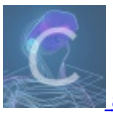
全国大学生信息安全竞赛writeup--拯救地球(reverse500)

原创

Anciety 于 2016-07-10 22:54:28 发布 3337 收藏 2

分类专栏： android security ctf 文章标签： 信息安全

本文链接：https://blog.csdn.net/qq_29343201/article/details/51873996



描述

什么？地球要爆炸了，据说拯救地球的代码就在这个程序里。使命貌似光荣又艰巨…

tips：flag是flag{结果}

附件描述：

文件名：程序

校验（SHA1）：D78073A4C06468DFC95822A764D792C09A87F78A

思路

打开看，一个question,逆向发现加壳了，不过这个壳还好比较裸，目测通过加断点dump dex可行，不过把这个东西自动化了，直接找了一个工具就脱了。

工具地址

破壳之后就是一个字符串，base64加密的，然后输入字符串为param，解密后的字符串为str,答案数组为answer[],验证过程是把一个字符串解密之后，在str里边找到其索引和answer数组依次比较，成功即为答案。那么逆过来就是把answer数组找到在str里边的索引并且打出来，就得到解密后的字符串，然后base64一次。

后记（吐槽）

不要使用网上的在线base64…因为这个耽搁几个小时，最后pwn300有思路都没有时间做了。。。