第15天：红帽杯2019-XX

原创

S1lenc3 于 2019-11-14 21:50:51 发布 915 收藏
分类专栏： CTF

比赛的时候一道逆向没做出来，ezre还被耍了，也没做出来，这两天搞android，那个AndroidStudio给我整了一天，我哭了，今天复现一道题，一天就这么没了。。。。

XX这道题思路很清晰：

1. 输入
2. 取输入的前四个字符
3. 进行XXTEA加密
4. 通过置换box进行置换
5. 3个为一组做循环异或
6. 和明文比较

难点就是那个XXTEA加密，然后装了一个插件，*FindCrypt*，百度有安装教程。这个插件只能简单识别是TEA加密，XXTEA加密当然是我看了writeup才知道的。

解题思路：

1. 用最后给出的明文写逆算法得到被XXTEA加密后的结果
2. 然后通过网上的脚本进行XXTEA解密，密钥就是输入的前四个字符（我也不知道哪个是密钥哪个是明文，网上都给我整糊涂了，暂且认为“flag”是密钥吧）

置换、异或脚本如下：

```
result = 'CEBC406B7C3A95C0EF9B202091F70235231802C8E75656FA'
res = []
for x in range(0,len(result),2):
    res.append(int(('0x'+result[x]+result[x+1]), 16))
print(res)
s1 = ''
res1 = res
for i in range(0, len(res)):
    d = i // 3
    if d > 0:
        for j in range(d):
            res[i] ^= res1[j]
s2 = ''.join(hex(i)[2:] for i in res)
print(s2)
box = [1,3,0,2,5,7,4,6,9,11,8,10,13,15,12,14,17,19,16,18,21,23,20,22]

res2 = []
for i in range(len(res)):
    res2.append(res[box[i]])
s3 = ''.join(hex(i)[2:] for i in res2)
print(s3)
```

XXTEA解密脚本我是找的java版本的，python很容易实现，但因为想更熟悉java，所以选择java，而且这也耗了不少时间，有些代码不会用，解出来不对，唉，还是自己写出来舒服（今后要好好对待java）。

直接给出代码作者的博客吧：https://blog.csdn.net/z100871519/article/details/79651822

参考文章：

https://blog.csdn.net/z100871519/article/details/79651822

https://impakho.com/post/redhat-2019-online-writeup