01-开班第一课

目录

**[一、](#_Toc138683320)****[作业内容](#_Toc138683320)** [3](#_Toc138683320)

[1. xxxx 3](#_Toc138683321)

[2. xxxxx 3](#_Toc138683322)

[3. …… 3](#_Toc138683323)

**[二、](#_Toc138683324)****[操作步骤](#_Toc138683324)** [4](#_Toc138683324)

[1. xxxxx 4](#_Toc138683325)

[2. xxxxx 4](#_Toc138683326)

[3. …… 4](#_Toc138683327)

**[三、](#_Toc138683328)****[作业总结](#_Toc138683328)** [5](#_Toc138683328)

[1. xxxxx 5](#_Toc138683329)

[2. xxxxx 5](#_Toc138683330)

[3. …… 5](#_Toc138683331)

1. **作业内容**

### xxxxx

### xxxxx

### ……

1. **操作步骤**

打开登录界面

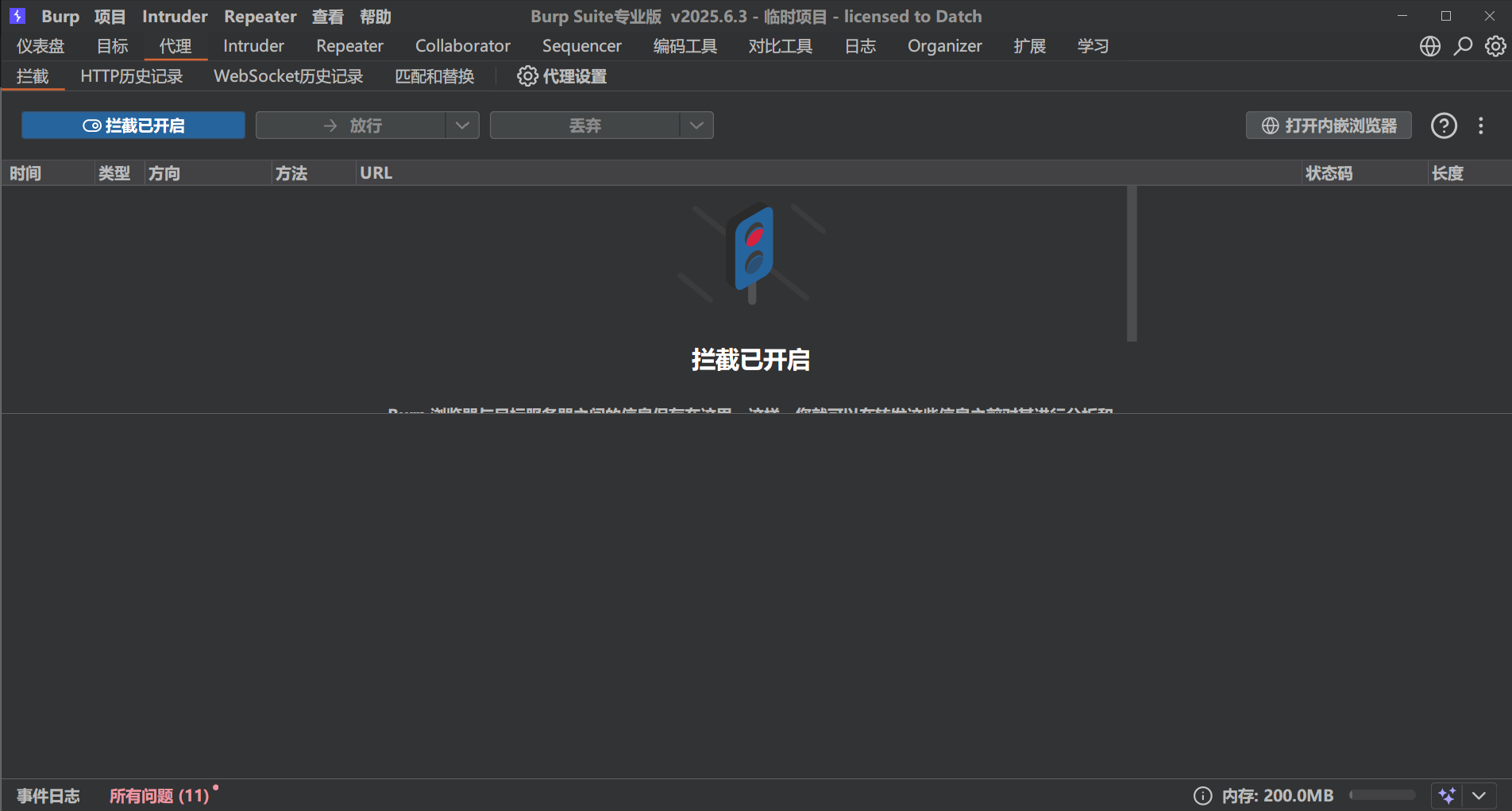


创建账号220221090722

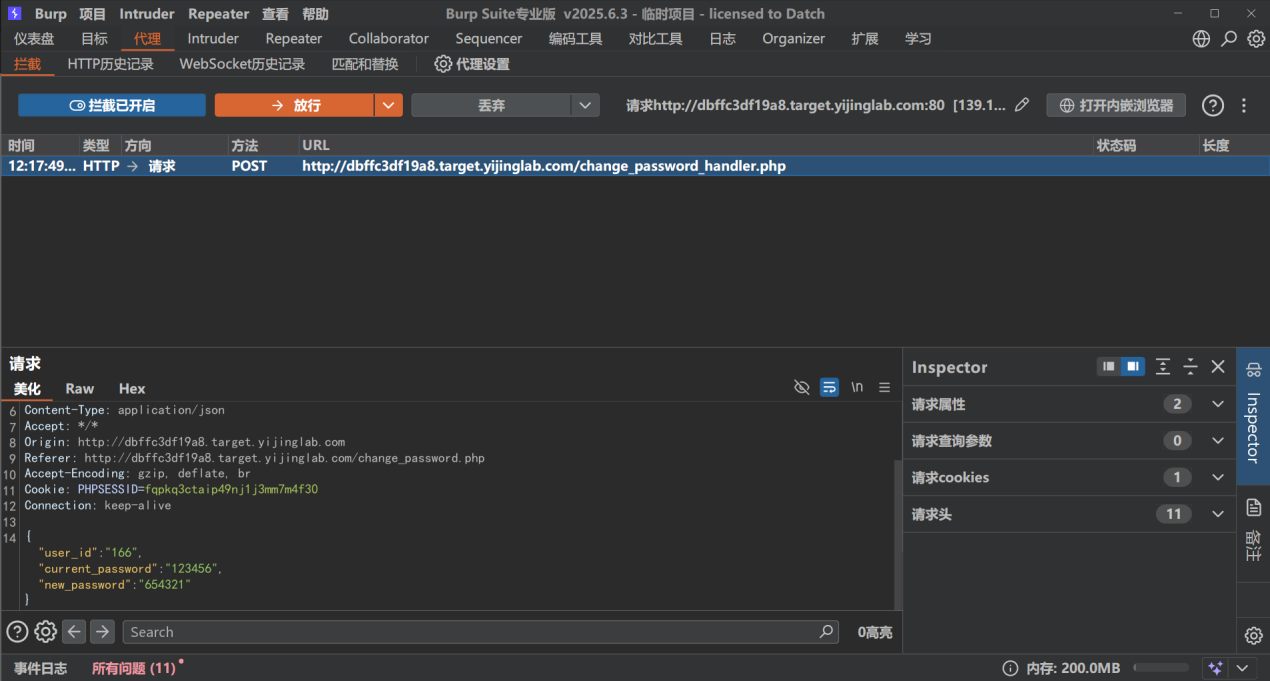
密码：123456



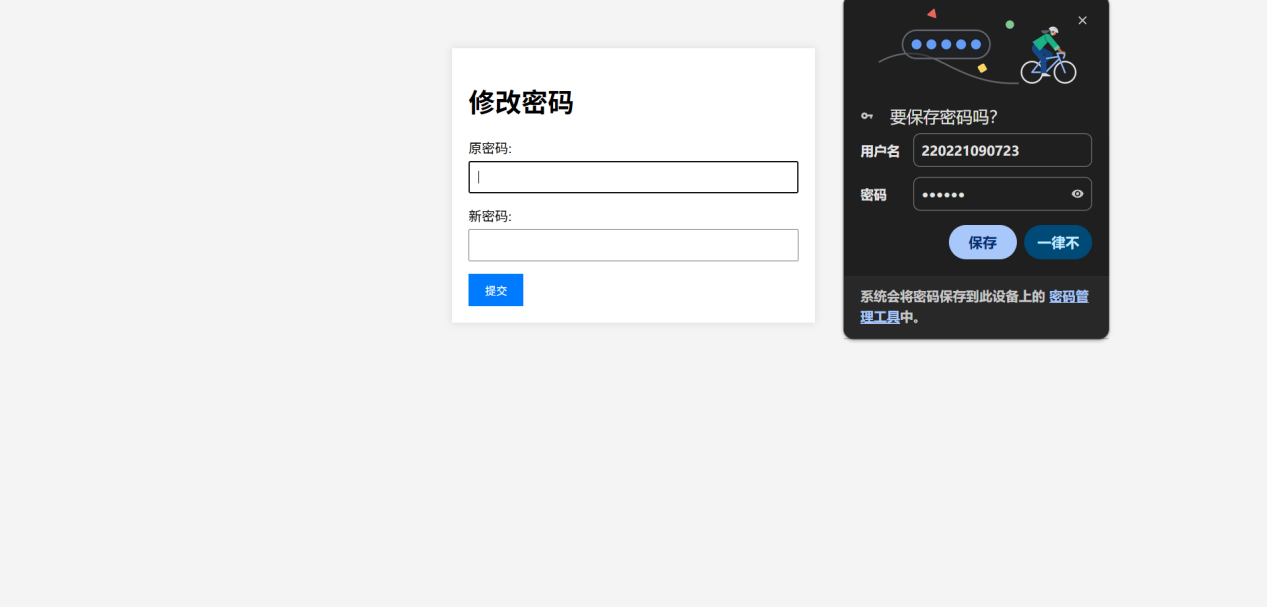
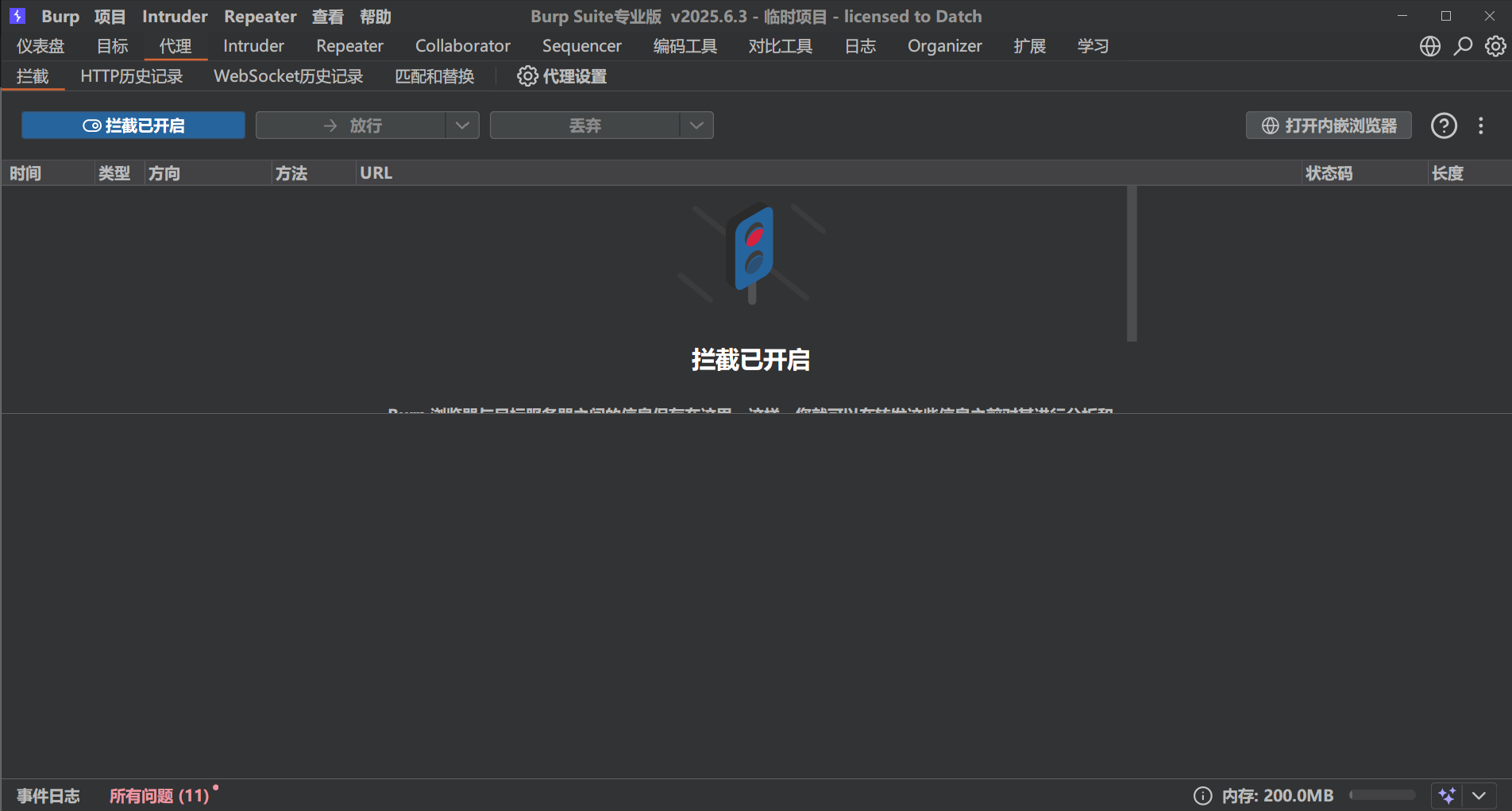
打开拦截



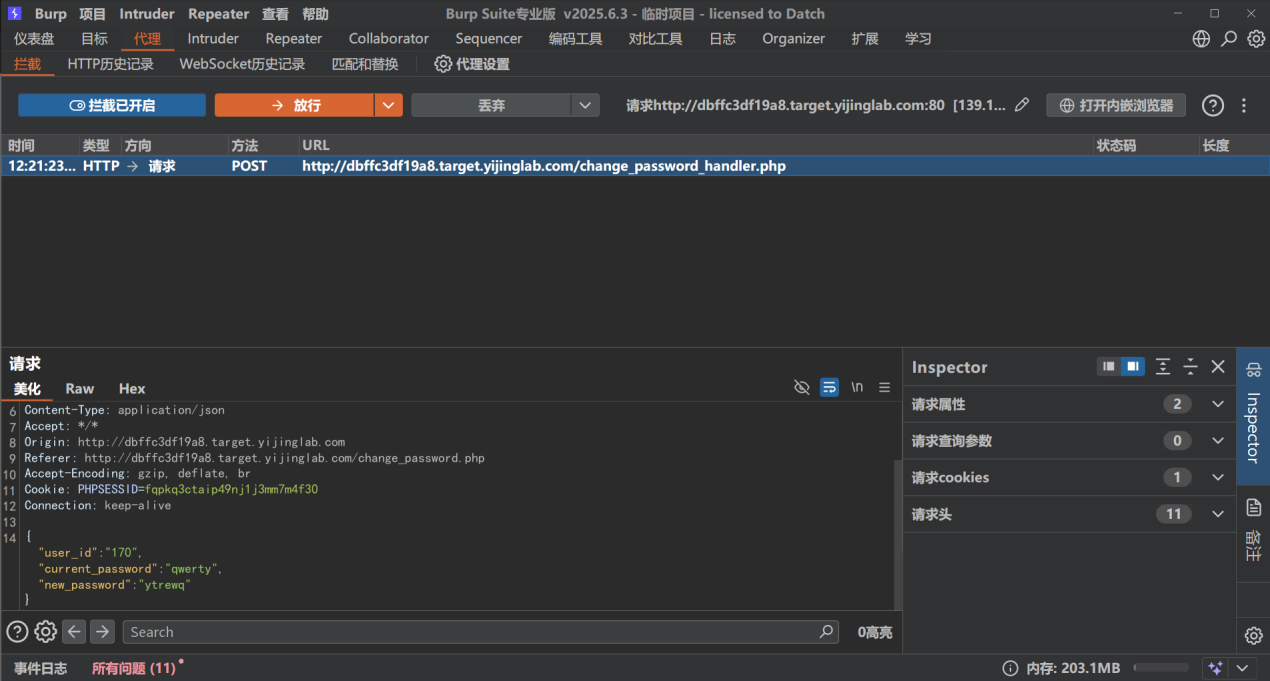
点击修改密码，点击输入原密码，以及新密码，使用burp抓包，发现存在数据包，此处有个userid=166的内容，判断为用户标识



点击创建新账号220221090723密码qwerty和上述一样的操作



点击修改密码，点击输入原密码，以及新密码，使用burp抓包，发现存在数据包，此处有个userid=170的内容，判断为用户标识  
此时修改userid:3 改成userid：1 再点击forward放包



退出了登录，进行使用第一个账号220221090722密码ytrewq进行登录，成功登录可以修改所有用户密码



1. **作业总结**

1.本次实验充分展示了在用户身份认证机制设计中，未对关键标识字段进行服务端校验所带来的严重安全隐患，即越权操作漏洞。

2.借助 Burp Suite 抓包工具，清晰观察并成功操纵 userid 参数，实现在未授权情况下对他人账户的控制，反映出该系统在用户标识绑定与验证机制方面存在严重缺陷。

3.实验表明：任何涉及敏感操作（如修改密码、删除用户等）的请求，必须在后端进行严密的身份校验与权限控制，仅依赖前端传参或 cookie/session 信息极易被绕过。