WUST-CTF2020 writeup

原创

abtgu 于 2020-04-02 20:26:44 发布 867 收藏

分类专栏： CTF

本文链接：https://blog.csdn.net/weixin_43790779/article/details/105278249

文章目录

- WEB
  - checkin
  - admin
- MISC
  - Space Club
  - Welcome
  - 爬
  - Find me
  - Shop
  - girlfriend
  - Alison likes jojo

WEB

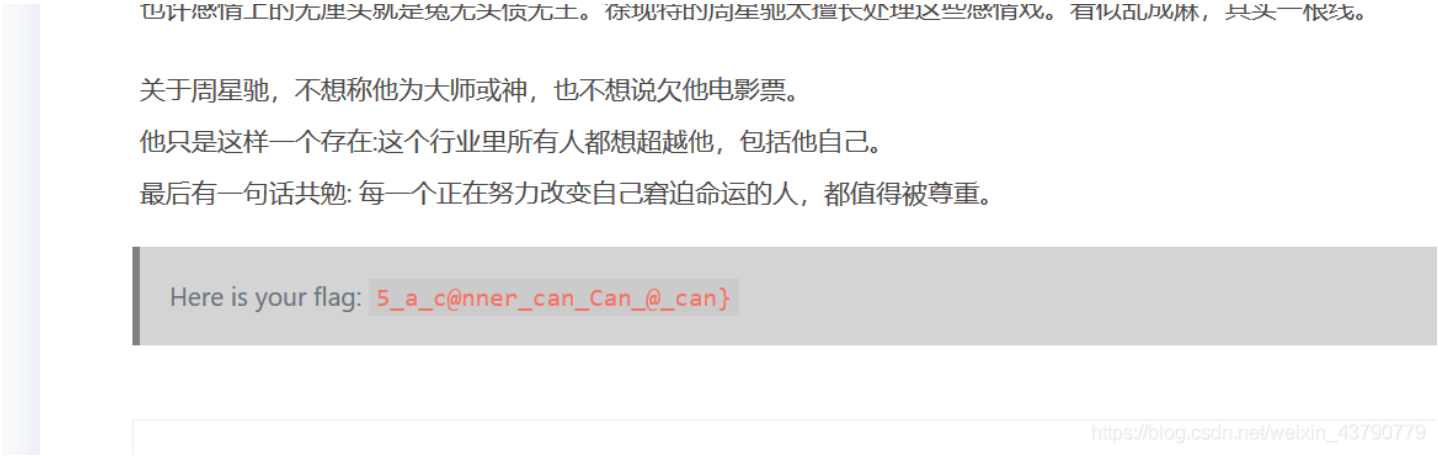
checkin

题目： 无

解题思路： 打开链接，发现提问作者，打开查看器，发现按钮被隐藏，输入框被限制，更改代码，输入作者名，提示一个博客

打开，在最上方发现flag的一部分

仔细查看，有一篇名为《远古的blog》的博客，打开
在最下方发现另一部分flag。



admin

题目： login in as admin.
解题思路： 打开是登录框，提示用户名是admin，使用万能密码，用户名输入：

```
admin' or '1
```

登录成功后进入/adddddddddddddddddddddddddminnnnnnnnnnnnnnnnnnnnn.php页面，提示本地ip才能访问，构造X-Forwarded-For:127.0.0.1，之后提示

```
用GET方式传一个参数ais, 值为520
用POST方式传一个参数wust, 值为1314
```

最后提示

```
你离flag已经很近了，网址给你了：4dz  aste.ubuntu.com/p/   https://p  Rqr  cSf2
```

手动拼接还原网址 https://paste.ubuntu.com/p/cSf24dzRqr ，访问得到

```
d2N0ZjlwMjB7bjB3X3lvdV9rbjB3X3RoZV9iYXNpY18wZl9zcWxfYW5kX2h0dHB9
```

base64转码，得到flag，wctf2020{n0w_you_kn0w_the_basic_0f_sql_and_http}。

MISC

Space Club

题目： 无
解题思路： 打开txt，未发现任何文字，由于题目是space，想到空格，ctrl+a全选文本，果然发现空格，观察形势，联想到0,1二进制数据，写脚本运行

```
import libnum
txt = open("space.txt","r").readlines()
tmp = ''
for i in txt:
    if len(i.strip('\n')) == 6:
        tmp = tmp + '0'
    else:
        tmp = tmp + '1'

flag = libnum.b2s(tmp)
print(flag)
```

得到flag，wctf2020{h3re_1s_y0ur_fl@g_s1x_s1x_s1x}。

Welcome

题目： 《论语》：三人行，必有我师焉。

解题思路： 打开压缩文件，发现需要打开摄像头，又提示三人行，尝试打开手机搜索一张带有三个人的图片，放到摄像头，flag出现。

wctf2020{We1cOme_t0_wCtF2o20_aNd_eNj0y_1t}

爬

题目： 链接: https://pan.baidu.com/s/1DatOBKD-3cee_Tp8LuvPLg

提取码: jm9z

解题思路： 查看文件头，发现是pdf，添加后缀名，打开，提示图片下隐藏flag，用ps打开，发现一张写有一串十六进制数的图片

```
'0x77637466323032307b746831735f31735f405f7064665f616e645f7930755f63616e5f7573655f70686f7430736830707d'
```

将其转换成文本，得到flag，wctf2020{th1s_1s_@_pdf_and_y0u_can_use_phot0sh0p}

Find me

题目： can u find me?

解题思路： 查看图片属性，发现备注有一段盲文，解密即可

解密地址：https://www.qqxiuzi.cn/bianma/wenbenjiami.php?s=mangwen

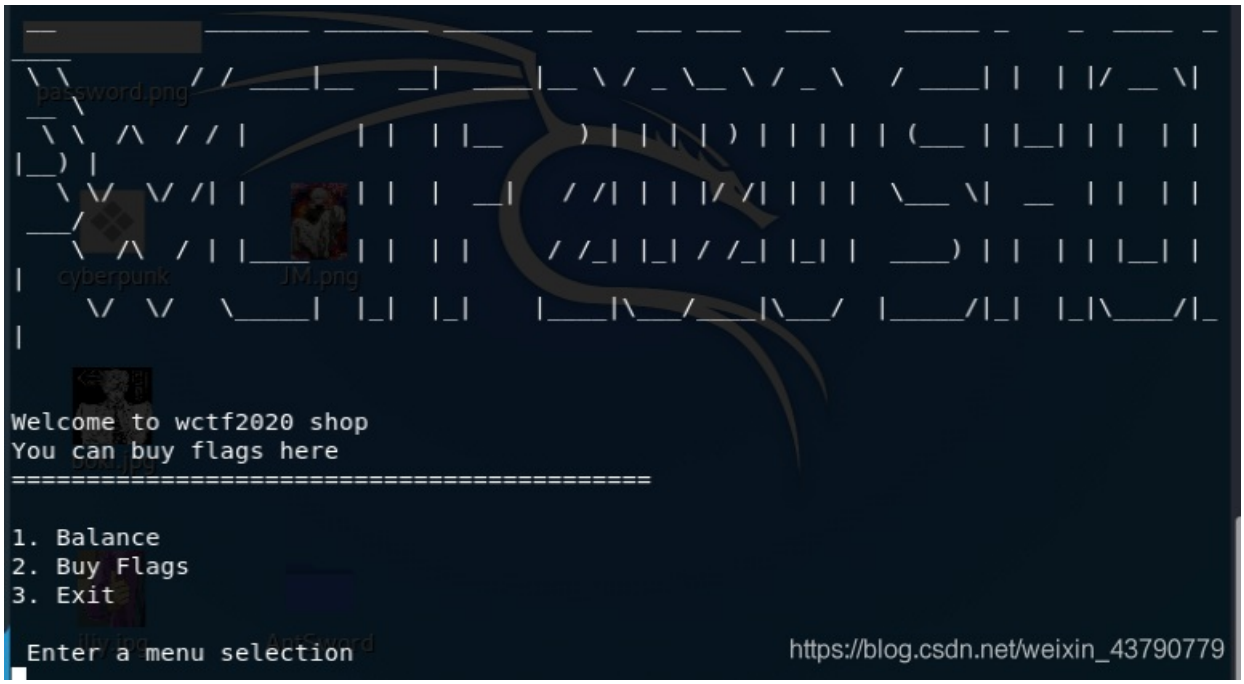
wctf2020{y_0u_f_1n$_d$_M$_e$ee$_e$e}

Shop

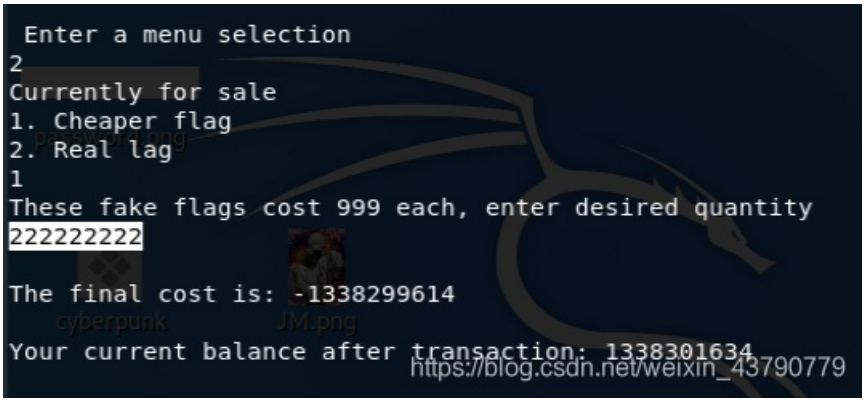
题目： you can buy the flag in the shop, here's your exchange.

nc 47.97.40.187 12306。

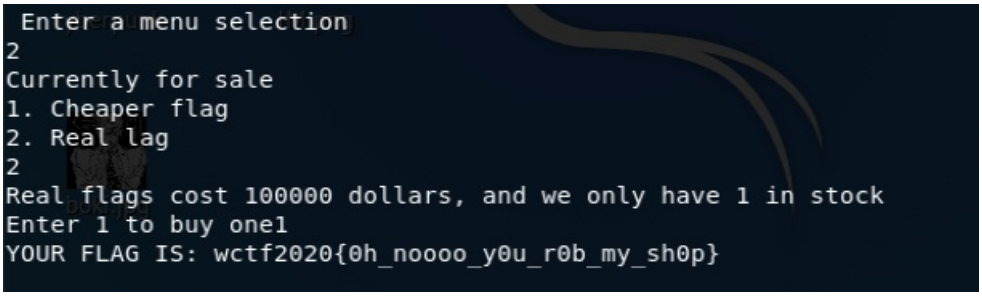
解题思路： 在kali中运行nc 47.97.40.187 12306，出现下图



选择2，出现cheaper，real两个选项，选择real，提示余额不足，选择cheaper，提示每个flag 999，让我们输入购买数量，这是想到 **整数溢出** ，输入一个大数，这里我输的是222222222



果不其然，花费是负数，余额增加。这时去购买real，得到flag，



wctf2020{0h_noooo_y0u_r0b_my_sh0p}。

girlfriend

题目： I want a girl friend !!! 将结果用wctf2020{}再提交

解题思路： 打开wav，仔细听，发现是拨号时的按键声，用DTMF解码器解码得到

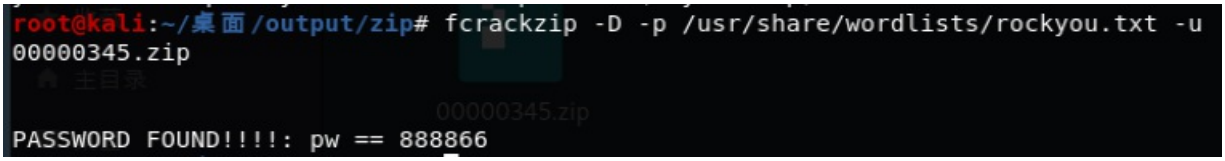
对应手机九键查找字母得到，youaremygirlfriends，flag是wctf2020{youaremygirlfriends}。

Alison likes jojo

题目： As we known, Alison is a pretty girl.

解题思路： 下载题中文件，得到两张jpg，放到kali中用binwalk查看，发现boki.jpg隐藏zip，foremost分离，得到zip需要密码。用fcrackzip破解

```
fcrackzip -D -p /usr/share/wordlists/rockyou.txt -u 00000345.zip
```



得到密码888866，打开beisi.txt，发现一串字符：WVRKc2MySkhWbmxqV0Zac1dsYzBQUT09，用base64多次解码得到killerqueen，猜测其是加密密钥。想到outguess隐写

```
outguess -r jljy.jpg -k killerqueen 1.txt
```

得到flag，wctf2020{pretty_girl_alison_likes_jojo}。