《XCTF》MOBILE--app3解题

原创

路人。你好 于 2022-02-12 18:01:12 发布 799 收藏
文章标签： android webview android studio

1.下载下来发现是.ab文件。.ab文件为安卓备份文件，可能会被加密，此处没有加密

下载android-backup-extractor

文件夹中执行

```
java -jar abe.jar unpack app3.ab app3.tar
```

```
F:\逆向\案例\CTF\app3>java -jar abe.jar unpack app3.ab app3.tar
0% 1% 2% 3% 4% 5% 6% 7% 8% 9% 10% 11% 12% 13% 14% 15% 16% 17% 18% 19% 20% 21% 22% 23% 24% 25% 26% 27% 28% 29% 30% 31% 32
% 33% 34% 35% 36% 37% 38% 39% 40% 41% 42% 43% 44% 45% 46% 47% 48% 49% 50% 51% 52% 53% 54% 55% 56% 57% 58% 59% 60% 61% 62
% 63% 64% 65% 66% 67% 68% 69% 70% 71% 72% 73% 74% 75% 76% 77% 78% 79% 80% 81% 82% 83% 84% 85% 86% 87% 88% 89% 90% 91% 92
% 93% 94% 95% 96% 97% 98% 99% 100%
9097216 bytes written to app3.tar.
```


得到bask.apk，.db文件，将apk文件拖入到jadx中

```
        edit.putString("Is_Encroty", "1");
        edit.putString("Encryto", "SqlCipher");
        edit.putString("ver_sion", "3_4_0");
        edit.apply();
        a();
    }

    private void a() {
        SQLiteDatabase.loadLibs(this);
        this.b = new a(this, "Demo.db", null, 1);
        ContentValues contentValues = new ContentValues();
        contentValues.put("name", "Stranger");
        contentValues.put("password", (Integer) 123456);
        a aVar = new a();
        String a2 = aVar.a(contentValues.getAsString("name"), contentValues.getAsString("password"));
        this.a = this.b.getWritableDatabase(aVar.a(a2 + aVar.b(a2, contentValues.getAsString("password")))).substring(
        this.a.insert("TencentMicrMsg", null, contentValues);
    }

    public void onClick(View view) {
        if (view == this.c) {
            Intent intent = new Intent();
            intent.putExtra("name", "name");
            intent.putExtra("password", "pass");
            intent.setClass(this, AnotherActivity.class);
            startActivity(intent);
        }
```


2.

3.对a()函数进行分析

加载了数据库，然后创建了一个a的对象，于是进行对这个类的查看

```java
/* compiled from: DatabaseManager */
public class a extends SQLiteOpenHelper {
    private int a = 0;

    public a(Context context, String str, SQLiteDatabase.CursorFactory cursorFactory, int i) {
        super(context, str, cursorFactory, i);
    }

    @Override // net.sqlcipher.database.SQLiteOpenHelper
    public void onCreate(SQLiteDatabase sQLiteDatabase) {
        sQLiteDatabase.execSQL("create table TencentMicrMsg(name text,password integer,F_l_a_g text)");
    }

    @Override // net.sqlcipher.database.SQLiteOpenHelper
    public void onUpgrade(SQLiteDatabase sQLiteDatabase, int i, int i2) {
    }
```


一步一步跟进到算法

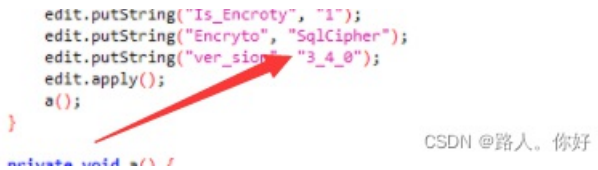
```java
/* compiled from: SHA1Manager */
public class b {
    public static final String a(String str) {
        char[] cArr = {'0', '1', '2', '3', '4', '5', '6', '7', '8', '9', 'a', 'b', 'c', 'd', 'e', 'f'};
        try {
            byte[] bytes = str.getBytes();
            MessageDigest instance = MessageDigest.getInstance("MD5");
            instance.update(bytes);
            byte[] digest = instance.digest();
            int length = digest.length;
            char[] cArr2 = new char[(length * 2)];
            int i = 0;
            for (byte b : digest) {
                int i2 = i + 1;
                cArr2[i] = cArr[(b >>> 4) & 15];
                i = i2 + 1;
                cArr2[i2] = cArr[b & 15];
            }
            return new String(cArr2);
        } catch (Exception e) {
            return null;
        }
    }

    public static final String b(String str) {
        char[] cArr = {'0', '1', '2', '3', '4', '5', '6', '7', '8', '9', 'a', 'b', 'c', 'd', 'e', 'f'};
        try {
            byte[] bytes = str.getBytes();
            MessageDigest instance = MessageDigest.getInstance("SHA-1");
            instance.update(bytes);
            byte[] digest = instance.digest();
            int length = digest.length;
            char[] cArr2 = new char[(length * 2)];
            int i = 0;
            for (byte b : digest) {
                int i2 = i + 1;
                cArr2[i] = cArr[(b >>> 4) & 15];
                i = i2 + 1;
                cArr2[i2] = cArr[b & 15];
            }
            return new String(cArr2);
        } catch (Exception e) {
            return null;
        }
    }
```


4.代码过来到idea，新建java，修改跑一下。得到 ”**ae56f99**“

5.使用SQLite打开数据库（此处有坑）

一定要选择3，因为代码中已经给出版本



打开数据

看起来有点像base64加密

总结：题目不难但是涉及到的东西比较多，代码比较繁琐。在反编译的时候，jadx有部分代码没有反编译成功，jeb可以。