【BUUCTF】梅花香之苦寒来

原创

shane_seven 于 2021-07-21 16:14:19 发布 235 收藏

分类专栏： ctf 文章标签： wp

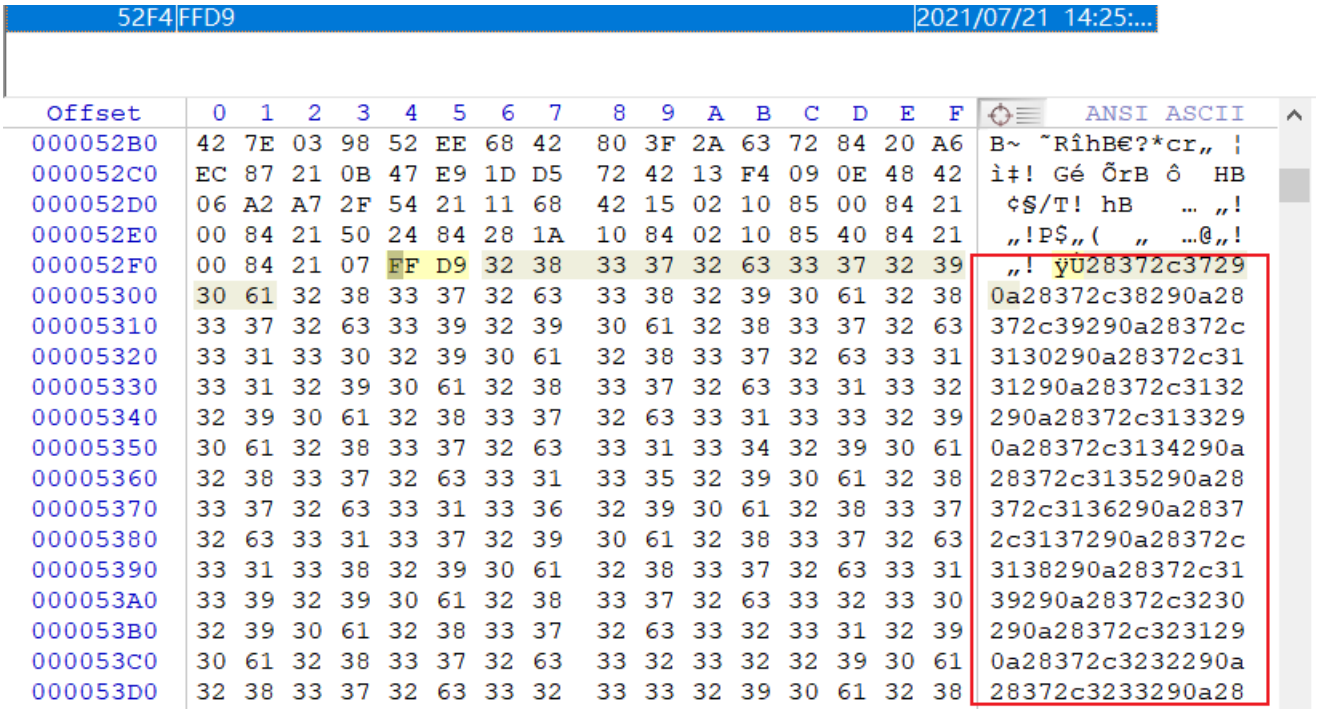
本文链接：https://blog.csdn.net/yoyoko_chan/article/details/118968176

0x00

做了几天BUU的题，发现这个题有点儿意思，学了几个工具，顺便写个WP。(参考了这位大佬的WP: BUUCTF 梅花香自苦寒来)

0x01

下载下来一个压缩包，打开是一张图片，先解压，发现容量还挺大的一定有隐藏，用winhex打开后在尾部发现问题

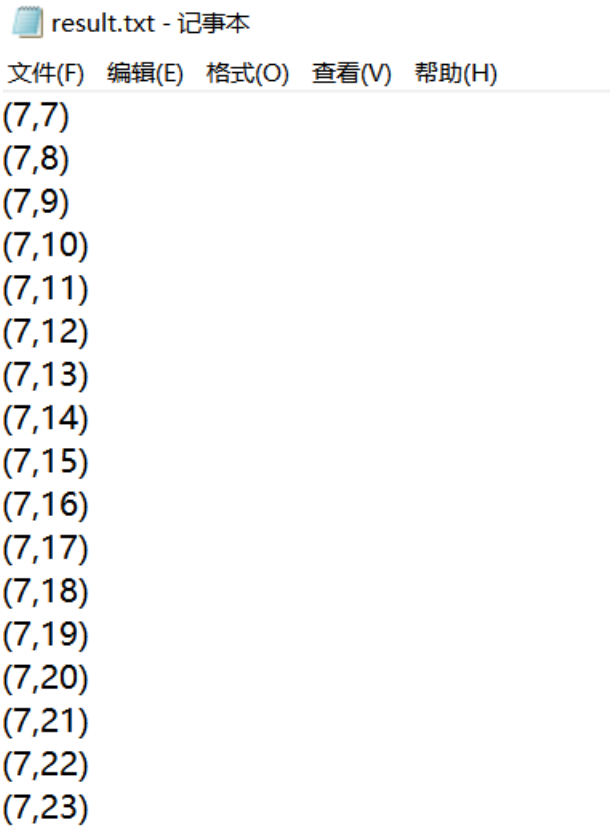


Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
000052B0	42	7E	03	98	52	EE	68	42	80	3F	2A	63	72	84	20	A6	B~ ˜RîhB€?*cr„ ¦
000052C0	EC	87	21	0B	47	E9	1D	D5	72	42	13	F4	09	0E	48	42	ì‡! Gé ÕrB ô HB
000052D0	06	A2	A7	2F	54	21	11	68	42	15	02	10	85	00	84	21	¢§/T! hB … „!
000052E0	00	84	21	50	24	84	28	1A	10	84	02	10	85	40	84	21	„!P$„(„ …@„!
000052F0	00	84	21	07	FF	D9	32	38	33	37	32	63	33	37	32	39	„! ÿÙ28372c3729
00005300	30	61	32	38	33	37	32	63	33	38	32	39	30	61	32	38	0a28372c38290a28
00005310	33	37	32	63	33	39	32	39	30	61	32	38	33	37	32	63	372c39290a28372c
00005320	33	31	33	30	32	39	30	61	32	38	33	37	32	63	33	31	3130290a28372c31
00005330	33	31	32	39	30	61	32	38	33	37	32	63	33	31	33	32	31290a28372c3132
00005340	32	39	30	61	32	38	33	37	32	63	33	31	33	33	32	39	290a28372c313329
00005350	30	61	32	38	33	37	32	63	33	31	33	34	32	39	30	61	0a28372c3134290a
00005360	32	38	33	37	32	63	33	31	33	35	32	39	30	61	32	38	28372c3135290a28
00005370	33	37	32	63	33	31	33	36	32	39	30	61	32	38	33	37	372c3136290a2837
00005380	32	63	33	31	33	37	32	39	30	61	32	38	33	37	32	63	2c3137290a28372c
00005390	33	31	33	38	32	39	30	61	32	38	33	37	32	63	33	31	3138290a28372c31
000053A0	33	39	32	39	30	61	32	38	33	37	32	63	33	32	33	30	39290a28372c3230
000053B0	32	39	30	61	32	38	33	37	32	63	33	32	33	31	32	39	290a28372c323129
000053C0	30	61	32	38	33	37	32	63	33	32	33	32	32	39	30	61	0a28372c3232290a
000053D0	32	38	33	37	32	63	33	32	33	33	32	39	30	61	32	38	28372c3233290a28

猜测是十六进制，将其转为字符串，下面是转换脚本

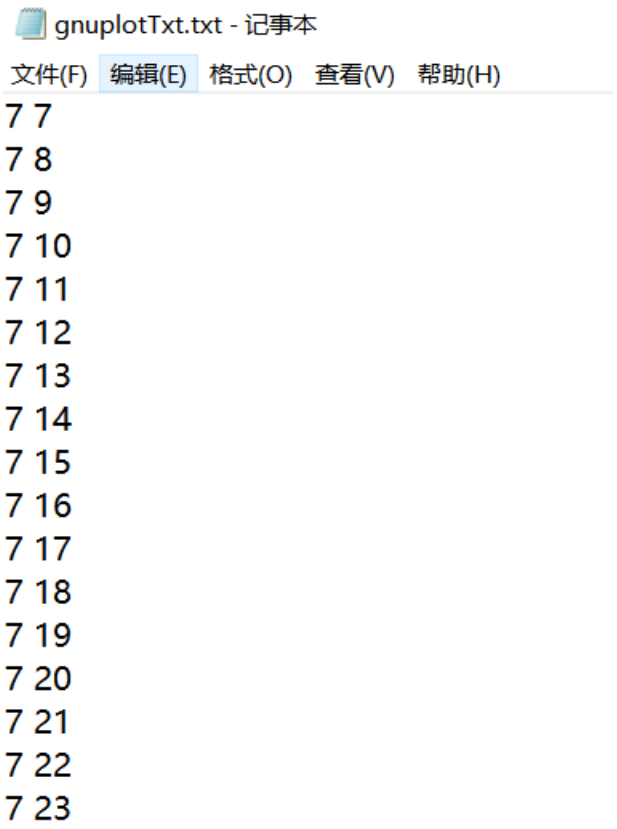
```
with open('hex.txt', 'r') as h:     # hex.txt为要转换的文本文件
    val = h.read()
    h.close()

with open('result.txt', 'w') as re: # 转换完成后写入result.txt
    tem = ''
    for i in range(0, len(val), 2):
        tem = '0x' + val[i] + val[i+1]
        tem = int(tem, base=16)
        print(chr(tem), end="")
        re.write(chr(tem))
    re.close()
```

打开result.txt，发现是一堆坐标

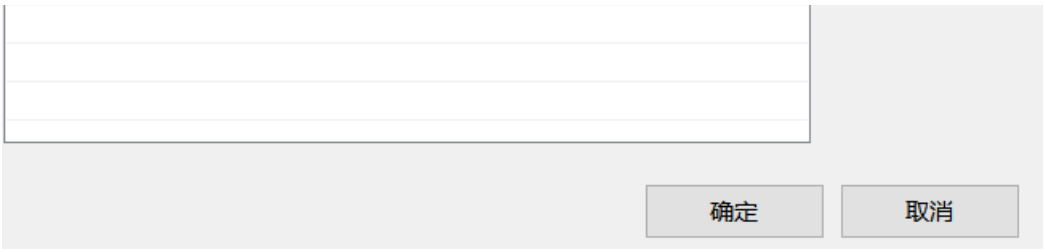


结合之前查看图片属性里的文件信息，发现要画图，所以这里就借用gnuplot来进行绘制(gnuplot下载地址, 提取码：wel5)
不过在使用gnuplot之前需要先将坐标格式转换成gnuplot可以识别的格式，下面是脚本

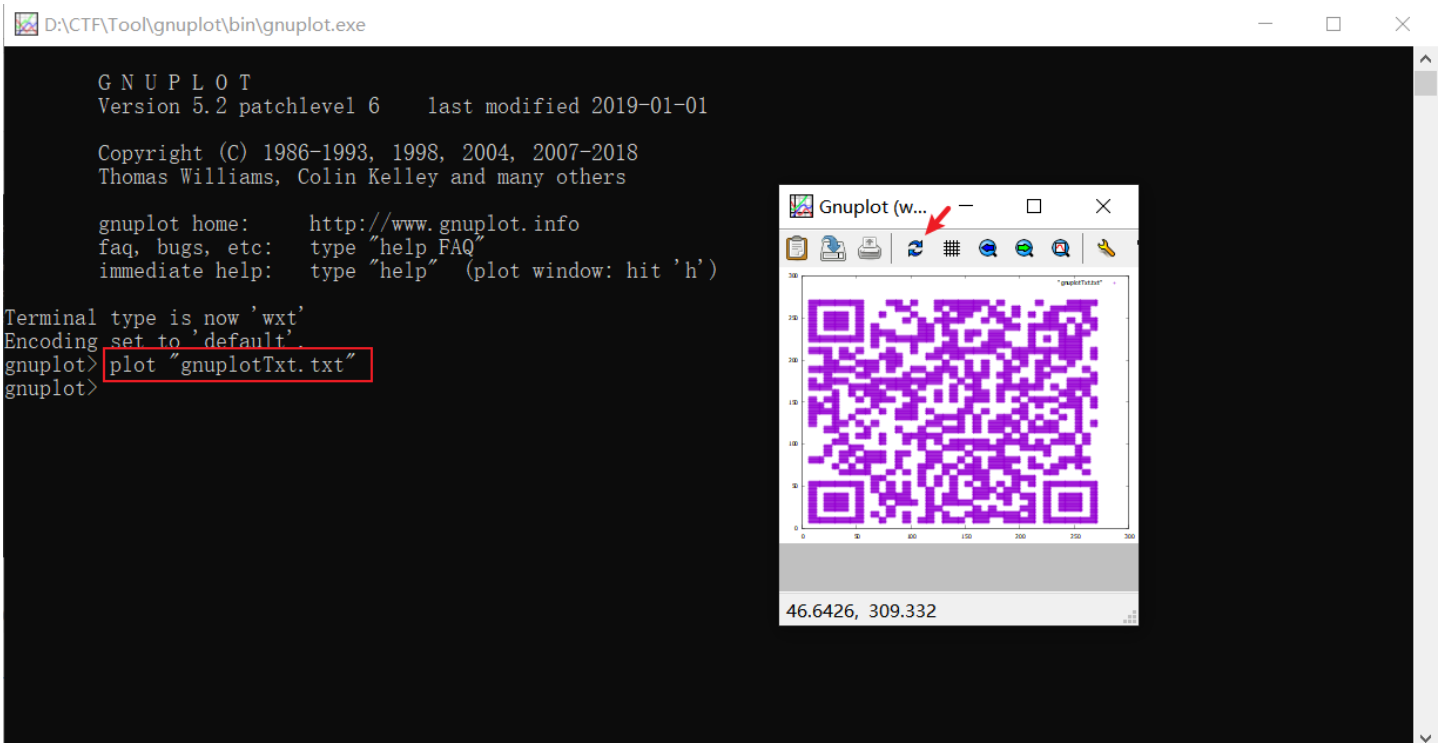
```
with open('result.txt', 'r') as res:  # 坐标格式文件比如(7,7)
    re = res.read()
    res.close()

with open('gnuplotTxt.txt', 'w') as gnup:   # 将转换后的坐标写入gnuplotTxt.txt
    re = re.split()
    tem = ''
    for i in range(0, len(re)):
        tem = re[i]
        tem = tem.lstrip('(')
        tem = tem.rstrip(')')
        for j in range(0, len(tem)):
            if tem[j] == ',':
                tem = tem[:j] + ' ' + tem[j+1:]
        gnup.write(tem + '\n')
    gnup.close()
```



安装好gnuplot后，可以去环境变量里添加变量，之后就可以直接在命令行里运行了



然后在gnuplotTxt.txt所在文件夹打开gnuplot，键入以下命令即可绘图(多用箭头处的重绘功能，调整角度，才能扫出来)



最后扫描二维码即可。

0x03

这题看起来工作量不大，但是需要掌握工具和脚本，还需要多接触工具才能做题。