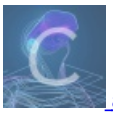
全国大学生信息安全竞赛writeup--珍贵资料(reverse200)

原创

Anciety 于 2016-07-10 22:27:33 发布 6384 收藏 7

分类专栏： android security ctf java android 文章标签： 信息安全 apk



描述

你无意间得到了一些珍贵资料，可惜他们看起来不知道是什么，据说解开它可以得到flag神器。

tips：flag是flag{结果}

附件描述：

文件名：珍贵资料.zip

校验（SHA1）：4EF84DF5B34C12DED8EC3F603CFBC065251864B4

思路

一个压缩文件，打开解压得到unknown和unknown2，unknown2是一个apk,unknown不知道是啥。安装apk得到一个登陆界面，jeb查看，发现有好几个activity.loginActivity用来登陆。登陆的检测是通过USER_NAME和输入的用户名直接比较，然后PASSWORD和加密之后的输入进行比较。加密过程

```
public static String Encryption(String s) {
        String v5;
        StringBuilder v4 = new StringBuilder();
        if(s == null || s.length() < 1) {
            System.out.println("you Input nothing.");
            v5 = null;
        }
        else {
            s = s.toLowerCase();
            int v3 = s.length();
            int v2;
            for(v2 = 0; v2 < v3; ++v2) {
                int v0 = "ijklmstuvwxyz0123abcdenopqrfgh456789".indexOf(s.charAt(v2));
                if(v0 == LoginActivity.LEN - 1) {
                    v0 = -1;
                }

                if(v0 == LoginActivity.LEN - 2) {
                    v0 = -2;
                }

                if(v0 == LoginActivity.LEN - 3) {
                    v0 = -3;
                }

                v4.append("ijklmstuvwxyz0123abcdenopqrfgh456789".charAt(v0 + 3));
            }

            v5 = v4.toString();
        }

        return v5;
    }

其中
 public static final String SOURCE = "ijklmstuvwxyz0123abcdenopqrfgh456789";
```

可是用来比较的用户名和密码哪里来的呢？ 打开unknown，二进制文件，不过可以看到文件头，是android backup。有一个工具是android-backup-extract-master，github上有，下下来，自己编译一下，打开unknown,就可以得到一个xml文件里边写了用户名和密码了。

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <string name="PASSWORD">dudqlvqrero1</string>
    <string name="USER_NAME">user</string>
</map>
```

根据加密规则，比较简单直接写出逆算法

```
    public static String Decryption(String arg) {

            String str = "ijklmstuvwxyz0123abcdenopqrfgh456789";
            StringBuilder stringBuilder = new StringBuilder();

            for (int i = 0;i < arg.length();i++) {
                int x = str.indexOf(arg.charAt(i));
                if (x - 3 == -1) {
                    x = Main.LEN - 1;
                }

                if (x - 3 == -2) {
                    x = Main.LEN - 2;
                }

                if (x - 3 == -3) {
                    x = Main.LEN - 3;
                }
                stringBuilder.append(str.charAt(x - 3));
            }

            return stringBuilder.toString();
        }
```

得到字符串为amanisnobody。其实试一下会发现这就是flag..然而如果有空看看另外的一个没用的activity会有一个简单的加密，是用的异或，再异或回来会发现。。这确实就是flag。