

BUUCTF Reverse 简单注册器 WriteUp

原创

PlumpBoy 于 2021-09-11 16:14:30 发布 37 收藏

分类专栏: [BUUCTF 逆向题解](#) 文章标签: [系统安全](#) [安全](#)

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/weixin_45723661/article/details/120228023

版权



[BUUCTF 逆向题解 专栏收录该内容](#)

18 篇文章 1 订阅

订阅专栏

简单注册器-WP

一个apk文件, 直接用jdax-gui打开

```
103 public View onCreateView(LayoutInflater inflater, ViewGroup container, Bundle savedInstanceState) {
104     return inflater.inflate(R.layout.fragment_main, container, false);
}

/* Access modifiers changed, original: protected */
21 public void onCreate(Bundle savedInstanceState) {
22     super.onCreate(savedInstanceState);
23     setContentView((int) R.layout.activity_main);
24     if (savedInstanceState == null) {
25         getSupportFragmentManager().beginTransaction().add((int) R.id.container, new PlaceholderFragment()).commit();
26     }
27 }
28
31 final TextView textview = (TextView) findViewById(R.id.textView1);
32 final EditText editview = (EditText) findViewById(R.id.editText1);
33 ((Button) findViewById(R.id.button1)).setOnClickListener(new OnClickListener() {
34     public void onClick(View v) {
35         int flag = 1;
36         String xx = editview.getText().toString();
37         if (!(xx.length() == 32 && xx.charAt(31) == 'a' && xx.charAt(1) == 'b' && (xx.charAt(0) + xx.charAt(2)) - 48 == 56)) {
38             flag = 0;
39         }
40         if (flag == 1) {
41             char[] x = "dd2940c04462b4dd7c450528835cca15".toCharArray();
42             x[2] = (char) ((x[2] + x[3]) - 50);
43             x[4] = (char) ((x[2] + x[5]) - 48);
44             x[30] = (char) ((x[31] + x[9]) - 48);
45             x[14] = (char) ((x[27] + x[28]) - 97);
46             for (int i = 0; i < 16; i++) {
47                 char a = x[31 - i];
48                 x[31 - i] = x[i];
49                 x[i] = a;
50             }
51             textview.setText("flag{" + String.valueOf(x) + "}");
52             return;
53         }
54         textview.setText("输入注册码错误");
55     }
56 });
57
76 public boolean onCreateOptionsMenu(Menu menu) {
```

定位到核心加密部分, 将其复制出来, 写一个c的解密程序

```
#include <iostream>

using namespace std;

int main()
{
    char x[] = "dd2940c04462b4dd7c450528835cca15";
    x[2] = (char)((x[2] + x[3]) - 50);
    x[4] = (char)((x[2] + x[5]) - 48);
    x[30] = (char)((x[31] + x[9]) - 48);
    x[14] = (char)((x[27] + x[28]) - 97);
    for (int i = 0; i < 16; i++) {
        char a = x[31 - i];
        x[31 - i] = x[i];
        x[i] = a;
    }
    puts(x);
    return 0;
}
```

得到flag `flag{59acc538825054c7de4b26440c0999dd}`