# 看雪CTF-2019-Q1

原创

VIP文章 坚强的女程序员 于 2019-04-02 09:39:51 发布 942 收藏

分类专栏： Re



本文链接：https://blog.csdn.net/qq_33438733/article/details/88963542



## 前言

比赛的时候抽空做了几题，赛后花了点时间把RE都做了。除了圆舞曲。

> pizza 实在太强了
> 简略的写写

## 变形金刚

android的逆向，比较简单。最好是拿真机调试。

主要就是根据字符串找到程序流程，然后在so中找到`eq`函数，算法也比较简单，RC4+base64 。

## 初入好望角

.Net 逆向，AES算法识别，其实是Rijndael算法，两者区别不大。

解密最好用C#来写。

## 流浪者

签到题

## 青梅足马

程序比较友好，主要就是RSA算法。需要对RSA的原理有所了解，否则这个数学问题还真不好解决。

## 影分身之术

delphi 程序，内嵌了浏览器，刚开始把我坑了。索性最后找到了webbroswer。

提取出js，解密，最后的回调函数根据特征容易找到。之后是一段简单的rop。

## 圆舞曲

这题卒，不会。

## REPWN

刚开始还以为是个pwn题，也就没做。

前面的几段校验都比较简单。最后一个DES算法的识别，我看到了16个子密钥序列。我用findcrypto没找到DES的特征。作者说用PEID可以识别处DES算法，我试了一下。确实很方便。

## 总结

人与人的差距怎么那么大。