

Bugku-一段Base64-Writeup

转载

[weixin_30929295](#) 于 2017-07-19 21:03:00 发布 59 收藏

文章标签: [python](#)

原文链接: <http://www.cnblogs.com/WangAoBo/p/7207874.html>

版权

转载请注明出处: <http://www.cnblogs.com/WangAoBo/p/7207874.html>

bugku - 一段Base64 - Writeup

题目:

题目 189 Solves

一段Base64

80

flag格式: flag{xxxxxxxxxxxx}

base64.txt

Key

SUBMIT

分析:

本来看到题目名字和分数以为是一道水题, 后来解的时候才发现有这么多编码方式, 当然如果熟悉这些编码方式找在线工具解得话很快就能拿到flag, 这篇writeup主要是记录一下用python实现所有解码

直接上脚本, 分析过程和编码方式都在注释中

```
1 #coding:utf-8
2 #python 2.7
3 import urllib
4 import re
5
6 #1. 第一层base64
7 with open('base64.txt') as f:
8     cipher1 = f.read()
9     plain1 = cipher1.decode('base64')
10 # print plain1, type(plain1)
11
12 #2. 第二层, 根据plain1的形式(0-7的整数), 推测为8进制加密
13 cipher2 = plain1
14 cipher2 = re.findall(r'\d+', cipher2)
15 # print cipher2
```

```

15 # print cipher2
16 plain2 = ''
17 for i in cipher2:
18     plain2 += chr(int(i, 8))
19 # print plain2
20
21 #3. 第三层, 根据plain2的形式 (\xdd), 推测为16进制加密
22 cipher3 = plain2
23 cipher3 = re.findall(r'\d+', cipher3)
24 # print cipher3
25 plain3 = ''
26 for i in cipher3:
27     plain3 += chr(int(i, 16))
28 # print plain3
29
30 #4. 第四层, 根据plain3的形式 (udd*), 推测为unicode
31 cipher4 = plain3
32 cipher4 = re.findall(r'u[\d\w]+', cipher4)
33 # print cipher4
34 cipher4 = ''.join(cipher4).replace('u', '\u')
35 # print cipher4
36 plain4 = cipher4.decode('unicode-escape').encode('utf-8')#将unicode转中文, 来自知乎
37 # print plain4
38
39 #5. 第五层, 根据plain4形式, 将所有数字转ASCII即可
40 cipher5 = plain4
41 cipher5 = re.findall('\d+', cipher5)
42 # print cipher5
43 plain5 = ''
44 for i in cipher5:
45     plain5 += chr(int(i))
46 # print plain5
47
48 #6. 第六层, 百度plain5的编码格式(&#x)得到解码方法
49 cipher6 = plain5
50 # print cipher6
51 cipher6 = re.findall(r'\d+\w?', cipher6)
52 # print cipher6
53 plain6 = ''
54 for i in cipher6:
55     plain6 += chr(int(i, 16))
56 # print plain6
57
58 #7. 第七层, 百度plain6的编码格式 (&#) 得到解码方法
59 cipher7 = plain6
60 cipher7 = re.findall('\d+', cipher7)
61 # print cipher7
62 flag = ''
63 for i in cipher7:
64     flag += unichr(int(i))
65 # print flag
66 flag = urllib.unquote(flag)
67 print flag

```

运行得到flag

```
C:\Python27\python.exe
flag {ctf_tfc201717qwe}
>>> -
```

再次声明：此题没有必要完全用python实现，此篇writeup只是为了记录python的解密脚本

转载于：<https://www.cnblogs.com/WangAoBo/p/7207874.html>