

【猿人学】APP逆向学习 demo-01

原创

老实人小林 于 2022-02-22 22:05:42 发布 107 收藏

分类专栏: [APP逆向](#) 文章标签: [学习](#)

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/u014685598/article/details/123057402>

版权



[APP逆向](#) 专栏收录该内容

2 篇文章 0 订阅

订阅专栏

1. 抓包:

名称	值
page	2
sign	8382920ef764e2bad4dc20c1b679ef5
t	1645451825336

CSDN @老实人小林

2. 分析

抓包看来就是一个sign加上一个翻页参数。这个sign看着像32位md5, 遗憾的是自吐MD5并没有什么结果,

3. 代码分析

跳转到@Page(name = "题目一") 很明显的参数提示, 虽然没有sign但

```
1 public /* synthetic */ void o00000(O0o0000 ooo0000) {
2     this.f60390oo00oo = 1;
3     StringBuilder sb = new StringBuilder();
4     sb.append("page=");
5     sb.append(this.f60390oo00oo);
6     long currentTimeMillis = System.currentTimeMillis();
7     sb.append(currentTimeMillis);
8     String Ooo02 = new Ooo00o.Ooo0000.Ooo000o.Ooo0o0.Ooo000o().Ooo0(sb.toString().getBytes(StandardCharsets.UTF_8));
9     Ooo00o.Ooo000.Ooo0000.Ooo0000.Ooo0000 ooo0000 = this.f60370oo0;
10    ooo0000.Ooo000o(((Ooo00o.Ooo0000.Ooo000o.Ooo00o0.Ooo000o.Ooo000o.Ooo0000) ooo0000.Ooo0000(Ooo00o.Ooo0000.Ooo000o.Ooo00o0.Ooo000o.O
11    });
12
13    /* access modifiers changed from: private */
14    /* renamed from: oo000o */
15    public /* synthetic */ void o00o00o(Ooo0000 ooo0000) {
16        this.f60390oo00oo++;
17        StringBuilder sb = new StringBuilder();
18        sb.append("page=");
19        sb.append(this.f60390oo00oo);
20        long currentTimeMillis = System.currentTimeMillis();
21        sb.append(currentTimeMillis);
22        String Ooo02 = new Ooo00o.Ooo0000.Ooo000o.Ooo0o0.Ooo000o().Ooo0(sb.toString().getBytes(StandardCharsets.UTF_8));
23        Ooo00o.Ooo000.Ooo0000.Ooo0000.Ooo0000 ooo0000 = this.f60370oo0;
24        ooo0000.Ooo000o(((Ooo00o.Ooo0000.Ooo000o.Ooo00o0.Ooo000o.Ooo000o.Ooo0000) ooo0000.Ooo0000(Ooo00o.Ooo0000.Ooo000o.Ooo00o0.Ooo000o.O
25    });
26    }
```

第六行看到了.toString().getBytes() 大概率没跑了 Hook 住OooO 看看组包规则然后尝试重现。

但是吧Hook OooO的时候会

```
Error: java.lang.ClassNotFoundException:
Didn't find class "Ooo00o.Ooo0000.Ooo000o.Ooo0o0.Ooo000o"
```

...