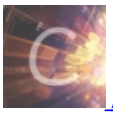
【猿人学】APP逆向学习 demo-01

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

本文链接：https://blog.csdn.net/u014685598/article/details/123057402



1. 抓包：

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

```
    /* renamed from: OOOOOO */
    public /* synthetic */ void o00ooo(OooOOOO oooOOOO) {
1       this.f60390oo00oo = 1;
2       StringBuilder sb = new StringBuilder();
3       sb.append("page=");
3       sb.append(this.f60390oo00oo);
4       long currentTimeMillis = System.currentTimeMillis();
5       sb.append(currentTimeMillis);
6       String OooO2 = new Ooo00o.OooO00O.Ooo000o.Ooo0o0.Ooo000o().OooO(sb.toString().getBytes(StandardCharsets.UTF_8));
7       Ooo00o.OooO00.OooO000.OooO00O.OooO000 oooO000 = this.f60370ooO;
7       oooO000.OooO00o(((OooO0o.OooO00O.Ooo000o.Ooo0o0.Ooo000o.Ooo000o.OooO000) oooO000.OooOOOO(Ooo00o.OooO00O.Ooo000o.Ooo0o0.Ooo000o.O
    }

    /* access modifiers changed from: private */
    /* renamed from: oo000o */
    public /* synthetic */ void o00o00o(OooOOOO oooOOOO) {
        this.f60390oo00oo++;
2       StringBuilder sb = new StringBuilder();
3       sb.append("page=");
3       sb.append(this.f60390oo00oo);
4       long currentTimeMillis = System.currentTimeMillis();
5       sb.append(currentTimeMillis);
6       String OooO2 = new Ooo00o.OooO00O.Ooo000o.Ooo0o0.Ooo000o().OooO(sb.toString().getBytes(StandardCharsets.UTF_8));
7       Ooo00o.OooO00.OooO000.OooO00O.OooO000 oooO000 = this.f60370ooO;
7       oooO000.OooO00o(((OooO0o.OooO00O.Ooo000o.Ooo0o0.Ooo000o.Ooo000o.OooO000) oooO000.OooOOOO(Ooo00o.OooO00O.Ooo000o.Ooo0o0.Ooo000o.O
    }
```


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.OooO00O.Ooo000o.Ooo0o0.Ooo000o"
```

…