

CTF挑战赛-合天网安实验室-Reverse逆向100writeup

原创

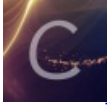
iqiqiya 于 2018-10-06 14:46:34 发布 842 收藏 1

分类专栏: [我的逆向之路](#) [我的CTF之路](#) -----[合天CTF](#) [我的CTF进阶之路](#) 文章标签: [CTF挑战赛-合天网安实验室-Reverse逆向100wri](#) [Reverse逆向100writeup](#) [逆向100writeup](#)

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/xiangshangbashaonian/article/details/82950944>

版权



[我的逆向之路](#) 同时被 3 个专栏收录

108 篇文章 10 订阅

订阅专栏



[我的CTF之路](#)

92 篇文章 5 订阅

订阅专栏



[-----合天CTF](#)

3 篇文章 0 订阅

订阅专栏

题目地址: <http://www.hetianlab.com/CTFace.html>

0x01:逆向100



下载后IDA载入发现就是一个apk

然后关掉IDA 将它载入JEB 双击MainActivity 然后tab键反汇编成java代码

可以看到就是将我们的输入与EYG3QMCS比较 成功就打印flag

```
protected void onCreate(Bundle savedInstanceState) {
    super.onCreate(savedInstanceState);
    this setContentView(2130903041);
    this.findViewById(2131230723).setOnClickListener(new View.OnClickListener() {
        public void onClick(View v) {
            if(MainActivity.this.findViewById(2131230722).getText().toString().compareTo("EYG3QMCS")
                == 0) {
                MainActivity.this.startActivity(new Intent(MainActivity.this, FlagActivity.class));
            }
        }
    });
}
```

<https://blog.csdn.net/xiangshangbashaonian>

那我们只要安装它 输入EYG3QMCS即可拿到flag



还有一种方法就是可以直接看到FlagActivity中这个数组 python就可以解得

The image shows a screenshot of an IDE (likely IntelliJ IDEA) displaying decompiled Java code for a class named `FlagActivity`. The code is as follows:

```
public class FlagActivity extends Activity {
    public FlagActivity() {
        super();
    }

    protected void onCreate(Bundle savedInstanceState) {
        int v5 = 22;
        super.onCreate(savedInstanceState);
        this setContentView(2130903040);
        String v1 = "";
        int[] v0 = new int[]{102, 108, 97, 103, 123, 119, 52, 110, 110, 52, 95, 106, 52, 114, 95, 109,
            121, 95, 100, 51, 120, 125};
        int v3 = 0;
        label_7:
        if(v3 < v5) {
            v1 = v1.concat(String.valueOf(((char)v0[v3]]));
            ++v3;
            goto label_7;
        }

        this.findViewById(2131230721).setText(((CharSequence)v1));
    }

    public boolean onCreateOptionsMenu(Menu menu) {
        this.getMenuInflater().inflate(2131165184, menu);
        return 1;
    }
}
```

The array `v0` is highlighted with a red box. Below the IDE, a Python 2.7.15 Shell window is open, showing the following code:

```
a = [102, 108, 97, 103, 123, 119, 52, 110, 110, 52, 95, 106, 52, 114, 95, 109,
    121, 95, 100, 51, 120, 125]
flag = ''
for i in a:
    flag += chr(i)
print flag
```

The Python code is also highlighted with a red box. The output of the Python script is shown in the shell window:

```
f
fl
fla
flag
flag{
flag{w
flag{w4
flag{w4n
flag{w4nn
flag{w4nn4
flag{w4nn4_j
flag{w4nn4_j4
flag{w4nn4_j4r
flag{w4nn4_j4r_
flag{w4nn4_j4r_n
flag{w4nn4_j4r_my
flag{w4nn4_j4r_my_
flag{w4nn4_j4r_my_d
flag{w4nn4_j4r_my_d3
flag{w4nn4_j4r_my_d3x
flag{w4nn4_j4r_my_d3x}/x
```

The final line of the output is highlighted with a red box.