

Alictf2014writeup Reverse200 技巧与python简单编程

原创

[dreaming_waiting](#) 于 2015-03-19 11:24:51 发布 769 收藏

分类专栏: [CTF--逆向](#) 文章标签: [CTF reverse python](#)

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/lxx_nico/article/details/44454913

版权



[CTF--逆向](#) 专栏收录该内容

7 篇文章 0 订阅

订阅专栏

Alictf2014writeup Reverse200 技巧与python简单编程

我们发现程序对flag.txt读入, 然后写出来flag.crypt, 观察一下发现它属于单值替换加密的那种类型, 然后逆向分析又没有很好的把加密算法弄出来, 于是我们想把全部的可显字符弄出来, 打一张表, 然后再利用这张表来解官方给的flag.crypt, 一开始把可显字符全部导到txt里面, 结果居然变成了fail!! 不知道为什么, 后来把可显字符分两段, 两次运行, 然后就是Python要上了, 编程打表解密, 刚学Python,虚得很!

```

import os
txt=open("1.txt","rb")
mingwen=txt.read()
mi=open("1.crpyt","rb")
miwen=mi.read()
print mingwen
print miwen
t_spilt=[]
m_spilt=[]
for x in(range(48)):
    t_spilt.append(mingwen[x])
n=0
while n<96:
    m_spilt.append(miwen[n:n+2])
    n=n+2
t2=open("2.txt","rb")
mi2=open("2.crpyt","rb")
mingwen2=t2.read()
miwen2=mi2.read()
print mingwen2
print miwen2
for x in(range(47)):
    t_spilt.append(mingwen2[x])
n2=0
while n2<94:
    m_spilt.append(miwen2[n2:n2+2])
    n2=n2+2
print t_spilt
print m_spilt
j=open("jie.crpyt","rb")
jie=j.read()
k=0
jiestr=[]
while k<64:
    jie_spilt=jie[k:k+2]
    k=k+2
    print m_spilt.index(jie_spilt)
    jiestr.append(t_spilt[m_spilt.index(jie_spilt)])
print ''.join(jiestr)##''.join() list转字符串

```

```

11
4
9
19
a1d1o3i87Qut<#$$^^kb25-+8=csm,%*4

```