

BUGKU CTF之misc篇（持续更新）

原创

山山得久 于 2018-09-23 14:25:08 发布 4739 收藏 13

分类专栏: [CTF学习之路](#) 文章标签: [bugku ctf misc](#)

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/drothy_zhang/article/details/82821978

版权



[CTF学习之路](#) 专栏收录该内容

4 篇文章 0 订阅

订阅专栏

题库链接: <http://ctf.bugku.com/challenges>

一. 签到题

下载二维码关注bugku得到flag

二. 这是一张单纯的图片

图片链接:

<http://120.24.86.145:8002/misc/1.jpg>

下载图片后用winhex或者hexworkshop打开可以看到

40	1D 64 06 8A 28 03 D0 A8 A2 8A 00 28 A2 8A 00 28	d š(Ď`čš (čš (
50	A2 8A 00 FF 26 23 31 30 37 3B 26 23 31 30 31 3B	čš ýke
60	26 23 31 32 31 3B 26 23 31 32 33 3B 26 23 31 32	y{
70	31 3B 26 23 31 31 31 3B 26 23 31 31 37 3B 26 23	1;ou&#
80	33 32 3B 26 23 39 37 3B 26 23 31 31 34 3B 26 23	32;ar&#
90	31 30 31 3B 26 23 33 32 3B 26 23 31 31 34 3B 26	101; r&
A0	23 31 30 35 3B 26 23 31 30 33 3B 26 23 31 30 34	#105;gh
B0	3B 26 23 31 31 36 3B 26 23 31 32 35 3B D9 D9	;t}00

这明显是一段加密编码:

所以我们直接进行解密, 这里 给大家提供一下在线解密网址: <http://tool.chinaz.com/tools/unicode.aspx>.

然后就可以得到flag。

三. 隐写


```
cd 桌面**
```

```
binwalk 2.jpg
```

可以看到里面有两张图片

```
root@bogon:~/Desktop# binwalk 2.jpg
```

```
output
-----
DECIMAL      HEXADECIMAL     DESCRIPTION
-----
0            0x0             JPEG image data, EXIF standard
12           0xC            TIFF image data, big-endian, offset of first image
directory: 8
13017       0x32D9         Unix path: /www.w3.org/1999/02/22-rdf-syntax-ns#>
<rdf:Description rdf:about="" xmlns:photoshop="http://ns.adobe.com/photoshop/1.
0/" xmlns
158792      0x26C48       JPEG image data, JFIF standard 1.02
158822      0x26C66       TIFF image data, big-endian, offset of first image
directory: 8
159124      0x26D94       JPEG image data, JFIF standard 1.02
162196      0x27994       JPEG image data, JFIF standard 1.02
164186      0x2815A       Unix path: /www.w3.org/1999/02/22-rdf-syntax-ns#>
<rdf:Description rdf:about="" xmlns:dc="http://purl.org/dc/elements/1.1/" xmlns
:xap="htt
168370      0x291B2       Copyright string: "Copyright (c) 1998 Hewlett-Pack
ard Company"
https://blog.csdn.net/drothy_zhang
```

然后输入:

```
formest 2.jpg
```

将图片分离，在虚拟机桌面上你可以看到多出一个文件夹，里面有一张图片上面含有flag。

七.猜

直接图片复制，百度识图，发现是神仙姐姐，根据提示：key{liuyifei}

八.宽带信息泄露

可以发现是一个配置文件，使用RouterPassView工具查看。根据flag格式可知需要查找用户名，查找关键字 **ctrl+F** 输入 **username**，即可得到。

九.隐写二

得到图片，用winhex没发现什么有用信息，放进kali里面binwalk查看，发现有异样，查看以及分离见题六，得到文件夹，里面有个flag压缩文件，发现打开需要密码，根据提示和人名可以知道密码扑克牌中的KJQ有关，又是三个数字，根据键盘发现字母和数字之间的关系，k->8,J->7,Q->1,得到密码是871.使用ARCHRP软件暴力破解也可以,解压得到3.jpg，内心无限卧槽，没办法，继续放到winhex中查看，在最底端发现了一段加密编码，在线base64位解码得到flag。

十.多种方法解决



[创作打卡挑战赛](#)

[赢取流量/现金/CSDN周边激励大奖](#)