




【BUUCTF】findit WriteUp

原创

古月浪子  于 2020-07-20 11:02:05 发布  745  收藏 1

分类专栏: [BUUCTF - RE](#) 文章标签: [CTF](#)

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/tqdyqt/article/details/107459057>

版权



[BUUCTF - RE 专栏收录该内容](#)

3 篇文章 0 订阅

订阅专栏

buuoj上的一道安卓逆向题

既然是apk，用JEB打开

```
Bytecode/Disassembly MainActivity/Source
public class MainActivity extends ActionBarActivity {
    @Override // android.support.v7.app.ActionBarActivity
    protected void onCreate(Bundle arg0) {
        super.onCreate(arg0);
        this setContentView(0x7F030018); // layout:activity_main
        ((Button)this.findViewById(0x7F05003D)).setOnClickListener(new View.OnClickListener() { // id:widget3
            @Override // android.view.View$OnClickListener
            public void onClick(View arg13) {
                char[] x = new char[17];
                char[] y = new char[38];
                int i;
                for(i = 0; i < 17; ++i) {
                    if(new char[]{'T', 'h', 'i', 's', 'I', 's', 'T', 'h', 'e', 'F', 'l', 'a', 'g', 'H', 'o', 'm', 'e'}[i] < 73 && new char[]{'T', 'h', 'i', 's', 'I', 's', 'T', 'h', 'e', 'F', 'l', 'a', 'g', 'H', 'o', 'm', 'e'}[i] + 18);
                }
                else if(new char[]{'T', 'h', 'i', 's', 'I', 's', 'T', 'h', 'e', 'F', 'l', 'a', 'g', 'H', 'o', 'm', 'e'}[i] >= 65 && new char[]{'T', 'h', 'i', 's', 'I', 's', 'T', 'h', 'e', 'F', 'l', 'a', 'g', 'H', 'o', 'm', 'e'}[i] - 8);
                }
                else {
                    x[i] = new char[]{'T', 'h', 'i', 's', 'I', 's', 'T', 'h', 'e', 'F', 'l', 'a', 'g', 'H', 'o', 'm', 'e'}[i];
                }
            }
        });

        if(String.valueOf(x).equals(((EditText)this.findViewById(0x7F05003E)).getText().toString())) { // id:widget2
            int v0_1;
            for(v0_1 = 0; v0_1 < 38; ++v0_1) {
                if(new char[]{'p', 'v', 'k', 'q', '{', 'm', '1', '6', '4', '6', '7', '5', '2', '6', '2', '0', '3', '3', 'l', '4', 'm', '4', '9'}[v0_1] = (char)(new char[]{'p', 'v', 'k', 'q', '{', 'm', '1', '6', '4', '6', '7', '5', '2', '6', '2', '0', '3', '3', 'l', '4', 'm', '4', '9'}[v0_1] > 90 && y[v0_1] < 97 || y[v0_1] >= 0x7A) {
                    y[v0_1] = (char)(y[v0_1] - 26);
                }
            }
        } else {
            y[v0_1] = new char[]{'p', 'v', 'k', 'q', '{', 'm', '1', '6', '4', '6', '7', '5', '2', '6', '2', '0', '3', '3', 'l', '4', 'm', '4', '9'};
        }
    }
}
System.out.println(y);
}
```

光看代码不是很明白程序要干什么，不过这碍事

可以看到有一行if判断，我们不需要管前面到底判断的啥，直接把后面的代码复制到IDEA里跑一下就出答案了

```
public static void main(String[] args) {
    char[] y = new char[38];
    int v0_1;
    for (v0_1 = 0; v0_1 < 38; ++v0_1) {
        if (new char[]{'p', 'v', 'k', 'q', '{', 'm', '1', '6', '4', '6', '7', '5', '2', '6', '2', '0', '3', '3', 'l', '4', 'm', '4', '9'}[v0_1] = (char) (new char[]{'p', 'v', 'k', 'q', '{', 'm', '1', '6', '4', '6', '7', '5', '2', '6', '2', '0', '3', '3', 'l', '4', 'm', '4', '9'}[v0_1] > 90 && y[v0_1] < 97 || y[v0_1] >= 0x7A) {
            y[v0_1] = (char) (y[v0_1] - 26);
        }
    } else {
        y[v0_1] = new char[]{'p', 'v', 'k', 'q', '{', 'm', '1', '6', '4', '6', '7', '5', '2', '6', '2', '0', '3', '3', 'l', '4', 'm', '4', '9'};
    }
}
System.out.println(y);
}
```

```
"C:\Program Files\Java\jdk1.8.0_121\bin\java.exe" ...
```

```
flag{c164675262033b4c49bdf7f9cda28a75}
```

Process finished with exit code 0

不得不说JEB的反编译真的很好用！