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)

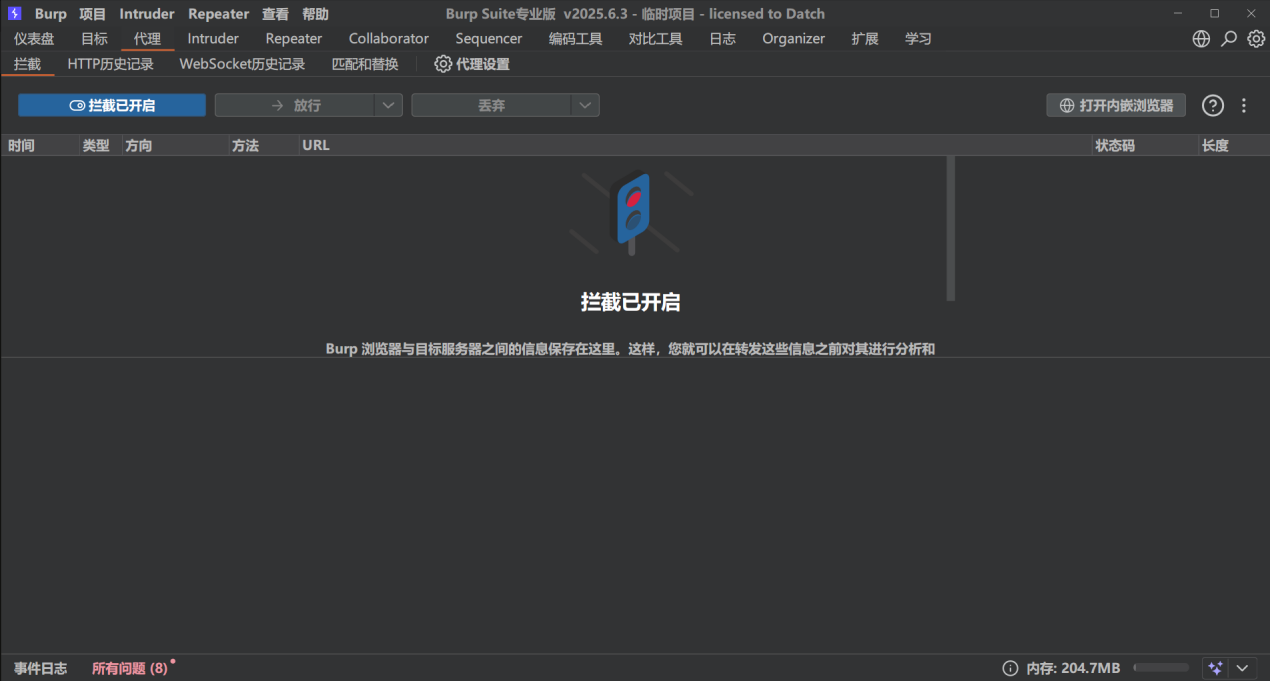
**[三、](#_Toc138683328)****[作业总结](#_Toc138683328)** [5](#_Toc138683328)

[1. xxxxx 5](#_Toc138683329)

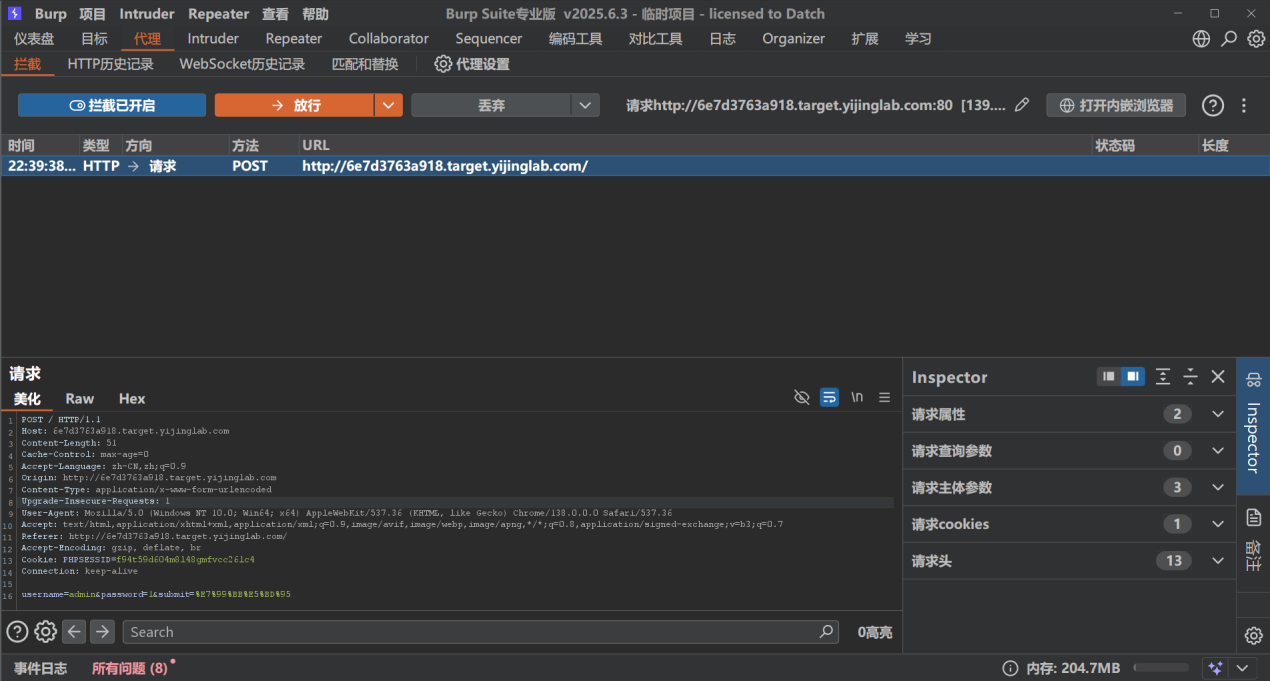
[2. xxxxx 5](#_Toc138683330)

[3. …… 5](#_Toc138683331)

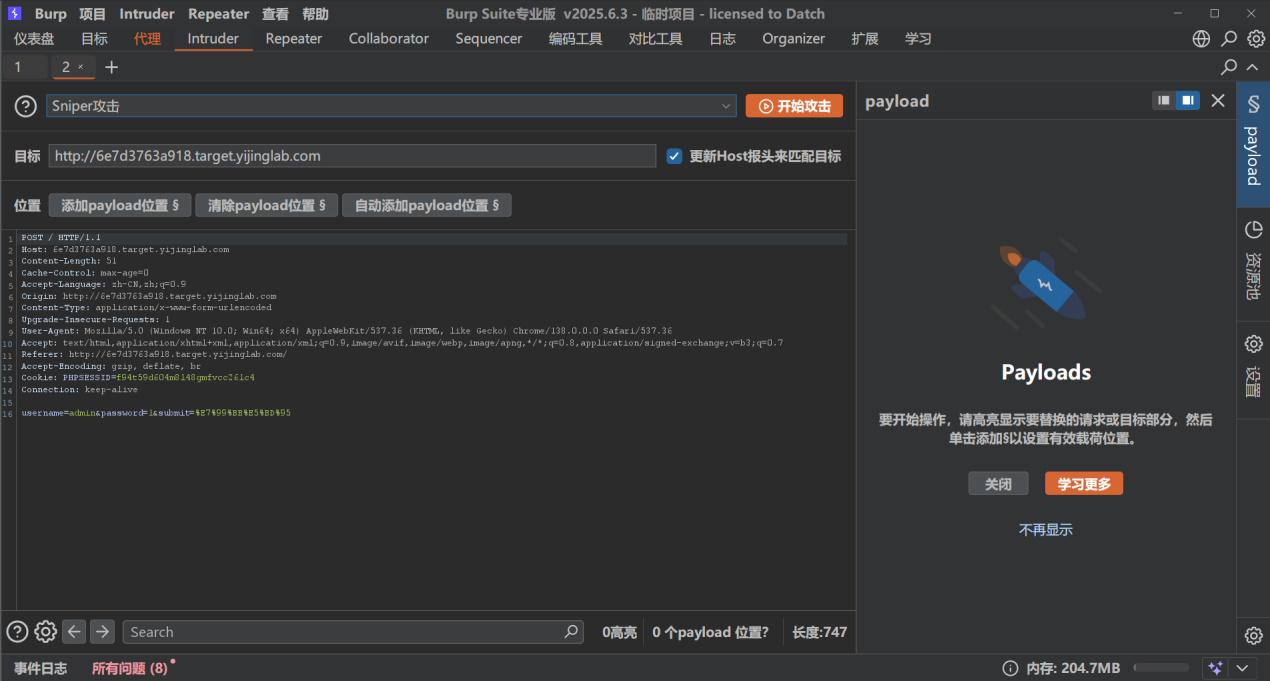
1. **作业内容**
2. 下载FUZZ字典理解FUZZ技术核心思想
3. 2、利用BP完成实验密码破解
4. **操作步骤**
5. 打开BP自带的浏览器，开启数据包拦截功能，输入账号密码



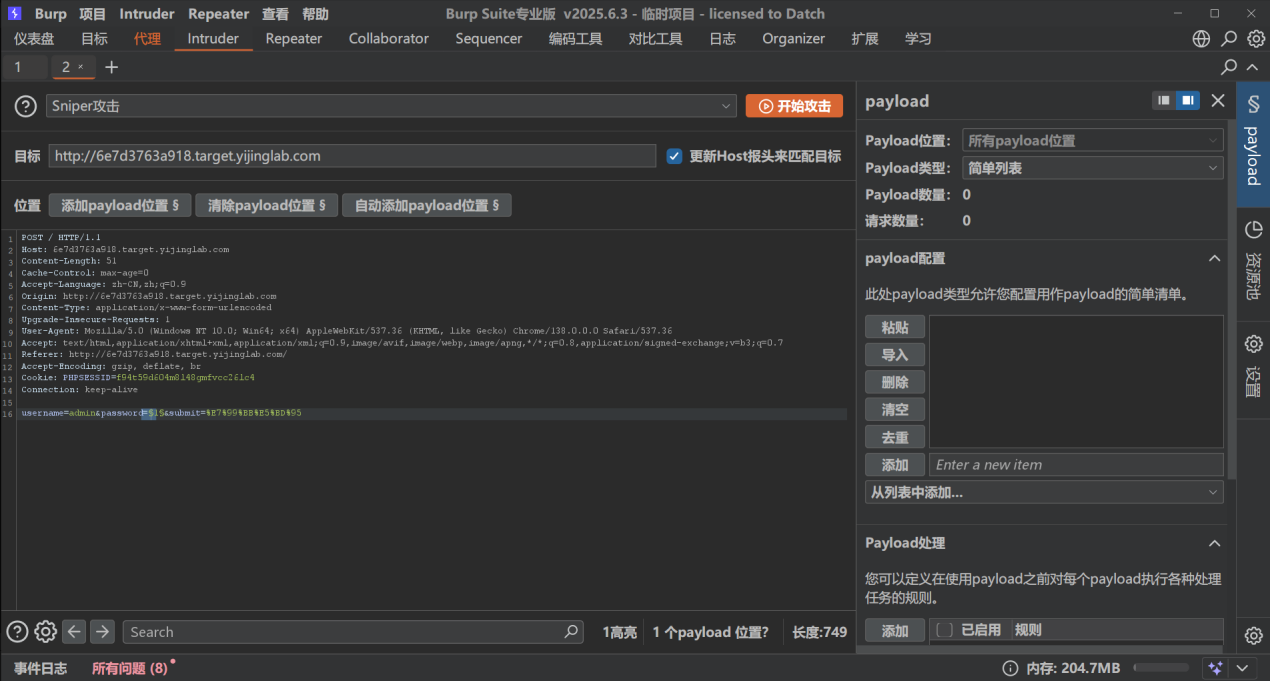
1. 点击登录、BP就会拦截到登录的数据包，俗称抓包



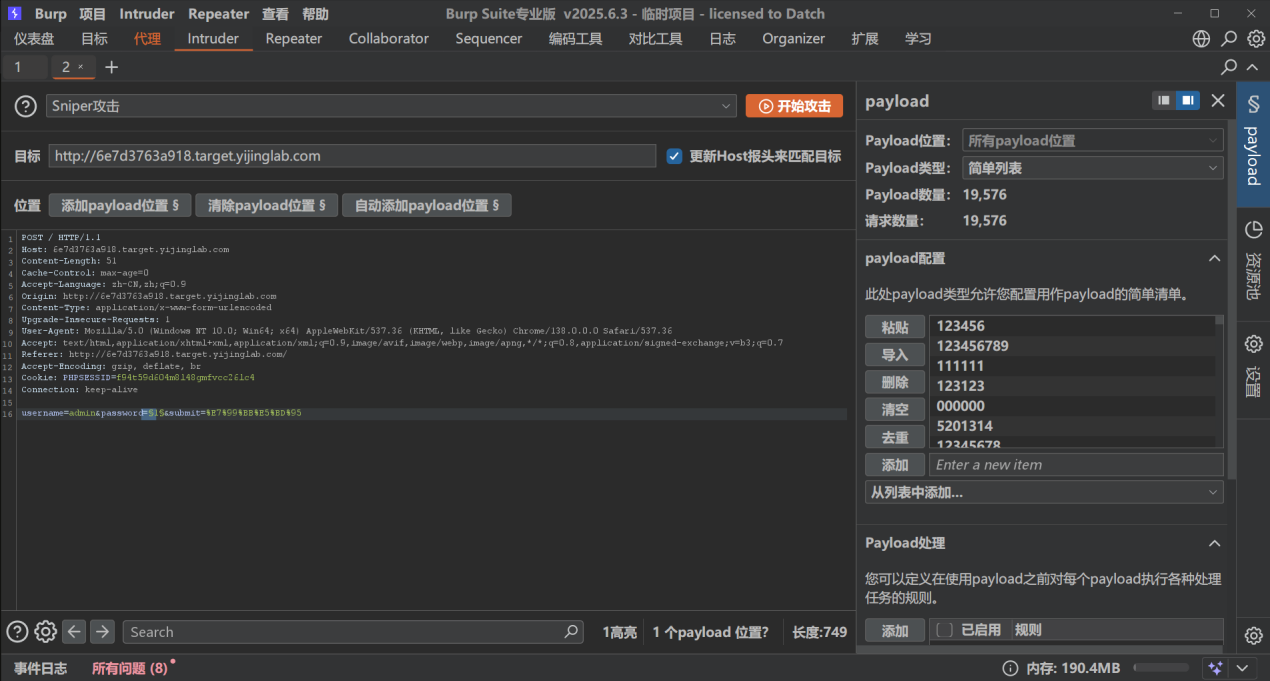
3.将数据包发送【intruder】模块，开始准备进行密码破解



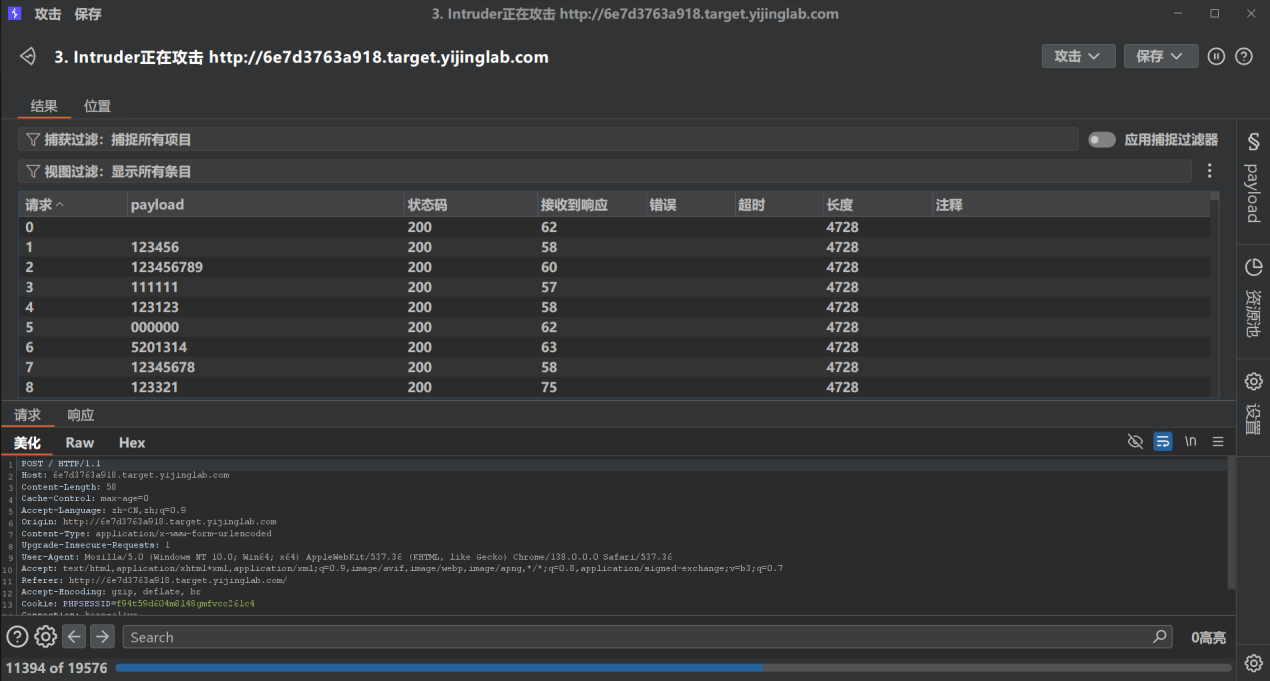
4.标记需要破解的内容，告诉BP你要破解什么地方

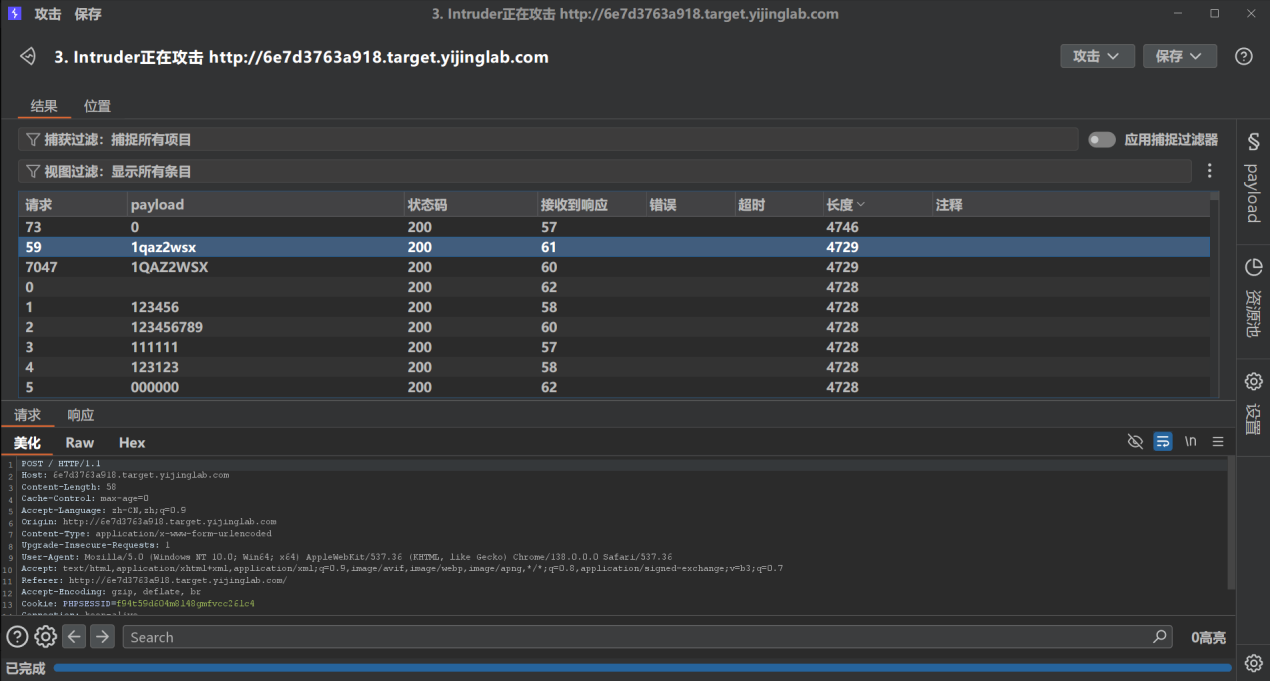


5.添加字典到BP中，【字典】在网盘中有教程



6.点击开始攻击，BP会新打开一个破解窗口



1. 通过【长度】【响应码】等判断是否成功  
     
   破解成功，密码为：1qaz2wsx
2. **作业总结**

1.深入理解FUZZ技术原理

通过查阅FUZZ字典并结合实际操作，对FUZZ技术的核心思想有了更系统的认识。FUZZ作为一种通过大量自动化输入测试以发现程序漏洞的技术，其本质是输入变异和结果反馈的自动迭代，广泛应用于接口测试、安全扫描与弱口令探测等场景。

2.掌握了Burp Suite的基础使用流程

本次实验通过Burp Suite实现了对Web登录接口的数据包拦截与分析，熟悉了从【抓包】到【intruder模块配置】再到【字典导入与爆破执行】的完整流程。特别是在标记爆破字段和分析响应差异（如响应长度）过程中，提升了对Web渗透测试工具实际应用的理解。

3.认识到信息安全攻防实践的重要性

实验虽然简单，但模拟了真实攻击者可能采取的手段，进一步意识到输入验证、异常响应控制等后端安全机制的重要性。今后的学习中需要继续关注防御机制设计，以形成“攻防一体”的技术思维。