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)

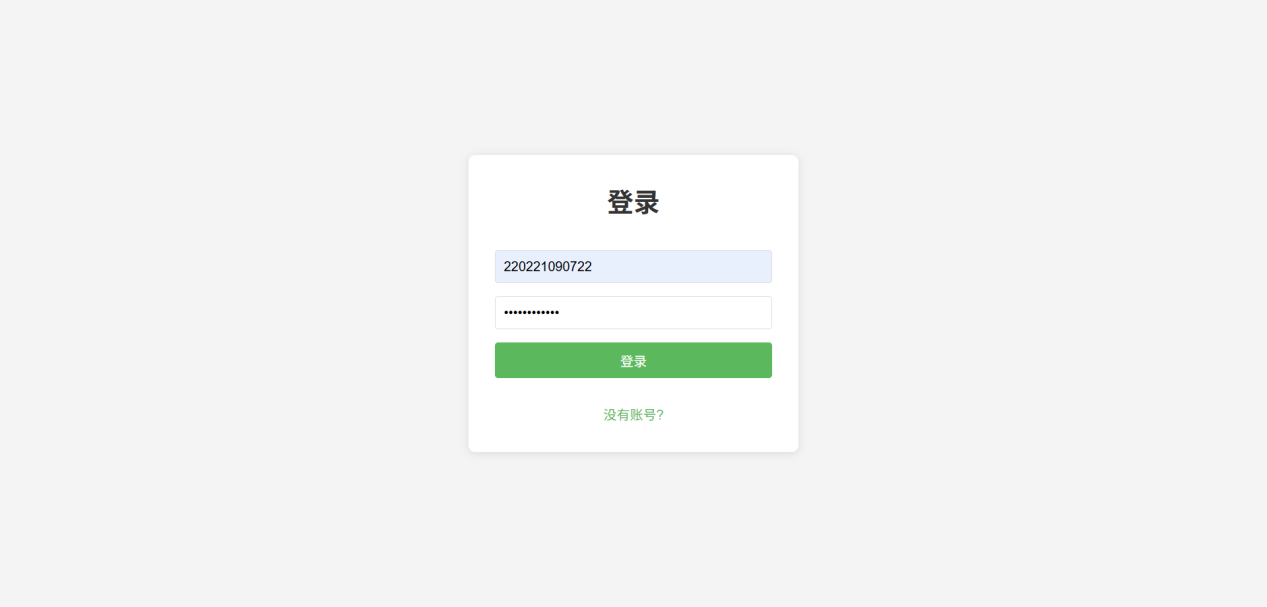
1. **作业内容**

完成越权漏洞靶场(两个任选其一即可)

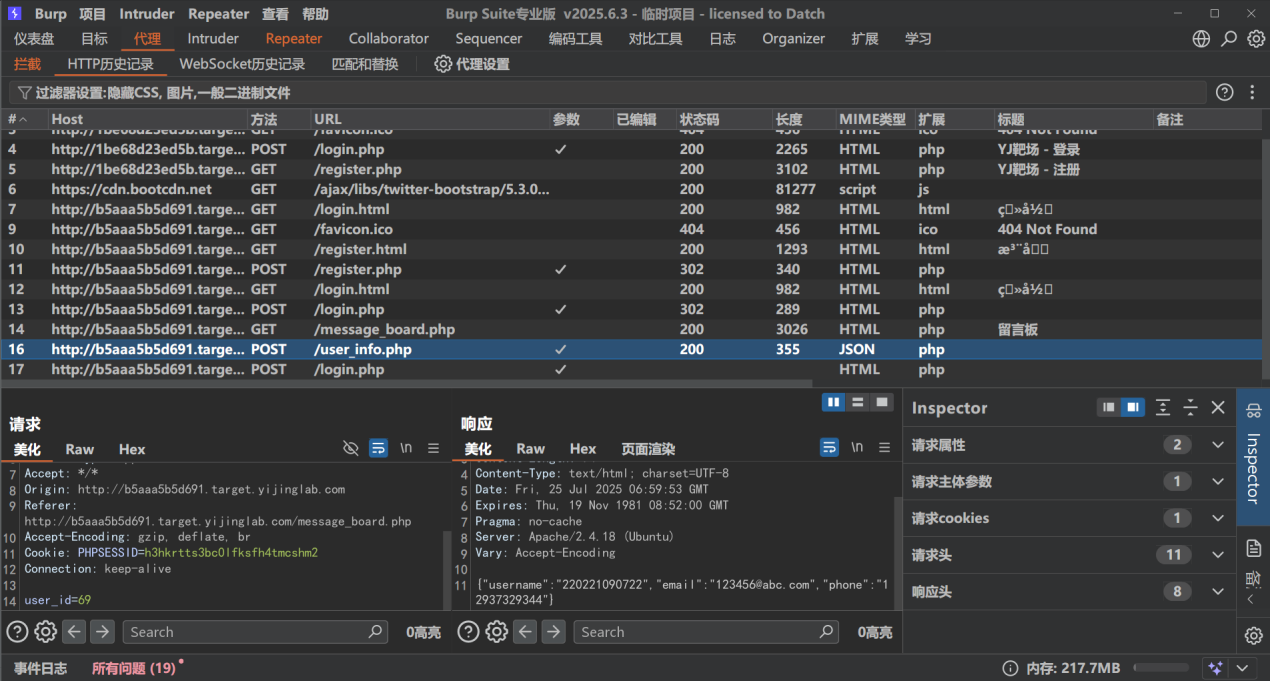
任务要求:安装完成截图写进word文档中即可

1. **操作步骤**

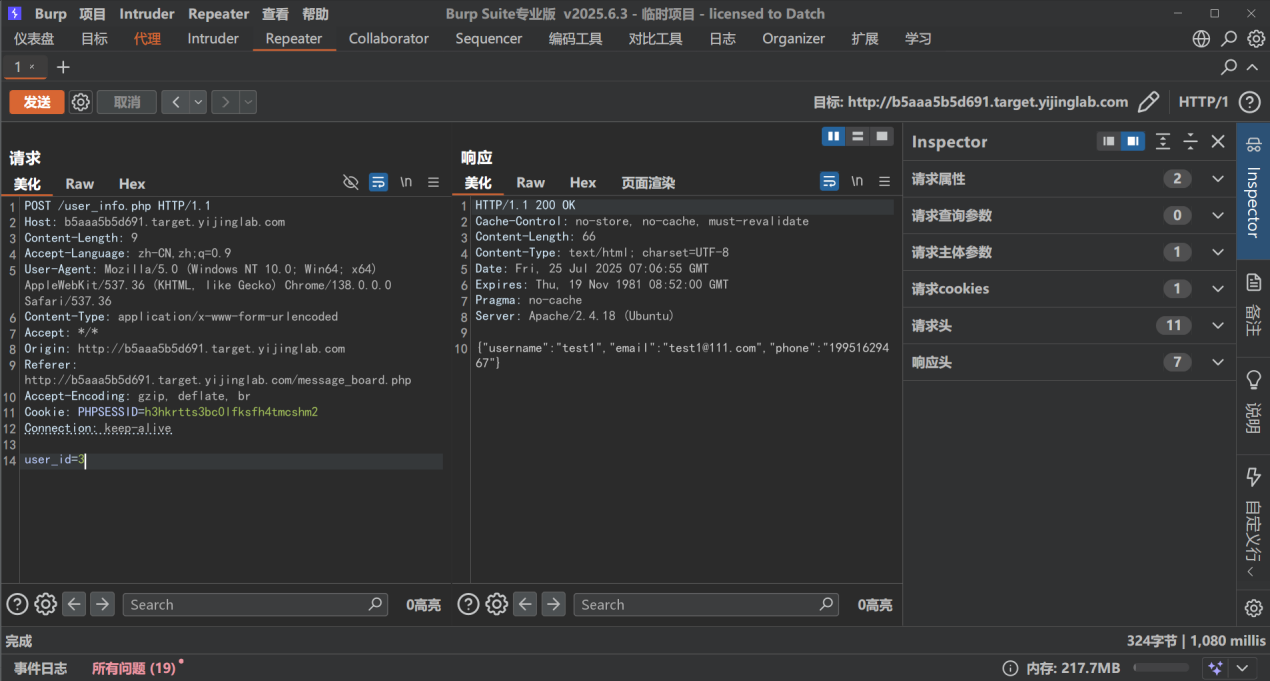
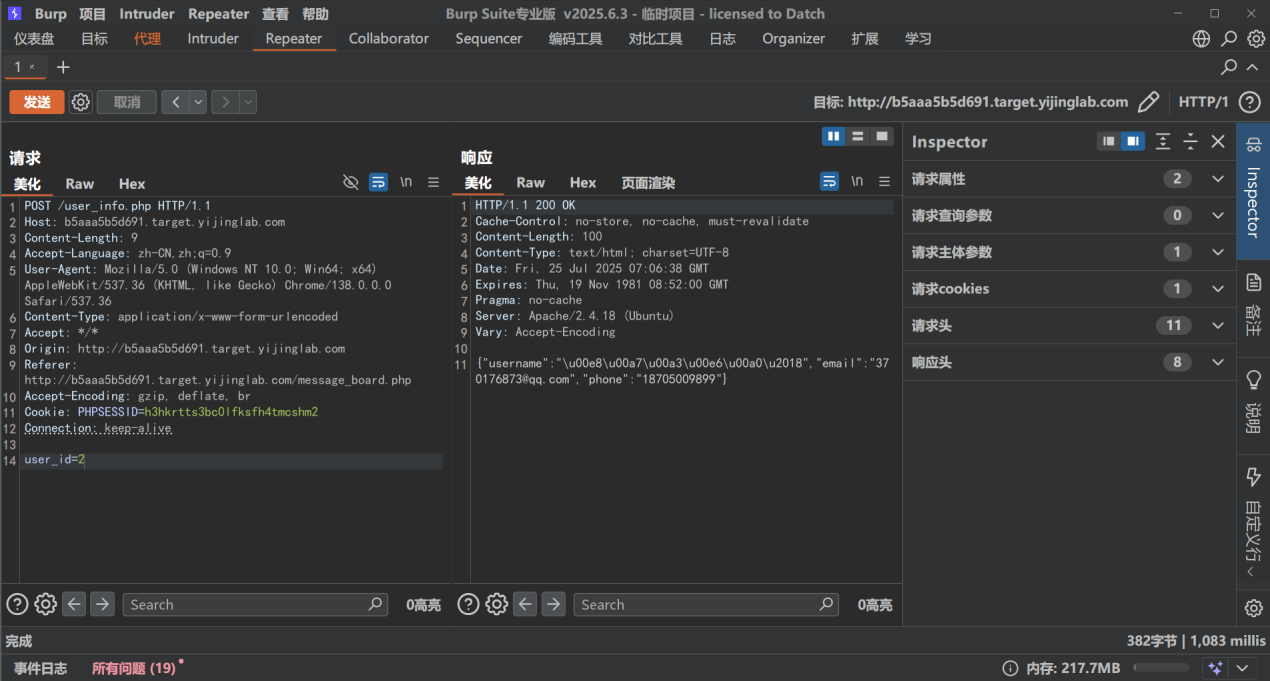
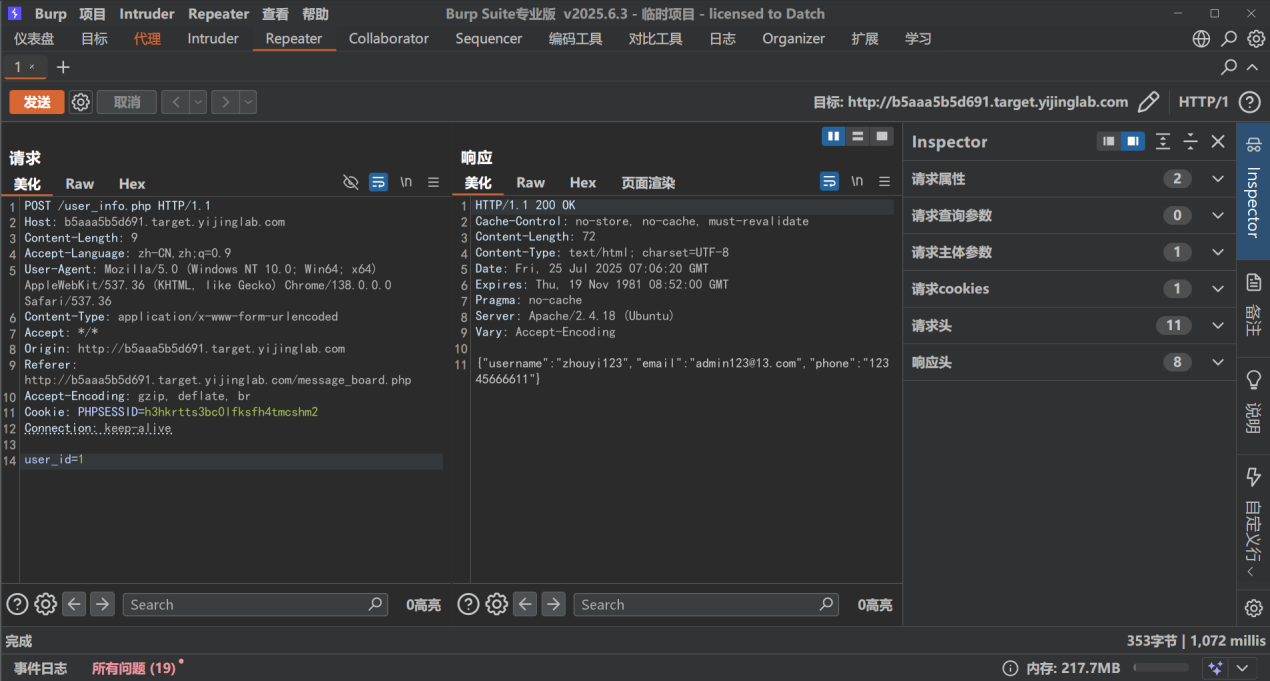
第一步注册账号进行登录



存在数据包加载，user\_id=1代表yiye用户身份信息，此时再注册用户yiye123登录发现加载数据包user\_id=2为Yiye123用户信息。



发送至重发器，发现可以通过userid查看其他用户账号信息



1. **作业总结**

1.本次作业掌握了 Web 应用中常见的水平越权漏洞成因和利用方式，尤其是 ID 参数未加访问控制时造成的数据泄露问题。

2.实操过程中，通过抓包工具（如 Burp Suite）成功模拟了攻击路径重现，锻炼了数据包分析、参数识别与请求重放能力。

3.越权漏洞在实际系统中危害较大，建议后台开发必须对敏感参数进行权限校验，避免仅靠前端逻辑或用户 session 控制。