【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

本文链接：https://blog.csdn.net/qq_43306559/article/details/96293841

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

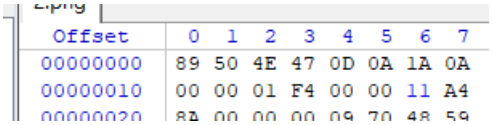
拖进notepad，在末尾发现密文

```
42  警ETX ? SI 愤  愍Cr SOH W GS d ACK ? ETX 楔  NUL (  NUL (  NUL  &#107;&#101;&#121;&#123;&#121;&#111;&#117;&#32;&#97
;&#114;&#101;&#32;&#114;&#105;&#103;&#104;&#116;&#125;傩
```

unicode解码得 key{you are right}

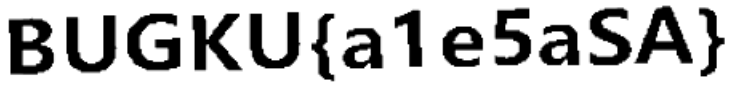
隐写

拖进winhex，发现高度不对



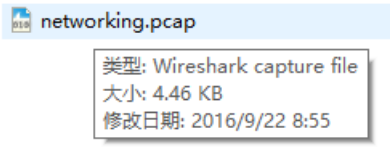
Offset	0	1	2	3	4	5	6	7
00000000	89	50	4E	47	0D	0A	1A	0A
00000010	00	00	01	F4	00	00	11	A4
00000020	8A	00	00	00	09	70	48	59

修改成11（往大的改），保存图片，打开得到flag

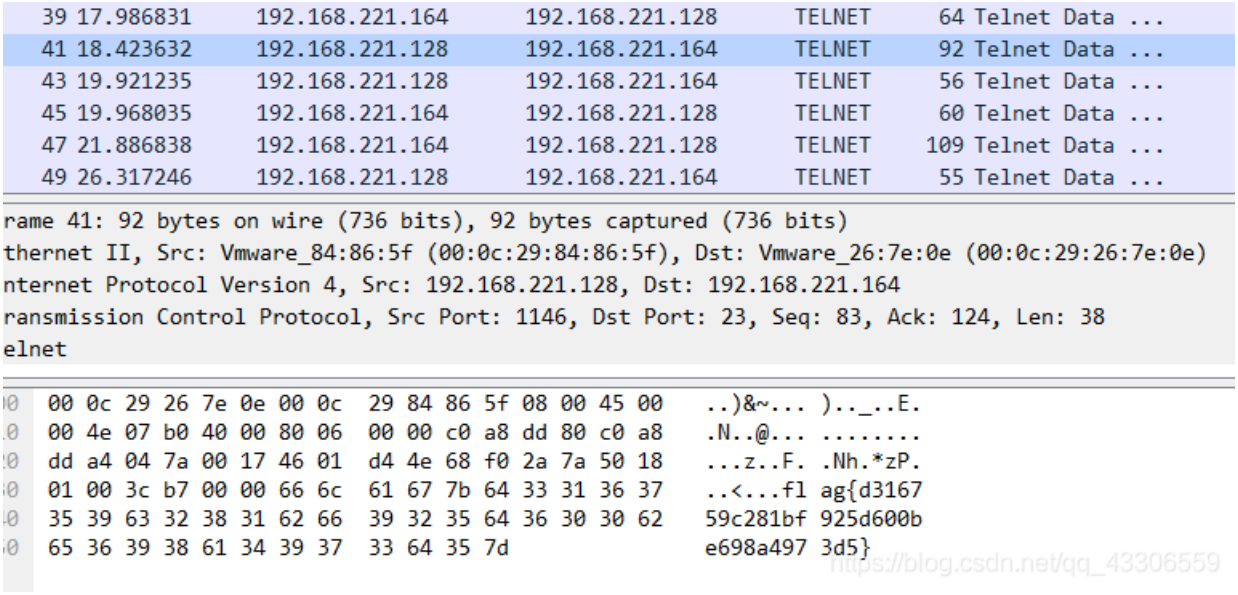


BUGKU{a1e5aSA}

telnet



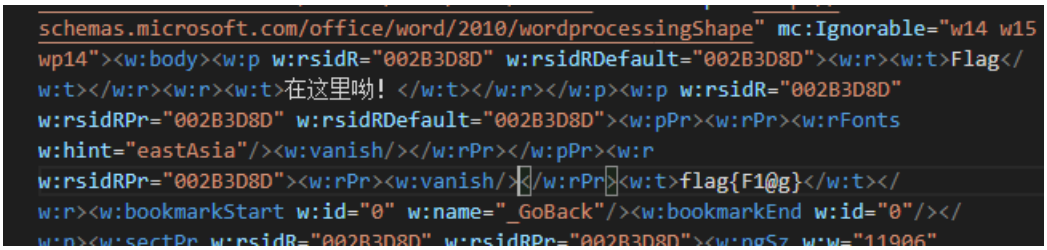
是个数据包，拖进wireshark里打开，看数据包得到flag



flag{d316759c281bf925d600be698a4973d5}

眼见非实(ISCCCTF)

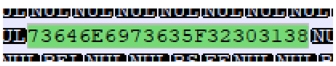
得到一个没有后缀的文件，改后缀名为zip，解压得到docx文件,拖进notepad里看有隐藏文件
继续改后缀rar，解压，得到一堆文件,在其中找到

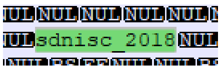


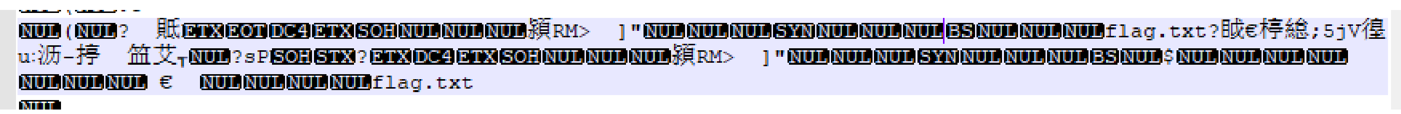
flag{F1@g}

啊哒

拖进notepad里发现有隐藏文件，还有一串数字，hex转ascii后得到明文





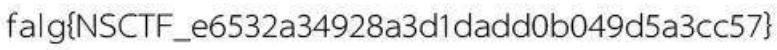


改后缀得到加密压缩包，输入明文，得到flag.txt

flag{3XiF_iNf0rM@ti0n}

又一张图片，还单纯吗

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



falg{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

key{liuyifei}

宽带信息泄露

是一个bin文件，根据提示宽带信息，用routerpassview打开

```
<Name val=pppoe_eth1_d />
<Uptime val=671521 />
<Username val=053700357621 />
<Password val=210265 />
<X_TP_IfName val=ppp0 />
```

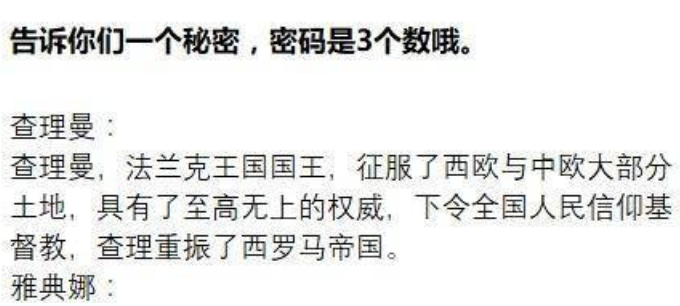
flag{053700357621}

隐写2

拖进notepad

```
NUL NUL BS NUL NUL 8~nK飛騰L SUB NUL NUL L SUB NUL NUL BS NUL $ NUL NUL NUL
NUL NUL NUL NUL NUL NUL NUL flag.rar
NUL
NUL NUL NUL NUL NUL SOH NUL CAN NUL ?" GS ] ? EM SYN $ GS ] ? EM SYN $ GS ] ?P SOH
鋒 SOH NUL
NUL $ NUL NUL NUL NUL NUL NUL NUL  NUL NUL NUL r SUB NUL NUL 鎖慆ず.jpg
NUL
```

改后缀rar解压得到文件

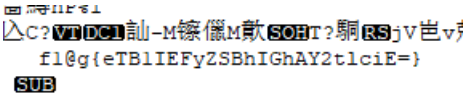


女神帕拉斯·雅典娜，是希腊神话中的女战神也是智慧女神，雅典是以她命名的。
兰斯洛特，
英格兰传说中的人物，是亚瑟王圆桌骑士团中的一员。看上去就是一个清秀年轻的帅小伙儿，由于传说中他是一名出色的箭手，因此梅花J手持箭支。兰斯洛特与王后的恋爱导致了他与亚瑟王之间的战争。
Hint:
其实斗地主挺好玩的。

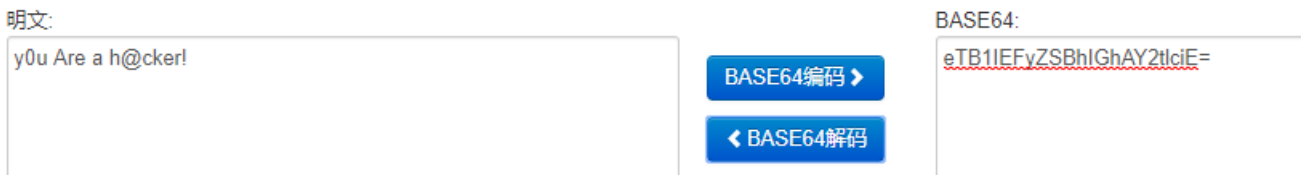
三个人物对应扑克牌中的KQJ，试了一些组合都没用，直接爆破

得到一张图片

拖进notepad结尾有flag



解base64



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

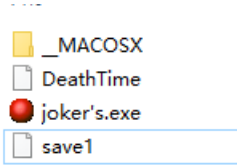
扫描得到 KEY{dca57f966e4e4e31fd5b15417da63269}

闪的好快

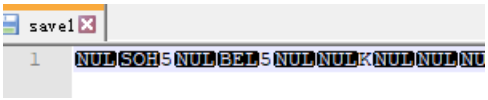
是个gif，stegsolve提取帧，有18张图片，每张都扫一下，把字符串起来
SYC{F1aSh_so_f4sT}

come_game

居然是我最喜欢的iwanna游戏！！（没忍住玩了一会）



拿到存档文件后,拖进notepad,修改关卡参数



及时截图

FLAG{6E23F259D98DF153}
提交出错,猜想和上一道题是同一个比赛的题,提交格式应该一样
SYC{6E23F259D98DF153}

白哥的鸽子

改后缀为jpg，打开是张鸽子

拖进notepad发现结尾有字符串

```
GSf个嚼鳝e瘸/SOH:揀RSs*荽?
复g2ivyo}l{2s3_o@aw__rcl@
```

看格式和栅栏密码有关，解密得到

fg2ivyo}l{2s3_o@aw__rcl@

每组字数 3 加密 解密

flag{w22_is_v3ry_cool}@@

flag{w22_is_v3ry_cool}

linux

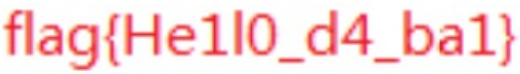
在winhex里搜key关键字就能找到

```
32  key{feb81d3834e2
34  423c9903f4755464
00  060b}
```

key{feb81d3834e2423c9903f4755464060b}

隐写3

解压是张(●—●)大白~
拖进winhex改高度，得到flag



flag{He1l0_d4_ba1}

做个游戏(08067CTF)

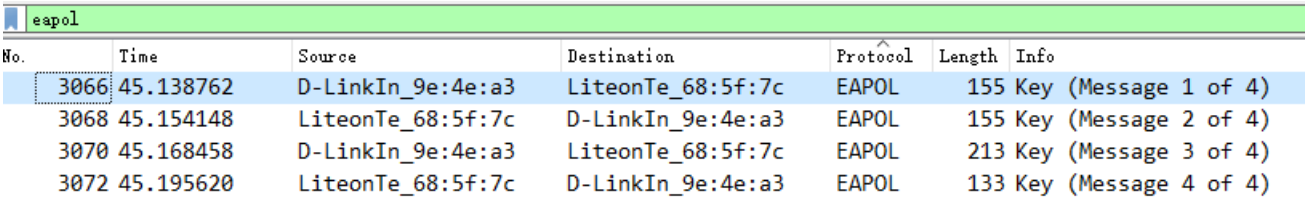
是个jar文件，右键用java打开，根据提示要坚持60s（不可能）
解压得到一些class文件，即编译过的java文件，用jd-gui打开

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

flag{RGFqaURhbGlfSmlud2FuQ2hpamk=}
base64解密得 flag{DajiDali_JinwanChiji}

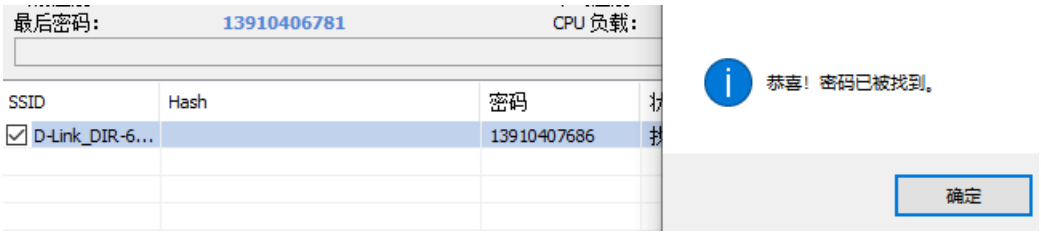
想蹭网先解开密码

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



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

。。v7版本下的太新了，换了个v6版本的试试



得到flag{13910407686}

linux2

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_0bd5902d44e80b78cb1cd01ca0e85f4a=1556623213;
Hm_lpvt_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

bkctftest@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

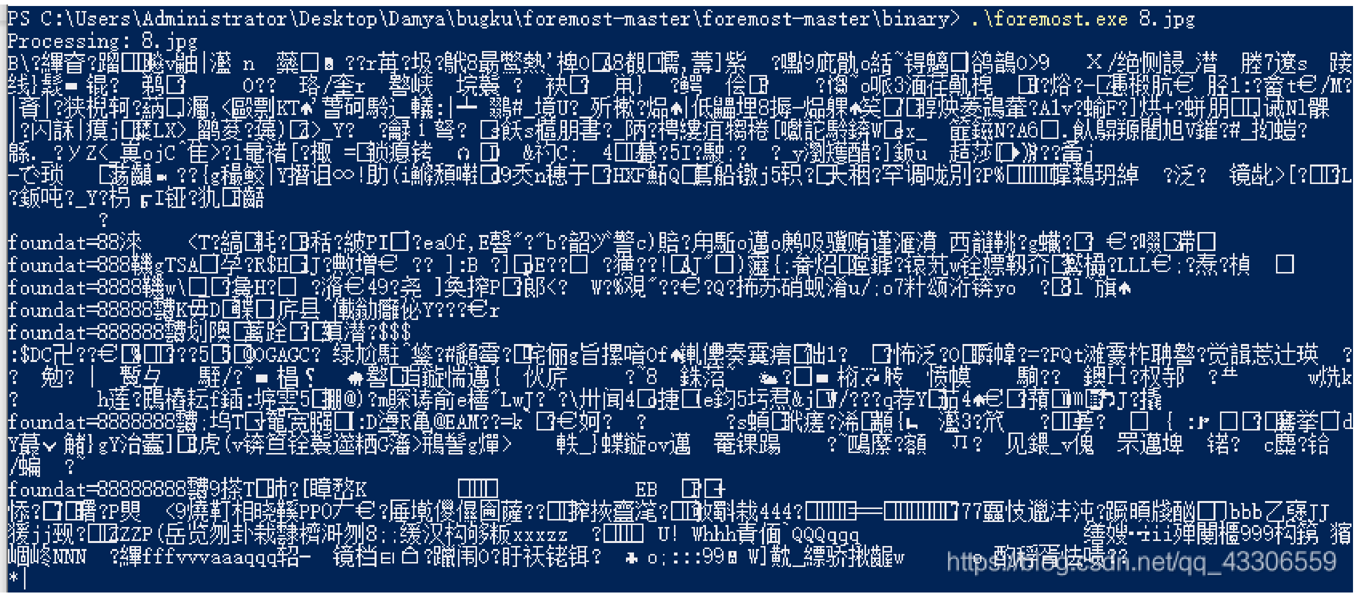
base64解密文 TVNEUzQ1NkFTRDEyM3p6 MSDS456ASD123zz
foremost分离一下，得到rar
用密码解压，得到一张图片，熟悉的改高度，得到flag

BUGKU{a1e5aSA}

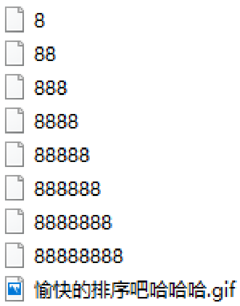
爆照(08067CTF)

格式 flag{xxx_xxx_xxx}

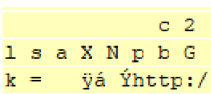
foremost分离下



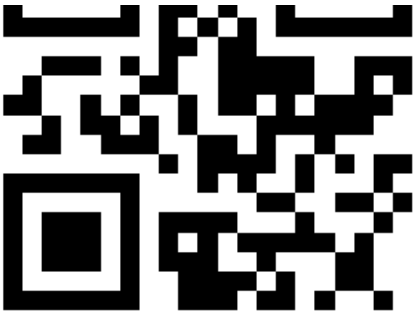
得到



给它们改后缀名成图片，在88.jpg里发现二维码，扫描得到 bilibili
接着发现888.jpg里也有点东西



c2lsaXNpbGk= 解base64得 silisili
8888.jpg里也有东西，是一张二维码

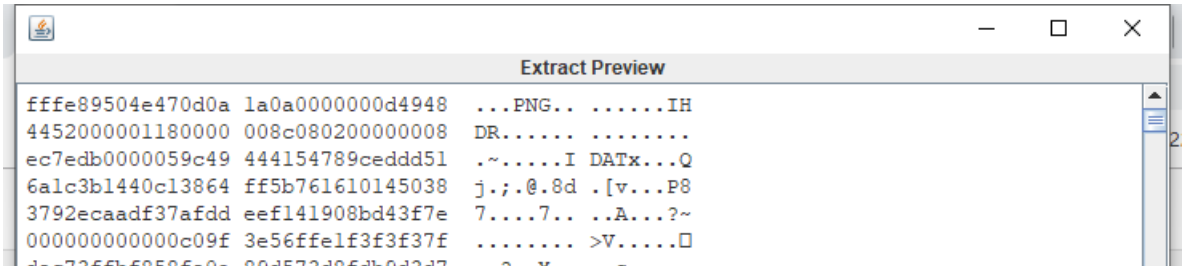


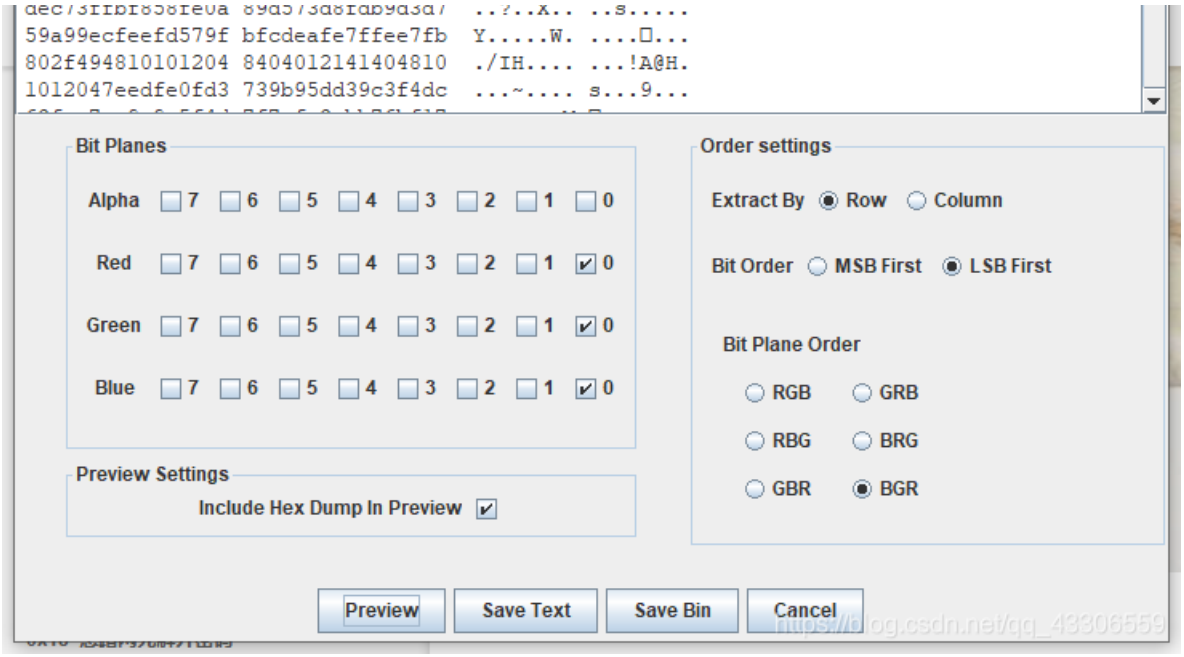
扫描得到 panama
按顺序来排 flag{bilibili_silisili_panama}

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)
☐	G:\Damya\bugku\0x23\flag.txt:flag.pyc	flag.pyc	755	1
☐	G:\Damya\bugku\0x23\ntfsstreamseditor.exe:Zone.Ident...	Zone.Identifier	129	0
☐	G:\Damya\bugku\0x23\png.png:Zone.Identifier	Zone.Identifier	146	0

导出flag.pyc文件,在线反编译

```python
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)

```python
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!}