

XCTF MOBILE 新手 app3



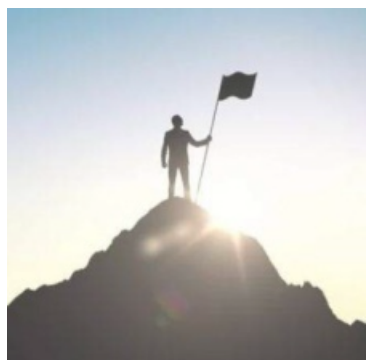
A_dmins 于 2019-10-03 01:15:50 发布 931 收藏 1

分类专栏: CTF题 XCTF

版权声明: 本文为博主原创文章, 遵循 CC 4.0 BY-SA 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/qq_42967398/article/details/101949942

版权



CTF题 同时被 2 个专栏收录

115 篇文章 11 订阅

订阅专栏



XCTF

24 篇文章 0 订阅

订阅专栏

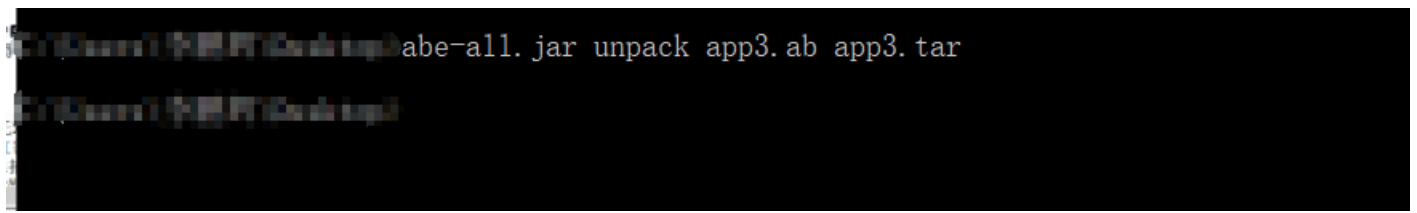
XCTF MOBILE 新手 app3

没事做, 随便玩玩, 谁知道一玩就是一晚上

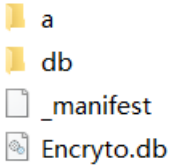
下载下来是个.ab文件, emmm, 直接使用notepad++查看一下:

```
app3.ab
1 ANDROID BACKUP
2 2
3 1
4 none
5 xPz鋸搗 舛?
6 PSC]cPWXa0:G栉"=ACK始翻? 0F#(*e燻?F#?H歷STX瀧嶺沂箭<9讚函慷蔚u)??景熈E ?Q
7 ?程ANCO?燻?* 宰#@FNAR鄔
8 BSV7g馬線R韻越BSE)xCOI苙?7DIB?ee慘DIB%UNAR???Q
9 ?CU?e銘梧'佼 敵) BMRiBOIrr?粮PFBSTU?BY至 ?囉BM經N温?妮惟?矯?e? b(?)鵠刹NAK糧DC1STX 曰疇 t闊~ <DIBedcBOIc
10 ' ?|?)'招爾@哇 莩各nDC3忍苦Q线量?阆鷓 J1 婪'秘VN RSBJ佗您壞符富WM候焘/<DC2X?Jht農 謎志娛兹枉RS 7?>?跟j;鶻?減|穆側~楮FSu傷馴絨:
11 BMV1福駐吝錫JVnd杣??K^n???程?藥化馱3s??農hi USA?x xz%???舖SOH拙???胎= 磔?靴-N位BOIqGS 脫塵>?瘳ACKH萬v'??VN?VNa煥SGBXVFF?"幘v??:
12 9Q
13 賤/巖窳銜\ε吧}<]: 钟 y準尾B盾qu?溢 , 洌?w]! 兎^宥?oO輯離J阿(SB!)?錯
14 涇德樺9SUBGS个z'鏽es爾
15 <翰?鈹 Zrb\替STX ??B璽wf繁D RS2墮滋礁離?PSC?案砌BFr3S1棚@液?D>HDC3?設 DC2揆SYN!縷 4`h<?继餽?SUBz 嗎 墙i? 進緝DC1NUU'曠gtSUBa
16 [鋪BFBRSWw餞衍籟?ESC... 槐 ?{ 悻?Kwz蝓O, 1覓劫h鐵]'燻麦鴉??專F
17 標RS?V歸"/領?3J?iGNO$!cm's樺繩九|?顯蚌蝦DC3DC3筓 ST甲X)! 嫗馭s&?U茲2鯨hw闕賀浙xf喲NUUs鈔岛z彪EStUS筊cVR混柁??ESC^} 9]BTX膠GSR 規y
18 貞到v?Q
19 賔I??DC1] 例--BNQ?>.t 脉朝狄?EX膏DDB祀NUU逃DC1維鄴/噉US7B瑯佑豚e[BXRu?+.k梨柳艺z再BX帥齶SO窵亘k诙?羽?0'冠?GS鄣陸* w, 褻葶v!吹○BF
20 潯I走○筵DC1?榕jQ病?,q&NJ犀DDEfNUU?痘雌碌?肱胖浯&?BNC 僅$?特缺B277辟-?撥VNJ槓9DIB2?Sm 4+~CS4
21 篙歎^?)遂BFI翁曹綺械9 V滢Ii?ACK煒轟*駟 ]靚/勃肥/DC1RS.?'誼|結譽椒彗7嘉苧諸 腥晚敷高部?*t耗# / 1豔 半vEP^疥O3殮KSYN豈?載憤斬"熬z+3
22 9 8?湿BFI? 1批岸 l'デDC3@e滔釅劬? sJ?脛?紫w匪桐m
23 ?狹覓羌SYN?*cR KDC3滿?站v孀J w浚潔GSSWXv2_g?F (?SOHh瘳脊祠?z慕 BBJE雅髒呀z涯酪*敵eDC1瀆c復RSr>磳嶼?潰?e?BS?林STXDC2麟]脍HQCBSO 柁姘
24 慈mo?Q?x|?VWl叫DC4? ?備燻u壘GAN改CS?i益NUU帛U
25 ?胤勇馴^Y'黉<2?2娘續{& o'U讀&YC坡噫?DC3?丹蕪BM/綽
26 ? PAFBSUB蓆乱o'繼m;"SUB(郵舩+伴DC3賊涪~&oAG, DIB?..?Q
27 Ci=?Q
28 ?槍z孰萝SI?z&崖隆?? Esj SQPpG?夕'ESC0DB?SWX?御'惡門N閏節BOLQ ?DC4祝澗n碓B+|抵膃iL ?SI狂NCAN#檳熟I捺SUBe搵畔 ,SOB?紗~帶矿孺起絨?
29 6BS筮嶢弟航t繇喋'?'闊魏嘲BOI?'J'炯v *梘舞 雉BSCBSB'戲襪趁l閏zb棗李y猗v端坐BVB萃K 藩錢營9問?鱒娛、 6B'說軒斬龜冬?韻/燧醜礙斌?饋"m隼
30 鷗] 視'Hs焔?Q
31 銀\?7
32 T/<?BFI窟gI誨姐?Q
33 ??BMCAL嶮煨>?BFB'皴RSRSD'造 駁?擇H研[DC3N?鶻CS鏽犀? 劾?zh [Gc'界脛駒宅煇*
34 ,雙{厚NAR{^鼻L頰顯Pas沃酪電區矩ng類1 鯢濡?.解NUU?
35 )CANH依J?僂oz床認BNO郑B捲oIcSIXp爿 恣披囁[采2a1BFB3詠k試形C汗DC3英7踰&.k呼徒USEB權詁bSI?DC2速遜?RS那_k格?調?閏ES席d?錫94棍蠶愚?Q
36 Gc'界脛駒宅煇*
length: 8843083 lines: 6 Ln: 2 Col: 2 Sel: 0|0 UNIX ANSI INS
```

emmm, 不知道是啥文件, 经过百度查找得知是apk的备份文件
可以使用abe.jar进行反编译, 直接使用工具:



解压最后可以得到这些文件:



在a文件夹中找到了apk文件, 直接使用APKIDE打开, 直接使用java反编译得到主函数:

```
private SQLiteDatabase a;
private a b;
private Button c;

private void a()
{
    SQLiteDatabase.loadLibs(this);
    this.b = new a(this, "Demo.db", null, 1);
    ContentValues localContentValues = new ContentValues();
    localContentValues.put("name", "Stranger");
    localContentValues.put("password", Integer.valueOf(123456));
    Object localObject = new com.example.yaphetshan.tencentwelcome.a.a();
    String str1 = ((com.example.yaphetshan.tencentwelcome.a.a)localObject).a(localContentValues.getAsString("name"), localContentValues.getAsString("password"));
    String str2 = ((com.example.yaphetshan.tencentwelcome.a.a)localObject).b(str1, localContentValues.getAsString("password"));
    localObject = ((com.example.yaphetshan.tencentwelcome.a.a)localObject).a(str1 + str2);
    this.a = this.b.getWritableDatabase(((String)localObject).substring(0, 7));
    this.a.insert("TencentMicrMsg", null, localContentValues);
}

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

protected void onCreate(Bundle paramBundle)
{
    super.onCreate(paramBundle);
    setContentView(2130968603);
    this.c = ((Button)findViewById(2131427417));
    this.c.setOnClickListener(this);
    paramBundle = getSharedPreferences("test", 0).edit();
    paramBundle.putString("Is_Encroty", "1");
    paramBundle.putString("Encrypto", "SqlCipher");
    paramBundle.putString("ver_sion", "3_4_0");
    paramBundle.apply();
    a();
}
```

好像是连接数据库啥的, , , , emmmm看样子还调用了a类和b类
直接去看看:

```
package com.example.yaphetshan.tencentwelcome.a;

public class a
{
    private String a = "yaphetshan";

    public String a(String paramString)
    {
```

```

    new b();
    return b.b(paramString + this.a);
}

public String a(String paramString1, String paramString2)
{
    paramString1 = paramString1.substring(0, 4);
    paramString2 = paramString2.substring(0, 4);
    return paramString1 + paramString2;
}

public String b(String paramString1, String paramString2)
{
    new b();
    return b.a(paramString1);
}
}

```

https://blog.csdn.net/qq_42967398

b类太长了就不截图了，粗略地看了下里面好像有两个加密的函数

```

for (;;)
{
    Object localObject;
    int k;
    int j;
    try
    {
        paramString = paramString.getBytes();
        localObject = MessageDigest.getInstance("MD5");
        ((MessageDigest)localObject).update(paramString);
        paramString = ((MessageDigest)localObject).digest();
        k = paramString.length;
        localObject = new char[k * 2];
        j = 0;
    }
    catch (Exception paramString)
    {
        return null;
    }
    paramString = new String((char[])localObject);
    return paramString;
    while (i < k)
    {
        int m = paramString[i];
        int n = j + 1;
        localObject[j] = arrayOfChar[(m >>> 4 & 0xF)];
        j = n + 1;
        localObject[n] = arrayOfChar[(m & 0xF)];
        i += 1;
    }
}
}

```

https://blog.csdn.net/qq_42967398

```

for (;;)
{
    Object localObject;
    int k;
    int j;
    try
    {
        paramString = paramString.getBytes();
        localObject = MessageDigest.getInstance("SHA-1");
        ((MessageDigest)localObject).update(paramString);
        paramString = ((MessageDigest)localObject).digest();
        k = paramString.length;
        localObject = new char[k * 2];
        j = 0;
    }
    catch (Exception paramString)
    {
        return null;
    }
}

```

```

paramString = new String((char[])localObject);
return paramString;
while (i < k)
{
    int m = paramString[i];
    int n = j + 1;
    localObject[j] = arrayOfChar[(m >>> 4 & 0xF)];
    j = n + 1;
    localObject[n] = arrayOfChar[(m & 0xF)];
    i += 1;
}
}
}

```

https://blog.csdn.net/qq_42967398

到这里思绪还是乱的，，，，，

稍微整理一下，，，要确定我们接下来该干嘛！！

首先我们是能看见有数据库的，也就是.db文件

我们使用DB Browser for SQLite打开数据库文件发现需要密码，，，ok，现在目标应该明确了

应该是要我们将密码给找出来，然后读取数据库中的内容，因为这里有提示：

```

public void onCreate(SQLiteDatabase paramSQLiteDatabase)
{
    paramSQLiteDatabase.execSQL("create table TencentMicrMsg(name text,password integer,F_l_a_g text)");
}

```

我们接下来又返回到主函数，，，，，

```

private void a()
{
    SQLiteDatabase.loadLibs(this);
    this.b = new a(this, "Demo.db", null, 1);
    ContentValues localContentValues = new ContentValues();
    localContentValues.put("name", "Stranger");
    localContentValues.put("password", Integer.valueOf(123456));
    Object localObject = new com.example.yaphetshan.tencentwelcome.a.a();
    String str1 = ((com.example.yaphetshan.tencentwelcome.a.a)localObject).a(localContentValues.getAsString("name"), localContentValues.getAsString("password"));
    String str2 = ((com.example.yaphetshan.tencentwelcome.a.a)localObject).b(str1, localContentValues.getAsString("password"));
    localObject = ((com.example.yaphetshan.tencentwelcome.a.a)localObject).a(str1 + str2);
    this.a = this.b.getWritableDatabase(((String)localObject).substring(0, 7));
    this.a.insert("TencentMicrMsg", null, localContentValues);
}

```

https://blog.csdn.net/qq_42967398

首先调用了a文件夹中的a类，三个构造函数都调用了

两个字符串进行一系列操作，然后传入getWritableDatabase（）函数

觉得getWritableDatabase这个函数很可疑！！！截取7个字符！！会不会就是数据库的密码呢

首先是给了我们明文的！！name和password，分别是Stranger和123456

进到a类中去查看一下构造函数：

```

public class a
{
    private String a = "yaphetshan";

    public String a(String paramString)
    {
        new b();
        return b.b(paramString + this.a);
    }

    public String a(String paramString1, String paramString2)
    {
        paramString1 = paramString1.substring(0, 4);
        paramString2 = paramString2.substring(0, 4);
        return paramString1 + paramString2;
    }

    public String b(String paramString1, String paramString2)
    {

```

```
new b();  
return b.a(paramString1);  
}  
}
```

https://blog.csdn.net/qq_42967398

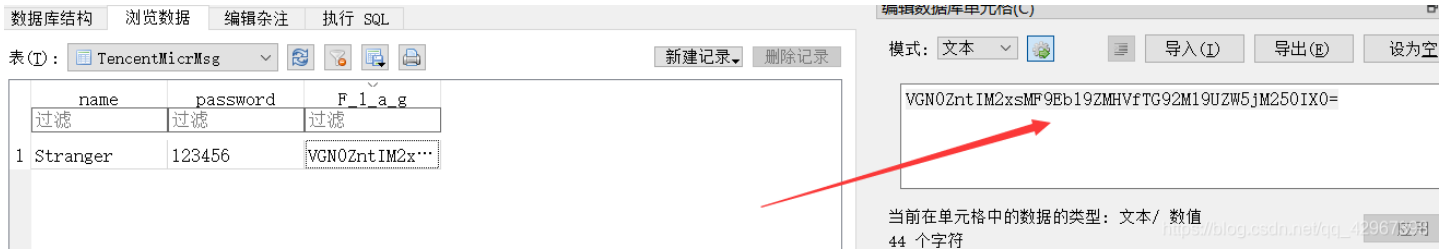
可以很明显的看到三个构造函数根据传入的字符串进行了不同的操作
刚刚b类中的两个函数也用到了，感觉那7个字符的应该就是密码了~~
我们直接将密码生成两个函数模拟一下，重现一下算法生成密码，利用python:

```
import hashlib  
  
def md5a(string):  
    tmp = "0123456789abcdef"  
    md5value = hashlib.md5(string.encode('utf-8')).digest()  
    k = len(md5value)  
    i = 0  
    j = 0  
    str = [0]*k*2  
    while i < k:  
        m = md5value[i]  
        n = j + 1  
        str[j] = tmp[(m >> 4 & 0xf)]  
        j = n + 1  
        str[n] = tmp[(m & 0xf)]  
        i += 1  
    return "".join(str)  
  
def shab(string):  
    tmp = "0123456789abcdef"  
    shavalue = hashlib.sha1(string.encode('utf-8')).digest()  
    k = len(shavalue)  
    i = 0  
    j = 0  
    str = [0]*k*2  
    while i < k:  
        m = shavalue[i]  
        n = j + 1  
        str[j] = tmp[(m >> 4 & 0xf)]  
        j = n + 1  
        str[n] = tmp[(m & 0xf)]  
        i += 1  
    return "".join(str)  
  
a = "yaphetshan"  
str1 = "Stra1234"  
str2 = md5a(str1)  
print(shab(str1+str2+a)[0:7])
```

运行得到密码:

```
python 1.py  
ae56f99
```

再次利用DB Browser for SQLite打开数据库，输入密码ae56f99成功进入，找到数据:



经过base64解密:

base16、base32、base64

VGN0ZntIM2xsMF9Eb19ZMHVfTG92M19UZW5jM250IX0=

编码 字符集

Tctf{H3110_Do_Y0u_Lov3_Tenc3nt!}

得到flag: Tctf{H3110_Do_Y0u_Lov3_Tenc3nt!}

我是真的服了，这种题目是给新手做的吗?? 日了狗了，看看评论都，，， 太难了啊



古月浪子 11 小时前

这道题放一般的比赛里，完全有资格成为防AK题了吧-_-...

← 回复

👍 0



cn.zzh 3 个月前

好难啊，需要的知识点太多了

← 回复

👍 1

https://blog.csdn.net/qq_42967398