## 1、EDUSRC-小程序抓包未授权逻辑安全

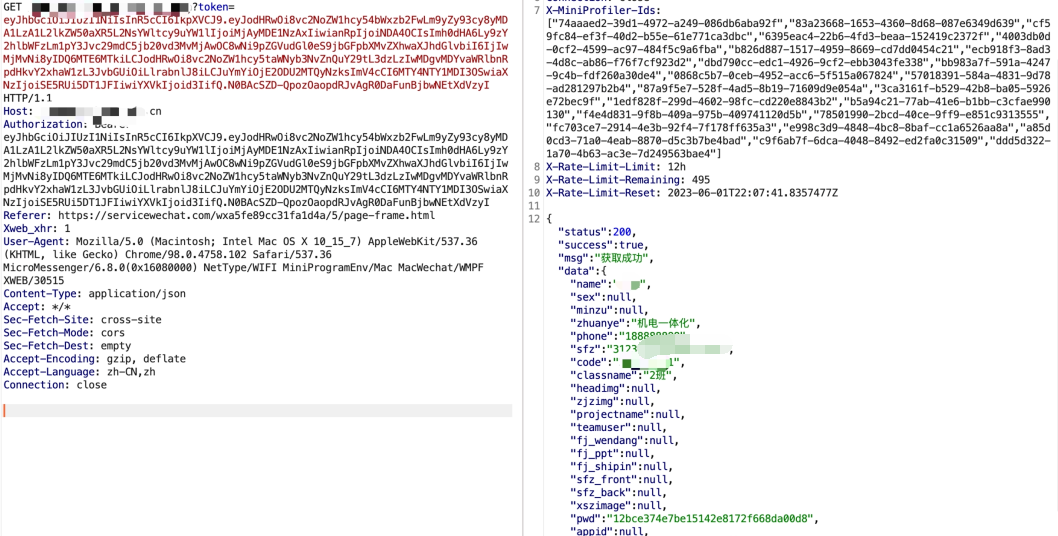
1、先搜索到目标资产小程序，注册并登录







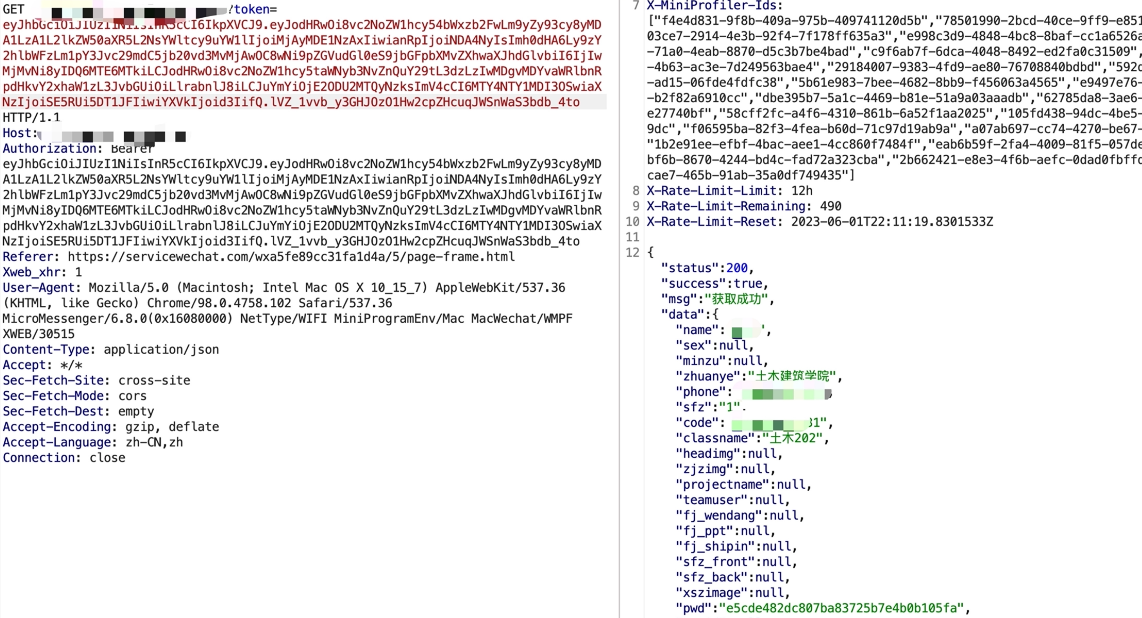
2、通过数据包中找到JWT特征，使用JWT安全测试





3、更改参数jti，组合JWT发包,

成功获取到其他学生的相关信息

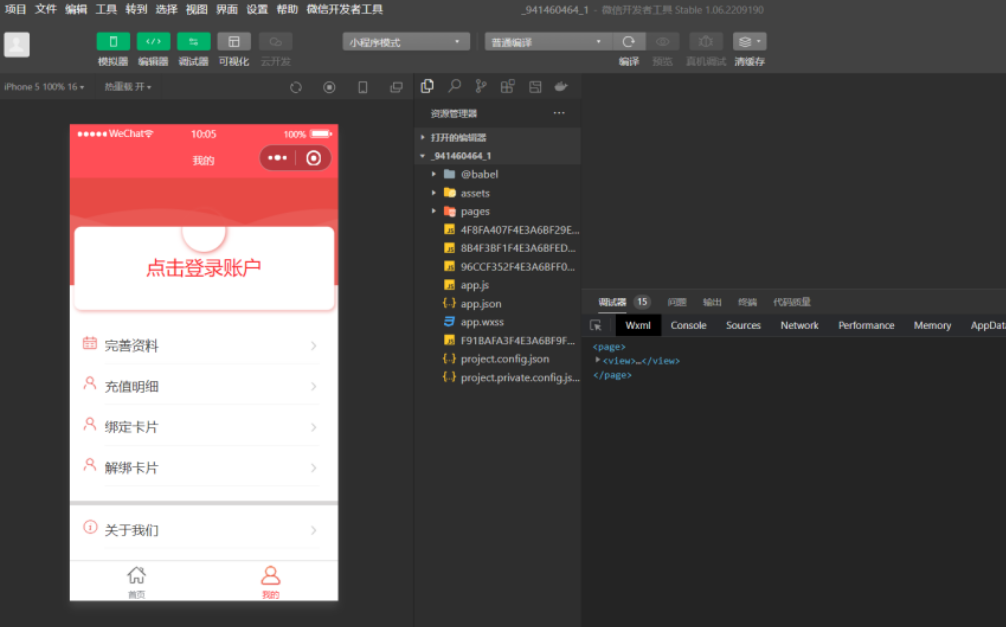


## 2、EDUSRC-小程序反编译接口信息泄漏

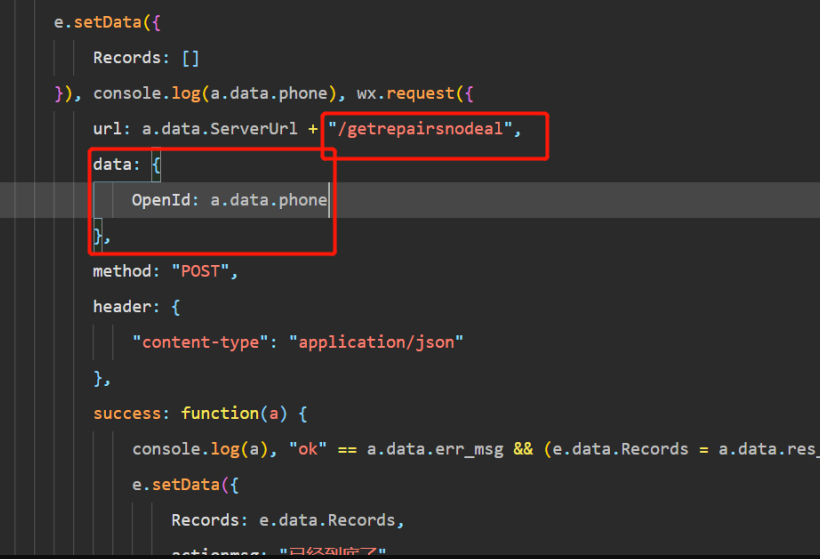
1、搜索目标资产小程序

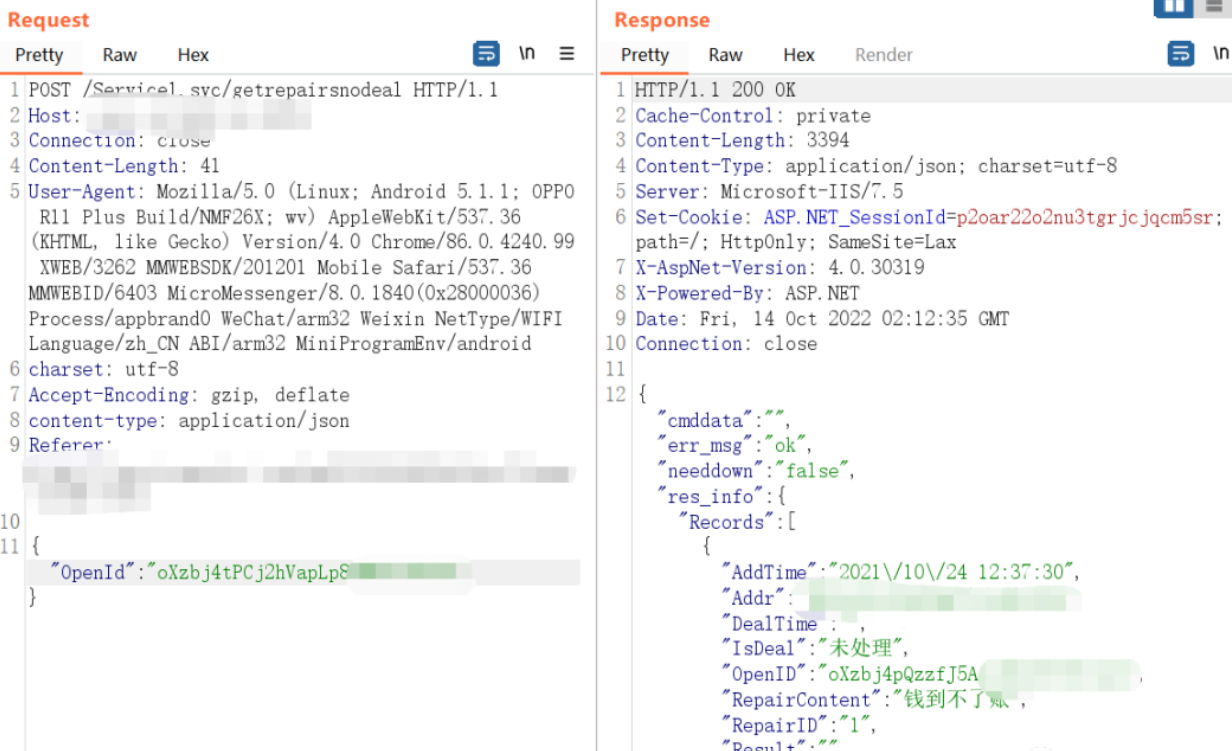


2、进行项目反编译导入开发者工具进行分析调试

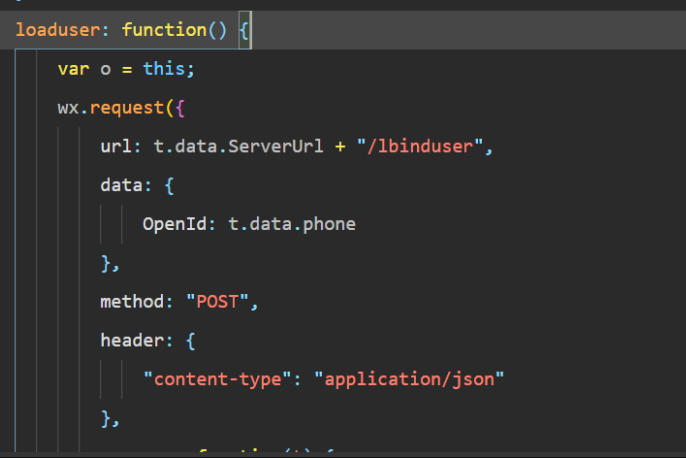


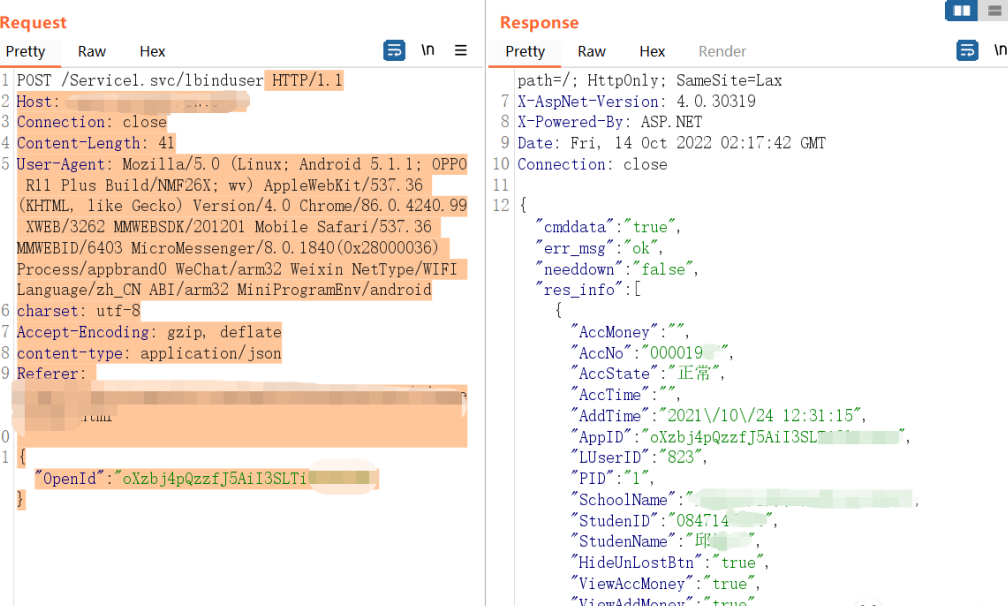
3、找到一处提交信息用户报修，可获取大量用户openid





4、使用获取到的openid在另一接口处可用户获取用户详细信息



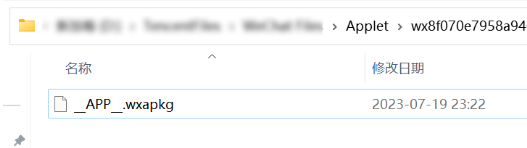


5、利用获取到的studentID又可对水卡进行绑定，绑定后水卡进行充值、挂失等操作。



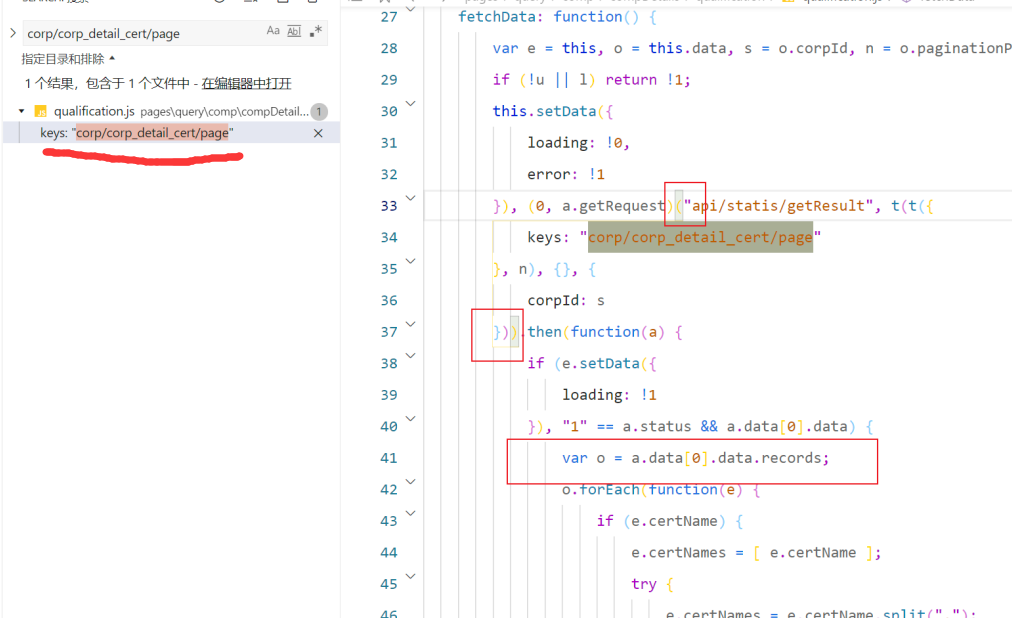
## 3、抓包逆向-小程序反编译加解密算法

1、目标进行反编译

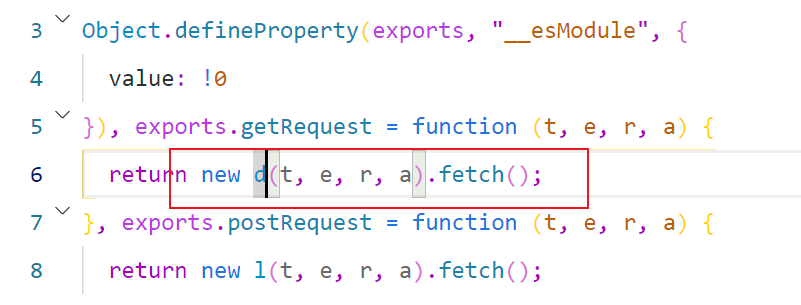




1. 通过抓包对比搜索关键字找到疑似加解密代码块



3、解密的过程应该就是在a 方法里了，点进去看一下



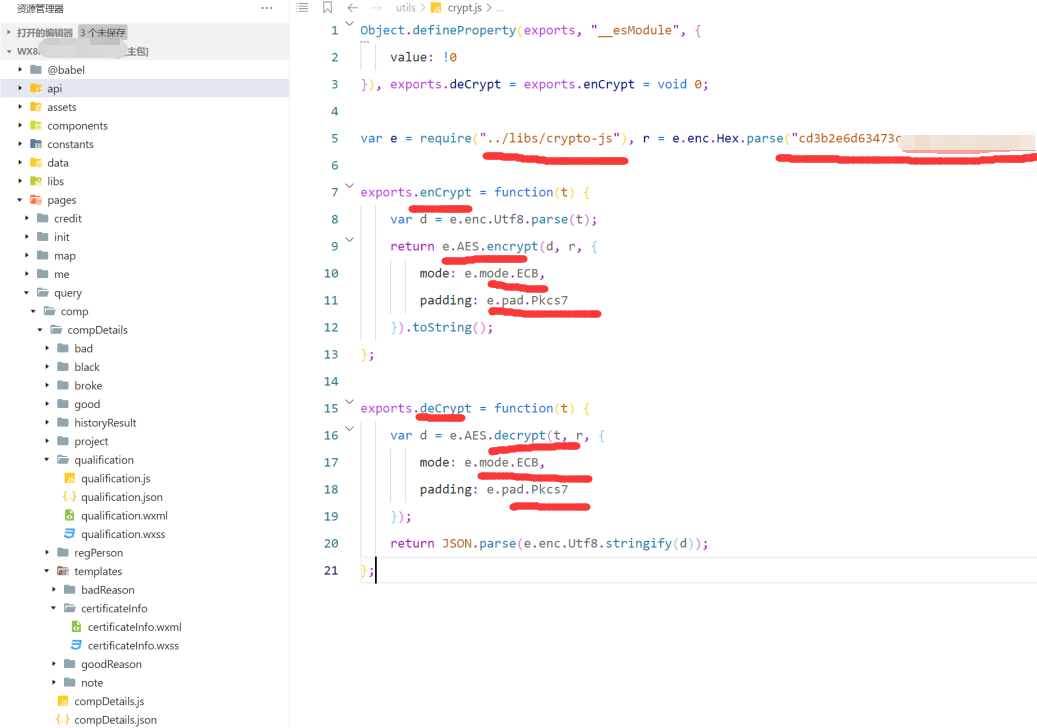
调用的是d对象的fetch方法，继续跟进去



最后调用的是request方法，大致看一下



4、找到加密配置代码，进行加密解密测试



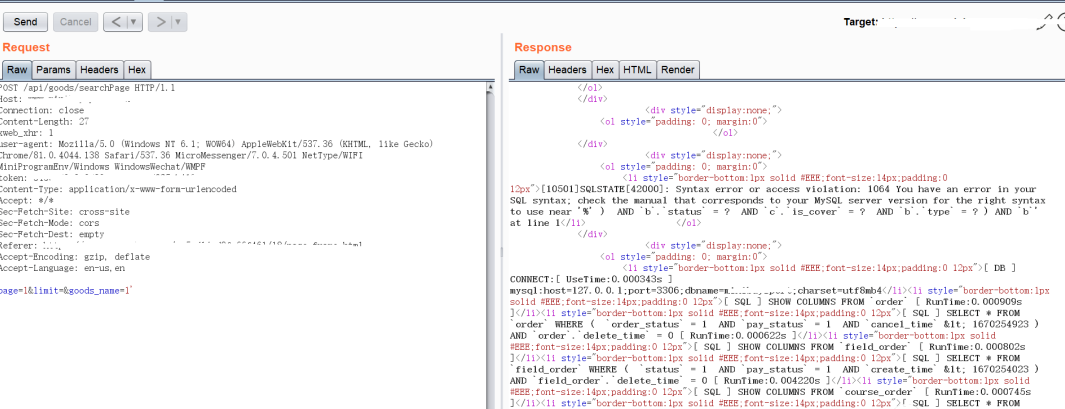
看起来是一个aes解密，测试一下，没啥问题



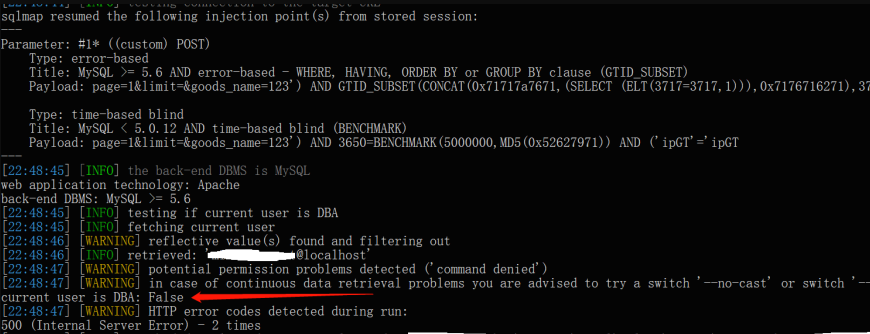
## 4、抓包测试-小程序抓包测试参数漏洞

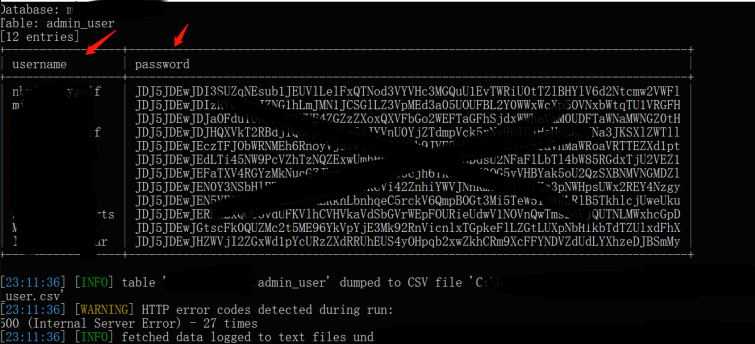


1、操作小程序抓包测试相关参数安全

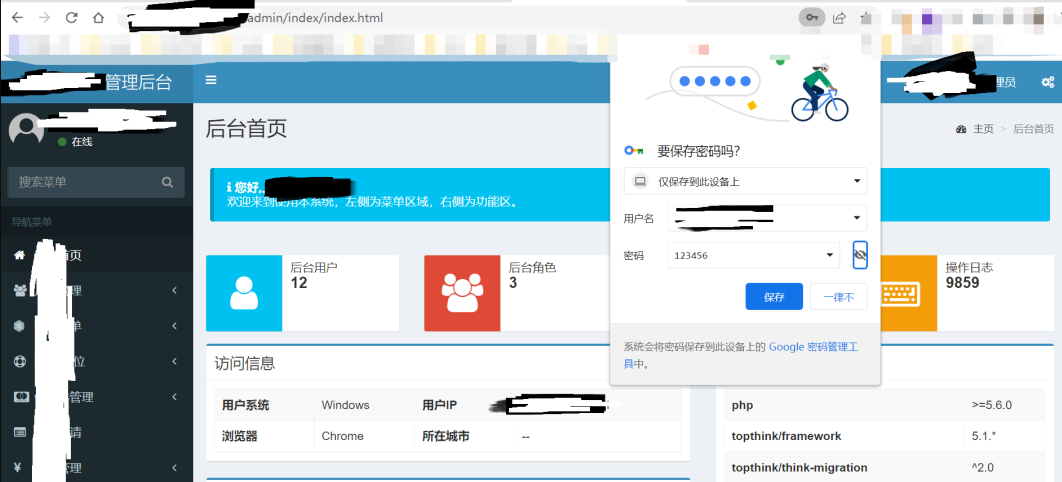


2、利用数据包进行SQL注入获取帐号密码



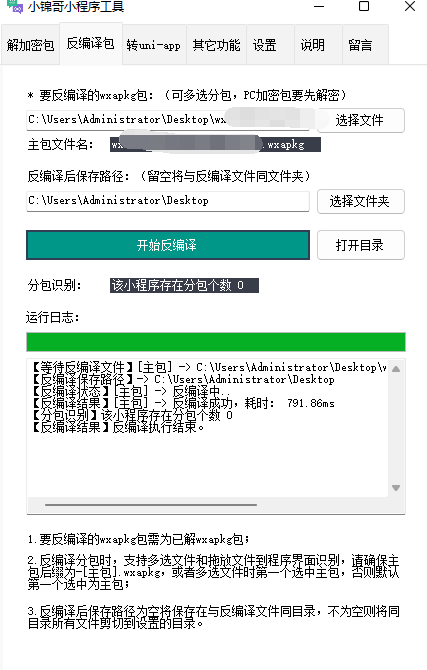


3、得到密码后通过反编译获取解密算法登录后台

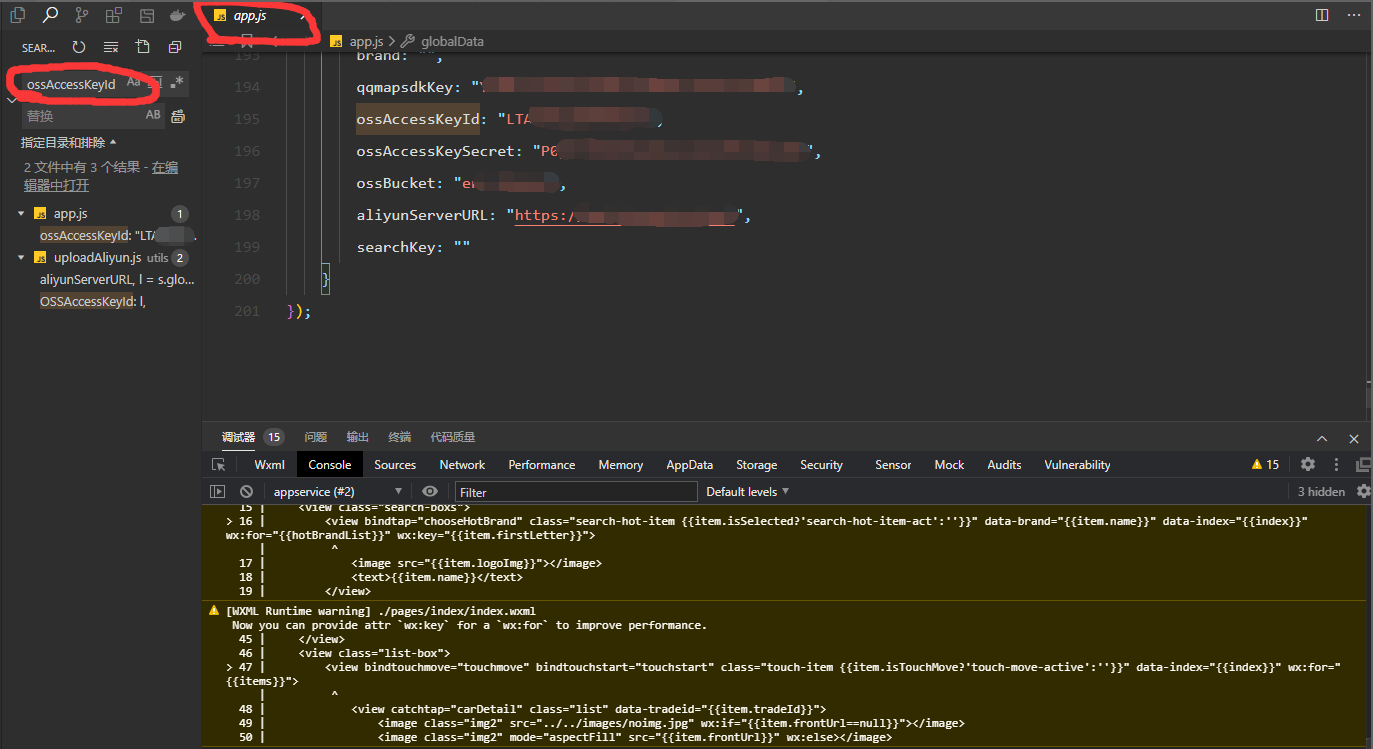


## 5、配置泄漏-小程序反编译获取云OSS

1、直接反编译



2、导入开发者工具，全局搜索配置关键字



3、利用OSS连接客户端连接

