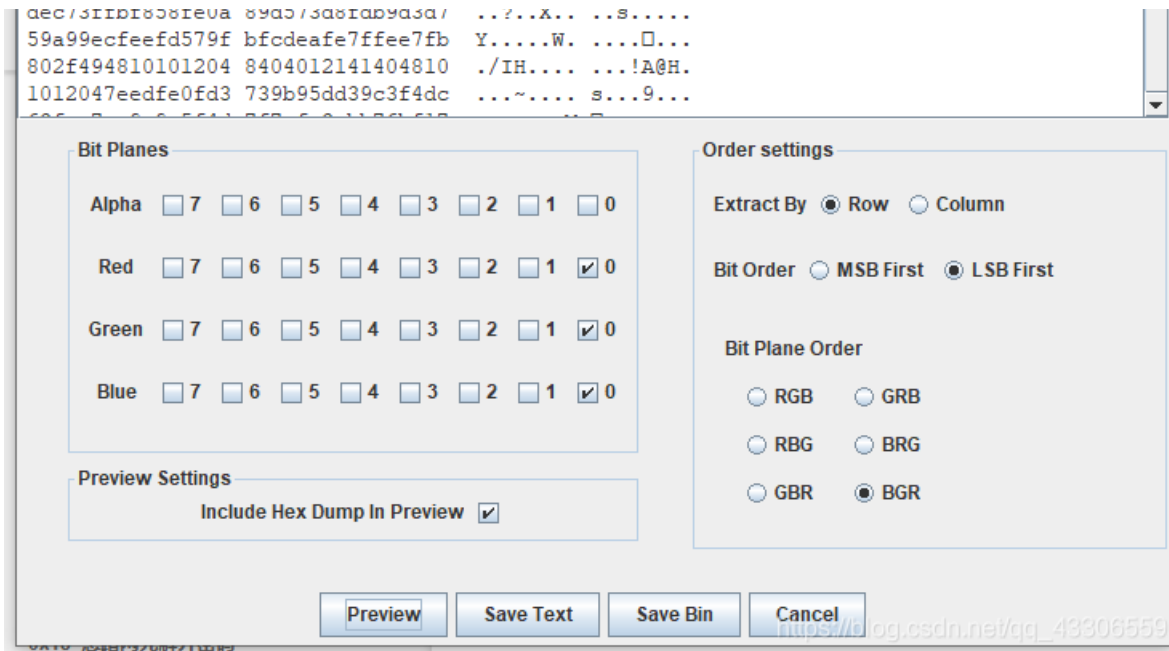
hint:LSB BGR NTFS

拖进winhex里发现png文件头, 改后缀名得到一只喵喵(好可爱)



根据提示去stegsolve里提取一下色素



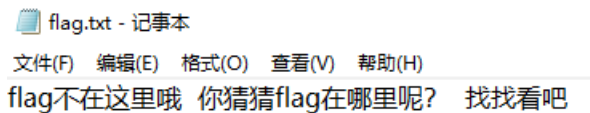


提取后改文件头得到新图片,半张二维码

继续改高度,反相后扫描,得到一个网址

<https://pan.baidu.com/s/1pLT2J4f>

下载得到flag.rar,解压后(呵)



根据最后一个hint提示,用到NtFsStreamsEditor工具捕捉数据流

* 文件	数据流名称	大小(字节)	可疑度(0-5)
<input type="checkbox"/> G:\Damya\bugku\0x23\flag.txt:flag.pyc	flag.pyc	755	1
<input type="checkbox"/> G:\Damya\bugku\0x23\ntfsstreamseditor.exe:Zone.Identifier	Zone.Identifier	129	0
<input type="checkbox"/> G:\Damya\bugku\0x23\png.png:Zone.Identifier	Zone.Identifier	146	0

导出flag.pyc文件,在线反编译

```

import base64

def encode():
    flag = '*****'
    ciphertext = []
    for i in range(len(flag)):
        s = chr(i ^ ord(flag[i]))
        if i % 2 == 0:
            s = ord(s) + 10
        else:
            s = ord(s) - 10
        ciphertext.append(str(s))

    return ciphertext[::-1]

ciphertext = [
    '96',
    '65',
    '93',
    '123',
    '91',
    '97',
    '22',
    '93',
    '70',
    '102',
    '94',
    '132',
    '46',
    '112',
    '64',
    '97',
    '88',
    '80',
    '82',
    '137',
    '90',
    '109',
    '99',
    '112']

```

根据这个写一个解密脚本(参考了一下师傅的)

```

def decode():
    ciphertext = [
        '96',
        '65',
        '93',
        '123',
        '91',
        '97',
        '22',
        '93',
        '70',
        '102',
        '94',
        '132',
        '46',
        '112',
        '64',
        '97',
        '88',
        '80',
        '82',
        '137',
        '90',
        '109',
        '99',
        '112']
    ciphertext.reverse()
    flag = ''
    for i in range(len(ciphertext)):
        if i % 2 == 0:
            s = int(ciphertext[i]) - 10
        else:
            s = int(ciphertext[i]) + 10
        s=chr(i^s)
        flag += s
    return flag

def main():
    flag = decode()
    print(flag)

if __name__ == '__main__':
    main()

```

跑一下得到flag

flag{Y@e\_Cl3veR\_C1Ever!}