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)

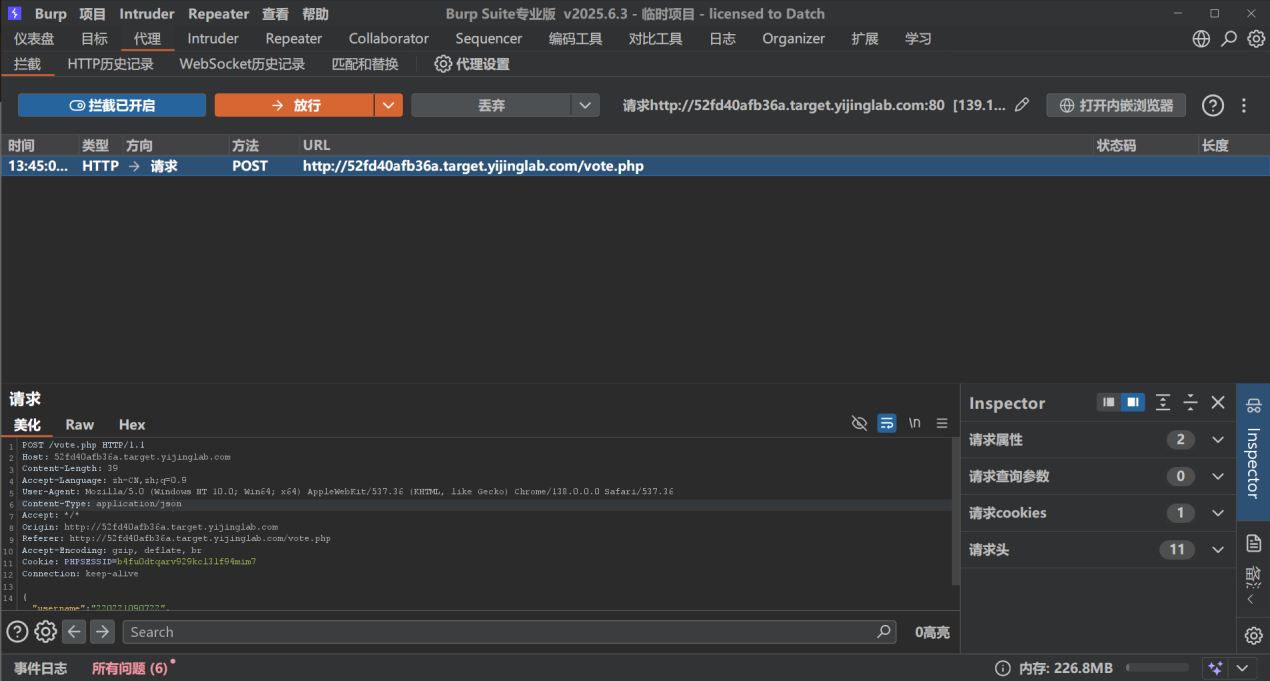
[3. …… 5](#_Toc138683331)

1. **作业内容**

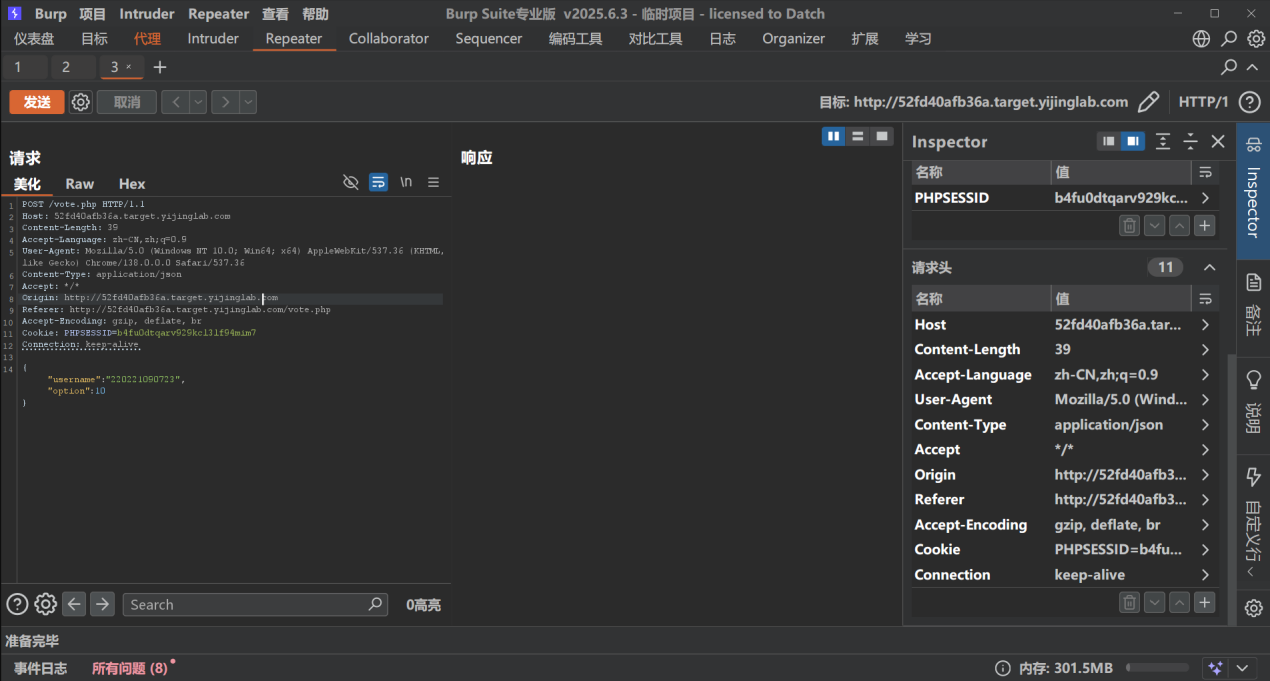
### 作业布置

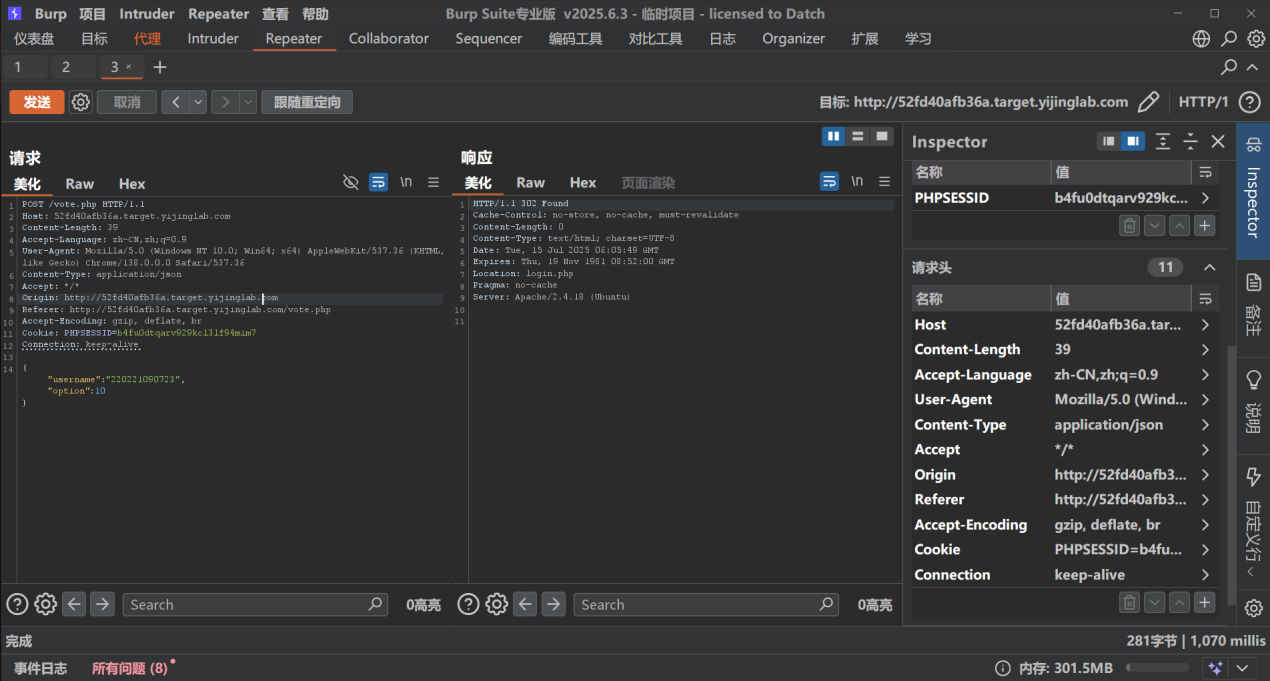
### 完成BP安装3开启投票实验，对其中一个用户投票5次以上

1. **操作步骤**
2. 打开教学平台，开启业务逻辑刷票实验  
   2、打开BP和内置浏览器，正常登录和注册(记住:不要开启拦截)



3、开启拦截、点击投票，抓取投票的数据包  
4、在数据包处，鼠标右键将数据发送给重放模块



5、选择重放器，点击发送，即可重放攻击和测试  


1. **作业总结**

本次作业主要围绕 Burp Suite 工具的安装与使用展开，通过实战操作加深了对 HTTP 请求拦截、数据包重放等核心功能的理解。按照课件内容，完成了 Burp Suite 的解压安装、授权激活及内置浏览器配置，顺利搭建完成测试环境。在业务逻辑刷票实验环节，通过开启教学平台并正常注册登录后，利用 Burp Suite 的 Proxy 模块成功抓取了投票操作对应的 HTTP POST 数据包。随后将该数据包发送至 Repeater 模块，并进行多次手动重放，模拟了对同一用户连续投票的攻击行为，最终实现对目标用户投票 5 次以上，符合实验预期目标。实验过程中进一步掌握了 Burp Suite 在 Web 渗透测试中的基础操作流程，包括数据拦截、中间人劫持、请求参数编辑与响应分析等，为后续深入学习漏洞挖掘（如重放攻击、权限绕过、参数污染等）奠定了良好基础。本次作业突出了“工具实操 + 渗透逻辑理解”的结合，帮助我明确了 Web 安全测试的技术路径与操作细节，认识到逻辑漏洞往往来源于对业务规则的滥用或绕过，今后需在理解业务流程的基础上灵活运用工具实现渗透测试目标。