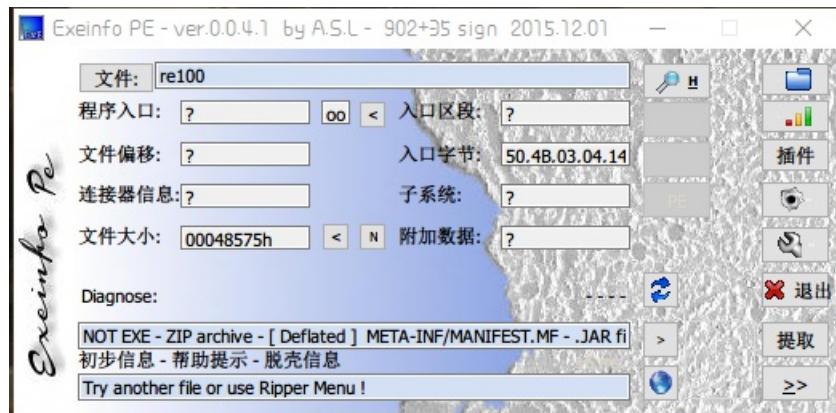


JCTF 2014 小菜一碟

原创

Hk_Mayfly 于 2019-10-12 00:00:00 发布 208 收藏
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_39542714/article/details/106834771
版权
测试文件：<https://static2.ichunqiu.com/icq/resources/fileupload//CTF/JCTF2014/re100>

1.准备



获得信息

- ZIP文件
- Java文件

用解压文件打开

	名称	压缩后大小	原始大小	类型
	META-INF			
> res	AndroidManifest.xml	642	1,704	XML 文档
	classes.dex	252,678	581,796	DEX 文件
	resources.arsc	2,368	2,368	ARSC 文件

获得信息

- APK文件

2.Smali2JavaUI打开

The screenshot shows the Android studio interface. On the left is the project tree with a folder named 're100.apk' containing a 'src' folder with packages 'android', 'com', and 'example'. Under 'example' is a 'encoding' package containing 'BuildConfig.java', 'MainActivity.java' (which is selected and highlighted with a red border), 'MyDialog.java', and 'R.java'. At the top, there are tabs for 'BuildConfig.java', 'R.java', 'MyDialog.java', and 'MainActivity.java'. The code editor on the right displays the content of 'MainActivity.java'.

```
/**  
 * Generated by smali2java 1.0.0.558  
 * Copyright (C) 2013 Hensence.com  
 */  
  
package com.example.encoding;  
  
import android.app.Activity;  
import android.widget.Button;  
import android.widget.EditText;  
import java.security.NoSuchAlgorithmException;  
import java.security.MessageDigest;  
import android.util.Base64;  
import android.os.Bundle;  
import android.view.View;  
import android.view.Menu;  
import android.view.MenuInflater;  
  
1 /**  
2  * Generated by smali2java 1.0.0.558  
3  * Copyright (C) 2013 Hensence.com  
4 */  
5  
6 package com.example.encoding;  
7  
8 import android.app.Activity;  
9 import android.widget.Button;  
10 import android.widget.EditText;  
11 import java.security.NoSuchAlgorithmException;  
12 import java.security.MessageDigest;  
13 import android.util.Base64;  
14 import android.os.Bundle;  
15 import android.view.View;  
16 import android.view.Menu;  
17 import android.view.MenuInflater;  
18  
19 public class MainActivity extends Activity {  
20     private Button button;  
21     private MyDialog dialog1;  
22     private MyDialog dialog2;  
23     private MyDialog dialog3;  
24     private EditText edittext;  
25     private StringBuffer str;  
26  
27     protected void onCreate(Bundle savedInstanceState) {  
28         super.onCreate(savedInstanceState);  
29         setContentView(0x7f030000);  
30         dialog1 = new MyDialog(this, "try again");  
31         dialog2 = new MyDialog(this, "congratulations, you success!!!");  
32         dialog3 = new MyDialog(this, "sorry,please try again");  
33         edittext = (EditText)findViewById(0x7f080000);  
34         button = (Button)findViewById(0x7f080001);  
35         button.setOnClickListener(new View.OnClickListener(this) {  
36  
37             1(MainActivity p1) {  
38                 }  
39  
40                 public void onClick(View v) {  
41                     MyDialog dialog3 = this$0new StringBuffer(edittext.getText().toString());  
42                     str = localString1;  
43                     if(str.length() < 0x5) {  
44                         edittext.setText("");  
45                         dialog3.show();  
46                     }  
47                 }  
48             }  
49         );  
50     }  
51  
52     public void onClick(View v) {  
53         MyDialog dialog3 = this$0new StringBuffer(edittext.getText().toString());  
54         str = localString1;  
55         if(str.length() < 0x5) {  
56             edittext.setText("");  
57             dialog3.show();  
58         }  
59     }  
60 }  
61
```

```
1 /**  
2  * Generated by smali2java 1.0.0.558  
3  * Copyright (C) 2013 Hensence.com  
4 */  
5  
6 package com.example.encoding;  
7  
8 import android.app.Activity;  
9 import android.widget.Button;  
10 import android.widget.EditText;  
11 import java.security.NoSuchAlgorithmException;  
12 import java.security.MessageDigest;  
13 import android.util.Base64;  
14 import android.os.Bundle;  
15 import android.view.View;  
16 import android.view.Menu;  
17 import android.view.MenuInflater;  
18  
19 public class MainActivity extends Activity {  
20     private Button button;  
21     private MyDialog dialog1;  
22     private MyDialog dialog2;  
23     private MyDialog dialog3;  
24     private EditText edittext;  
25     private StringBuffer str;  
26  
27     protected void onCreate(Bundle savedInstanceState) {  
28         super.onCreate(savedInstanceState);  
29         setContentView(0x7f030000);  
30         dialog1 = new MyDialog(this, "try again");  
31         dialog2 = new MyDialog(this, "congratulations, you success!!!");  
32         dialog3 = new MyDialog(this, "sorry,please try again");  
33         edittext = (EditText)findViewById(0x7f080000);  
34         button = (Button)findViewById(0x7f080001);  
35         button.setOnClickListener(new View.OnClickListener(this) {  
36  
37             1(MainActivity p1) {  
38                 }  
39  
40                 public void onClick(View v) {  
41                     MyDialog dialog3 = this$0new StringBuffer(edittext.getText().toString());  
42                     str = localString1;  
43                     if(str.length() < 0x5) {  
44                         edittext.setText("");  
45                         dialog3.show();  
46                     }  
47                 }  
48             }  
49         );  
50     }  
51  
52     public void onClick(View v) {  
53         MyDialog dialog3 = this$0new StringBuffer(edittext.getText().toString());  
54         str = localString1;  
55         if(str.length() < 0x5) {  
56             edittext.setText("");  
57             dialog3.show();  
58         }  
59     }  
60 }  
61
```

```

45             dialog1.showDialog();
46             return;
47         }
48         str.reverse();
49         Log.i("ClownQiang", localString1.append(new String(str)).toString());
50         String md5_string = encode(new String(str));
51         Log.i("ClownQiang", str);
52         String base64 = getBASE64(md5_string).trim();
53         Log.i("ClownQiang", md5_string);
54         if(base64.equalsIgnoreCase("NzU2ZDJmYzg0ZDA3YTM1NmM4ZjY4ZjcxZmU3NmUxODk=")) {
55             dialog2.showDialog();
56             return;
57         }
58         edittext.setText("");
59         dialog3.showDialog();
60     }
61 });
62 }
63
64 public static String getBASE64(String s) {
65     if(s == null) {
66         return null;
67     }
68     return Base64.encodeToString(getBytes(), 0x0);
69 }
70
71 public static final String encode(String s) {
72     // :( Parsing error. Please contact me.
73 }
74
75 public boolean onCreateOptionsMenu(Menu menu) {
76     getMenuInflater().inflate(0x7f070000, menu);
77     return true;
78 }
79 }

```

3.代码分析

提取出主要的代码

```

str.reverse(); //字符串反向
Log.i("ClownQiang", localString1.append(new String(str)).toString());
String md5_string = encode(new String(str)); //md5加密
Log.i("ClownQiang", str);
String base64 = getBASE64(md5_string).trim(); //base64加密
Log.i("ClownQiang", md5_string);
if(base64.equalsIgnoreCase("NzU2ZDJmYzg0ZDA3YTM1NmM4ZjY4ZjcxZmU3NmUxODk=")) {
    dialog2.showDialog();
    return;
}

```

根据代码，我们只需要将经过md5和base64加密后的字符串 "NzU2ZDJmYzg0ZDA3YTM1NmM4ZjY4ZjcxZmU3NmUxODk=" 解密后反向即可。

base64解密：756d2fc84d07a356c8f68f71fe76e189

md5解密：}321nimda{galfij

反向输出：jflag{admin123}

4.get flag !

flag{admin123}