CTF show MISC base一条龙

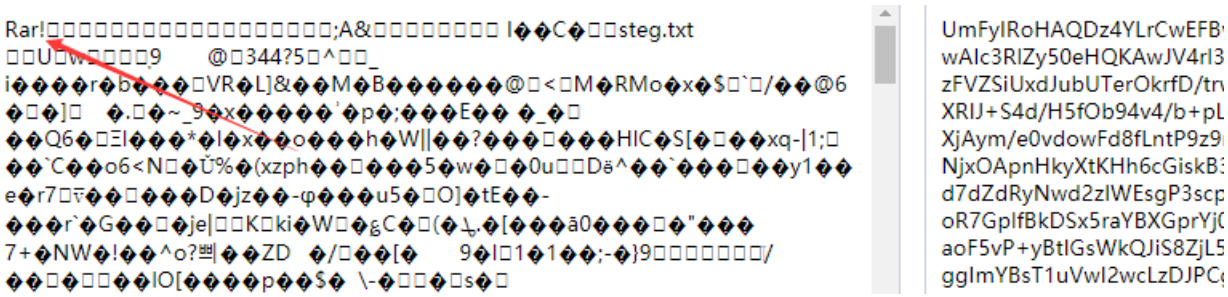
原创

yu22x 于 2020-03-11 10:47:44 发布 1368 收藏 3

题目地址：https://ctf.show

0x01

打开下载下来的文档，base64解码发现关键字 Rar!，然后保存下来解压得到steg.txt



0x02

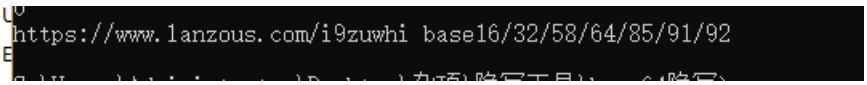
打开steg.txt，发现为一堆base64，解码出来暂时没发现新的可利用信息，尝试base64隐写解密，脚本如下：

```
def get_base64_diff_value(s1, s2):
    base64chars = 'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/'
    res = 0
    for i in xrange(len(s2)):
        if s1[i] != s2[i]:
            return abs(base64chars.index(s1[i]) - base64chars.index(s2[i]))
    return res


def solve_stego():
    with open('1.txt', 'rb') as f:
        file_lines = f.readlines()
        bin_str = ''
        for line in file_lines:
            steg_line = line.replace('\n', '')
            norm_line = line.replace('\n', '').decode('base64').encode('base64').replace('\n', '')
            diff = get_base64_diff_value(steg_line, norm_line)
            print diff
            pads_num = steg_line.count('=')
            if diff:
                bin_str += bin(diff)[2:].zfill(pads_num * 2)
            else:
                bin_str += '0' * pads_num * 2
            print goflag(bin_str)


def goflag(bin_str):
    res_str = ''
    for i in xrange(0, len(bin_str), 8):
        res_str += chr(int(bin_str[i:i + 8], 2))
    return res_str


if __name__ == '__main__':
    solve_stego()
```



运行后结果为网站加提示

0x03

访问网站下载下来文件，看来这是要我们一直用base的各种类型解码了，尝试了一番以后（大概七八次）发现文件还是很大，算了，写个脚本。(说多了都是泪)

```
#author:羽
import base64
import base91
import base58
import py3base92
def hex_to_str(s):
        k=''
        for i in range(0,len(s),2):
                j = s[i]+s[i+1]
                k+=chr(int(j,16))
        print('16')
        return k
```

```
def ba32(s):
        s = base64.b32decode(s)
        s = bytes.decode(s)
        print('32')
        return s

def ba58(s):
        s = base58.b58decode(s)
        s = bytes.decode(s)
        print('58')
        return s

def ba64(s):
        s = base64.b64decode(s)
        s = bytes.decode(s)
        print('64')
        return s

def baa85(s):
        s = base64.a85decode(s)
        s = bytes.decode(s)
        print('a85')
        return s

def bab85(s):
        s = base64.b85decode(s)
        s = bytes.decode(s)
        print('b85')
        return s

def ba91(s):
        s = base91.decode(s)
        s = s.decode()
        print('91')
        return s

def ba92(s):
        s = py3base92.decode(s)
        print('91')
        return s

def start(s):
        for i in range(50):
                if len(s)<50:
                        print(s)
                try:
                        s=hex_to_str(s)
                except:
                        try:
                                s=ba32(s)
                        except:
                                try:
                                        s=ba58(s)
                                except:
                                        try:
                                                s=ba64(s)
                                        except:
                                                try:
                                                        s = baa85(s)
```

```
                                        except:
                                                try:
                                                        s=bab85(s)
                                                except:
                                                        try:
                                                                s = ba92(s)
                                                        except:
                                                                try:
                                                                        s=ba91(s)
                                                                except:
                                                                        print('nonono')

if  __name__=="__main__":
        f = open('BaseAllInOne.txt','r')
        s = f.read()
        start(s)
```

0x04

当出现的值为TkVLTFdUQVpvUlNda1ZXRUpAZVldTltgJCQhLCAgGSknPjc=时base64解码出现乱码，看来这是最后一个了，需要进行写变换，经过询问终于发现原来需要异或。

```
import base64

s='TkVLTFdUQVpvUlNda1ZXRUpAZVldTltgJCQhLCAgGSknPjc='
s=base64.b64decode(s)
for i in range(256):
 flag=""
 k=0
 for j in s:
  res=j^(k+i)
  flag+=chr(res)
  k+=1
 print(i,flag)
```

运行之后在第40条发现flag

PS：base91，base58可以直接pip下载，base85在base64中，base92也可以在pip中下载，但是我的下载下来没法用，于是在网上又下载了py3base92，如果你的也不可以用，可以看下这篇文章下载
py3base92https://blog.csdn.net/Gu_fCSDN/article/details/103427721