《XCTF》MOBILE--app3解题



<u>路人。你好</u> 于 2022-02-12 18:01:12 发布 文章标签: <u>android webview android studio</u> 版权声明:本文为博主原创文章,遵循<u>CC 4.0 BY-SA</u>版权协议,转载请附上原文出处链接和本声明。 本文链接: <u>https://blog.csdn.net/weixin_43729769/article/details/122899344</u> 版权

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% 33
% 33% 34% 35% 36% 37% 33% 39% 40% 41% 42% 43% 44% 45% 46% 47% 48% 49% 50% 51% 52% 53% 54% 55% 56% 57% 58% 59% 60% 61% 63
% 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% 93
% 93% 94% 95% 96% 97% 98% 99% 100%
9097216 bytes written to app3.tar.
CSDN @路人。你好
```

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("wor size" "To the "");
          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);
                                                                                                 CSDN @路人。你好
              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

```
/* 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);
    3
    @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) {
                                                                                                   CSDN @路人。你好
一步一步跟进到算法
   /* compiled from: SHA1Manager */
10
  public class b {
      public static final String a(String str) {
11
           char[] cArr = {'0', '1', '2', '3', '4', '5', '6', '7', '8', '9', 'a', 'b', 'c', 'd', 'e', 'f'};
12
           try
15
               byte[] bytes = str.getBytes();
16
               MessageDigest instance = MessageDigest.getInstance("MD5");
17
               instance.update(bytes);
               byte[] digest = instance.digest();
18
٤9
               int length = digest.length;
20
               char[] cArr2 = new char[(length * 2)];
               int i = 0;
               for (byte b : digest) {
                   int i2 = i + 1;
24
24
                   cArr2[i] = cArr[(b >>> 4) & 15];
                   i = i2 + 1;
25
                   cArr2[i2] = cArr[b & 15];
25
27
               return new String(cArr2);
           } catch (Exception e) {
29
               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'};
32
33
           try {
               byte[] bytes = str.getBytes();
36
37
               MessageDigest instance = MessageDigest.getInstance("SHA-1");
38
               instance.update(bytes);
               byte[] digest = instance.digest();
39
10
               int length = digest.length;
               char[] cArr2 = new char[(length * 2)];
41
               int i = 0;
               for (byte b : digest) {
45
                  int i2 = i + 1;
                   cArr2[i] = cArr[(b >>> 4) & 15];
15
16
                   i = i2 + 1;
                   cArr2[i2] = cArr[b & 15];
46
18
               return new String(cArr2);
          } catch (Exception e) {
50
               return null;
                                                                                                       CSDN @路人。你好
      }
```

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)

💽 SQLCipher 加額	호 ·			?
请输入加密数据库的 如果此数据库的任(密码(P)	的密码。 可其他设置发生变化,您也需要提	供此信息。	[」 令
加密设置(型)	● <mark>SQLCipher 3 默认</mark>	○ SQLCipher 4 默认	〇 自定义(114)	
页大小(Z)	, 024			
KDF迭代(<u>K</u>)	64000			
HMAC算法	SHA1			
KDF算法	SHA1			
纯文本文件头大小	0		CSDN @路人。你如	-

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

清空 加密 解密 ■解密为UTF-8字节流	
清空 加密 解密 ■解密为UTF-8字节流	
清空 加密 解密 □ 解密为UTF-8字节流	
Tetf (H2110 De VOu Lew2 Tere2nt)	

CSDN @路人。你好

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。