BUUCTF Reverse/简单注册器

原创

这就是强者的世界么 于 2021-07-17 15:32:46 发布 85 收藏 1

分类专栏： # BUUCTF Reverse

本文链接：https://blog.csdn.net/ookami6497/article/details/118857363

BUUCTF Reverse/简单注册器

> 下载得到一个apk文件,直接拿JEB打开查看伪代码

```
package com.example.flag;

import android.os.Bundle;
import android.support.v4.app.Fragment;
import android.support.v7.app.ActionBarActivity;
import android.view.LayoutInflater;
import android.view.Menu;
```

```
import android.view.Menu;
import android.view.MenuItem;
import android.view.View$OnClickListener;
import android.view.View;
import android.view.ViewGroup;

public class MainActivity extends ActionBarActivity {
    public class PlaceholderFragment extends Fragment {
        public PlaceholderFragment() {
            super();
            super();
        }

        public View onCreateView(LayoutInflater arg4, ViewGroup arg5, Bundle arg6) {
            // Method was not decompiled
        }
    }

    public MainActivity() {
        super();
    }

    protected void onCreate(Bundle arg7) {
        super.onCreate(arg7);
        this.setContentView(0x7F030017);
        if(arg7 == null) {
            this.getSupportFragmentManager().beginTransaction().add(0x7F05003C, new PlaceholderFragment()).commi
t();
        }

        this.findViewById(0x7F05003F).setOnClickListener(new View$OnClickListener(this.findViewById(0x7F05003D),
 this.findViewById(0x7F05003E)) {
            public void onClick(View arg13) {
                int v11 = 0x1F;
                int v9 = 2;
                int v2 = 1;
                String v6 = this.val$editview.getText().toString();
                if(v6.length() != 0x20 || v6.charAt(v11) != 97 || v6.charAt(1) != 98 || v6.charAt(0) + v6.charAt
(v9) - 0x30 != 56) {
                    v2 = 0;
                }

                if(v2 == 1) {
                    char[] v5 = "dd2940c04462b4dd7c450528835cca15".toCharArray();
                    v5[v9] = ((char)(v5[v9] + v5[3] - 50));
                    v5[4] = ((char)(v5[v9] + v5[5] - 0x30));
                    v5[30] = ((char)(v5[v11] + v5[9] - 0x30));
                    v5[14] = ((char)(v5[27] + v5[28] - 97));
                    int v4;
                    for(v4 = 0; v4 < 16; ++v4) {
                        char v0 = v5[0x1F - v4];
                        v5[0x1F - v4] = v5[v4];
                        v5[v4] = v0;
                    }

                    this.val$textview.setText("flag{" + String.valueOf(v5) + "}");
                }
                else {
                    this.val$textview.setText("输入注册码错误");
                }
```

```
            }
        });
    }

    public boolean onCreateOptionsMenu(Menu arg3) {
        this.getMenuInflater().inflate(0x7F0C0000, arg3);
        return 1;
    }

    public boolean onOptionsItemSelected(MenuItem arg3) {
    label_3:
        boolean v1 = arg3.getItemId() == 0x7F050040 ? true : super.onOptionsItemSelected(arg3);
        return v1;
        if(arg3.getItemId() == 0x7F050040) {
            goto label_3;
            v1 = true;
        }
        else {
            v1 = super.onOptionsItemSelected(arg3);
        }

        return v1;
    }
}
```

分析得知flag就存储在v5当中

```
    char[] v5 = "dd2940c04462b4dd7c450528835cca15".toCharArray();
                v5[v9] = ((char)(v5[v9] + v5[3] - 50));
                v5[4] = ((char)(v5[v9] + v5[5] - 0x30));
                v5[30] = ((char)(v5[v11] + v5[9] - 0x30));
                v5[14] = ((char)(v5[27] + v5[28] - 97));
                int v4;
                for(v4 = 0; v4 < 16; ++v4) {
                    char v0 = v5[0x1F - v4];
                    v5[0x1F - v4] = v5[v4];
                    v5[v4] = v0;
                }
```

根据代码写出脚本

```c
#include <stdlib.h>
#include <stdio.h>
#include <string.h>

int main()
{
   char v5[] = "dd2940c04462b4dd7c450528835cca15";
   int v11 = 0x1F;
   int v9 = 2;
   int v2 = 1;
    v5[v9] = v5[v9] + v5[3] - 50;
    v5[4] = v5[v9] + v5[5] - 0x30;
    v5[30] = v5[v11] + v5[9] - 0x30;
    v5[14] = v5[27] + v5[28] - 97;
   int v4;
   for(v4 = 0;  v4 < 16 ; ++v4)
   {
       char v0 = v5[0x1F - v4];
       v5[0x1F - v4] = v5[v4];
       v5[v4] = v0;
   }
    v5[32] = '\0';
    printf("flag{%s}\n",v5);
   return 0;

}
```

得到flag