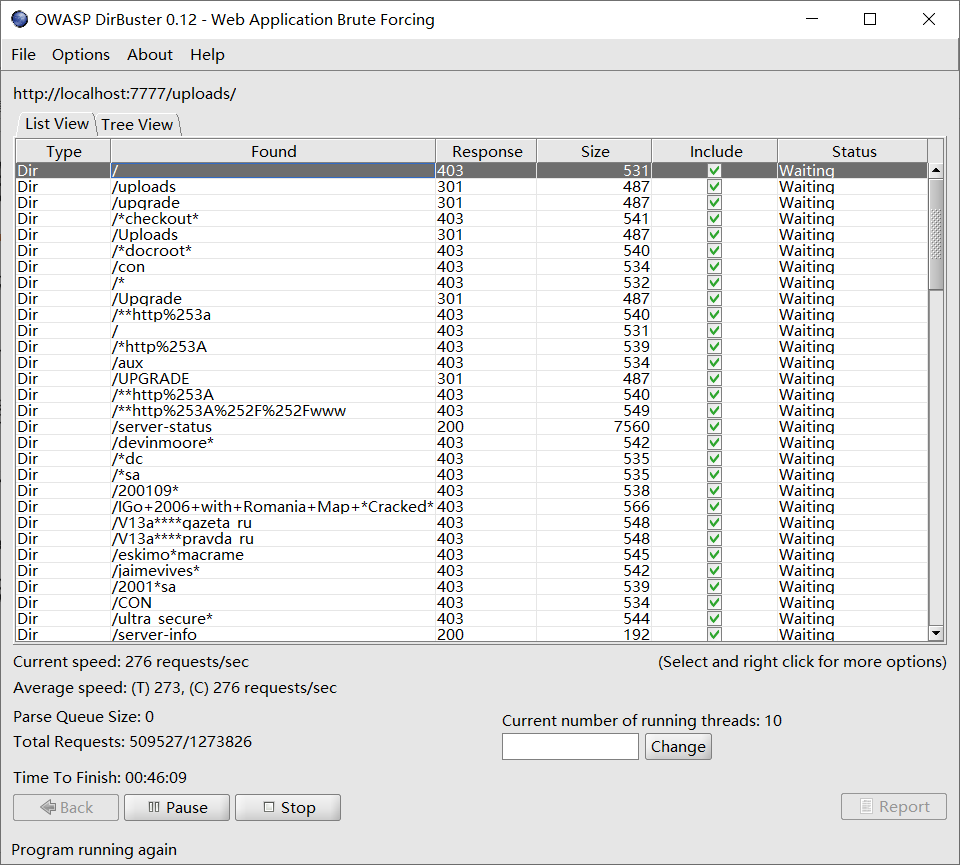
对网站bluecms\_1.6进行渗透测试

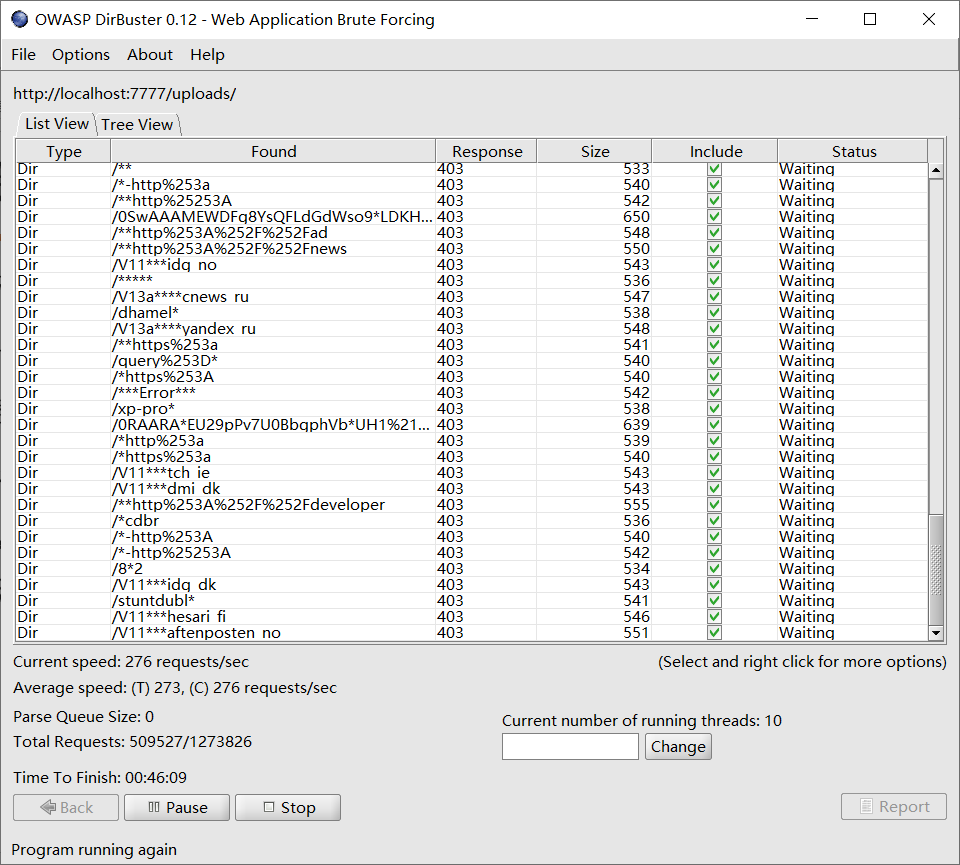
测试的内容：

**一、信息收集：**

（一）域名信息：无

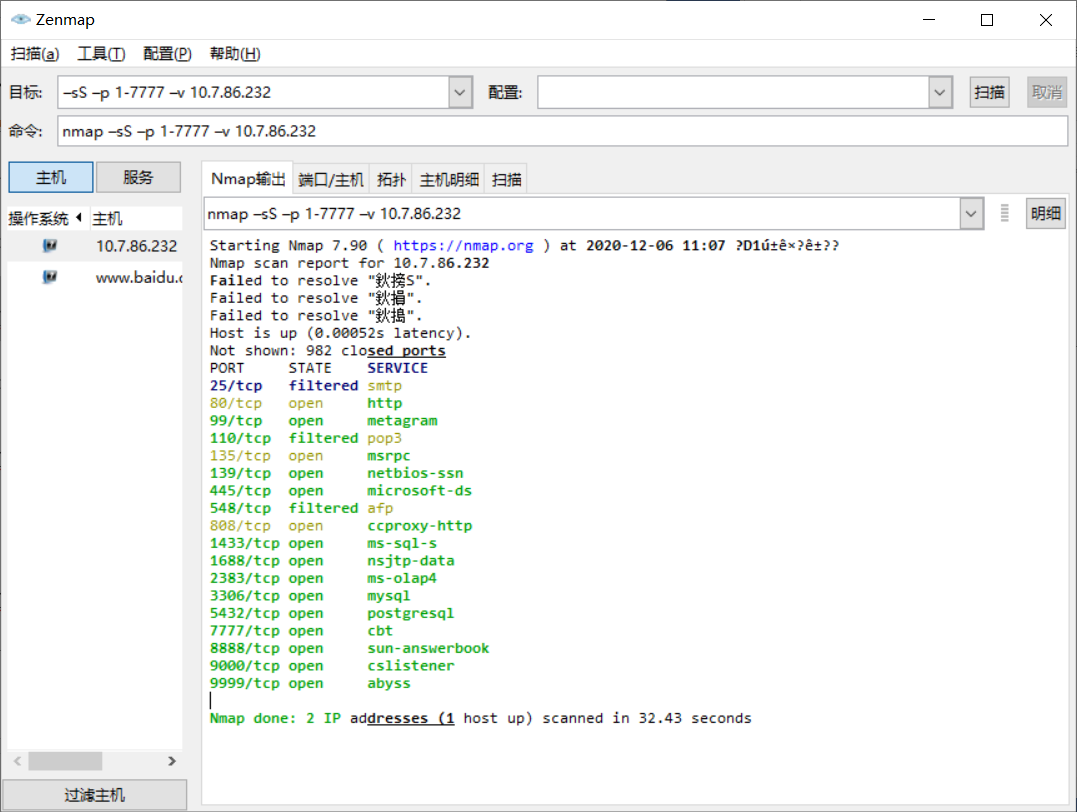
（二）敏感目录：使用DirBrust扫描





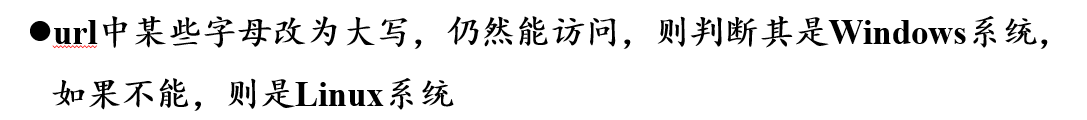
（三）端口扫描：（四）旁站C段：

1.扫描指定ip所开放的端口：



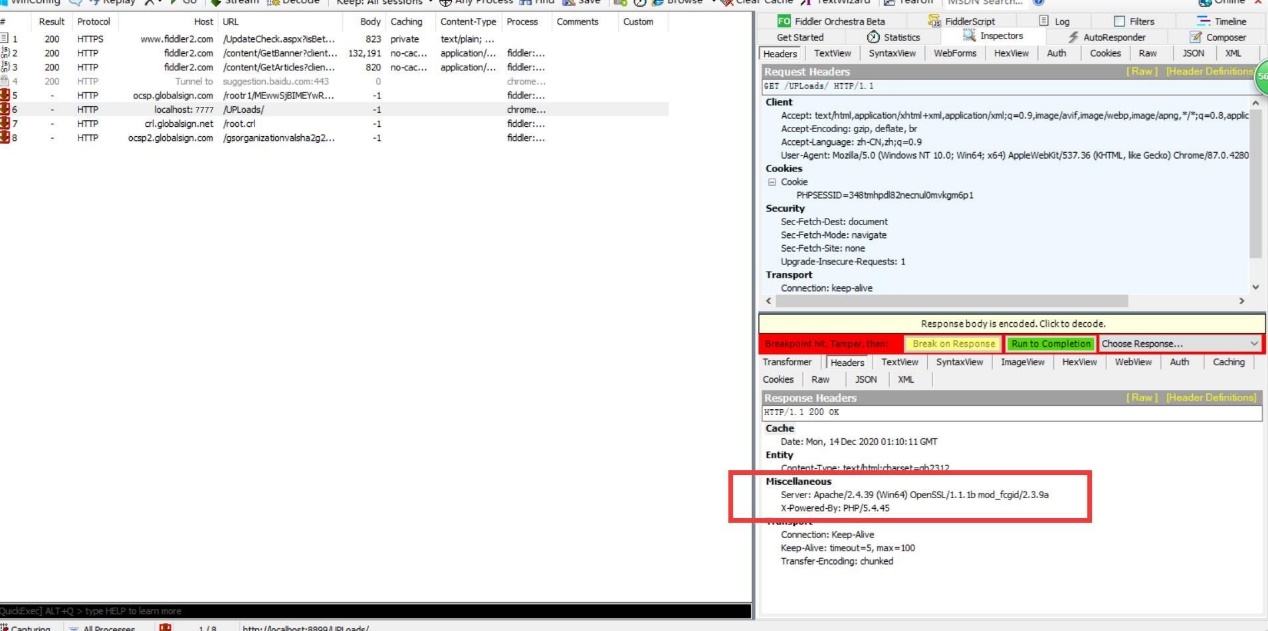
（五）整站分析

1.服务器的操作系统：



访问<http://localhost:7777/UPloads/>，仍能访问，是Windows系统

2.网站容器：Apache

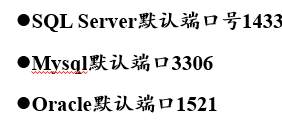


3.脚本类型：



脚本类型是php

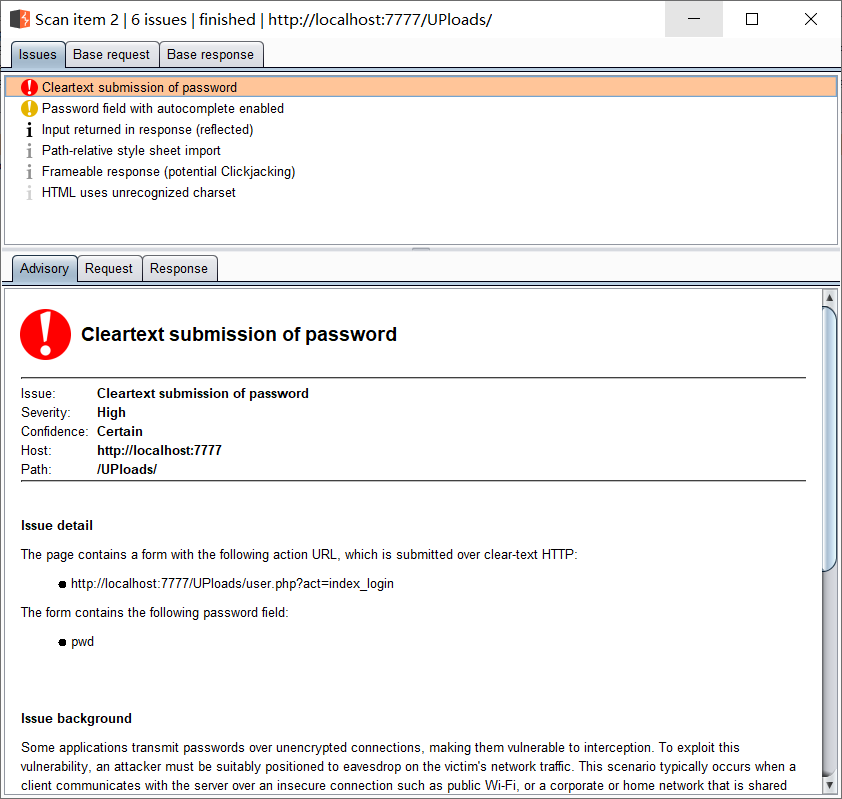
4.数据库类型:

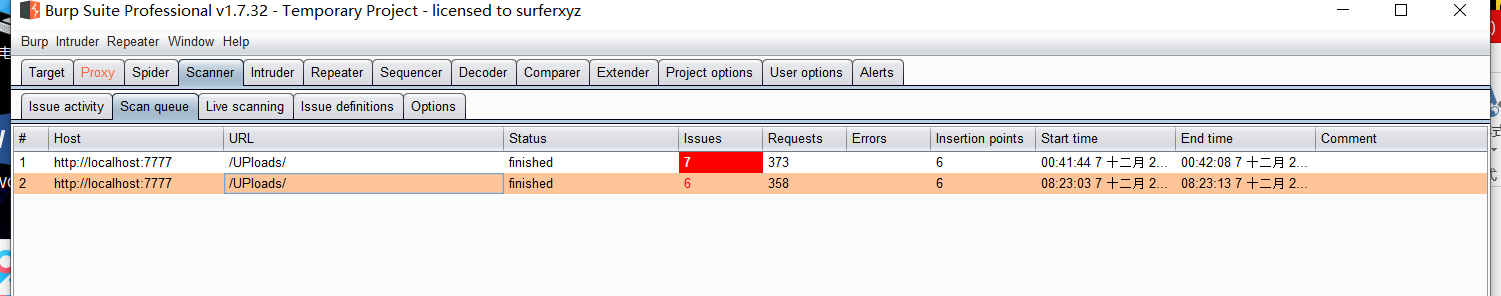


根据Nmap扫描结果来看，数据库是SQL server 和Mysql

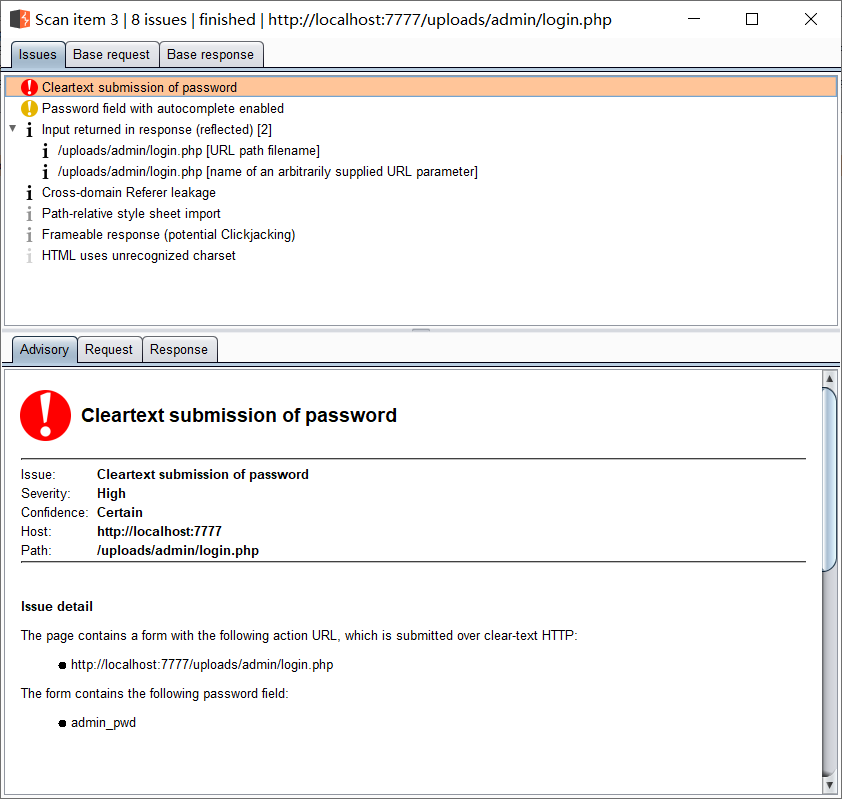
**二、利用burpsuit进行漏洞扫描：**

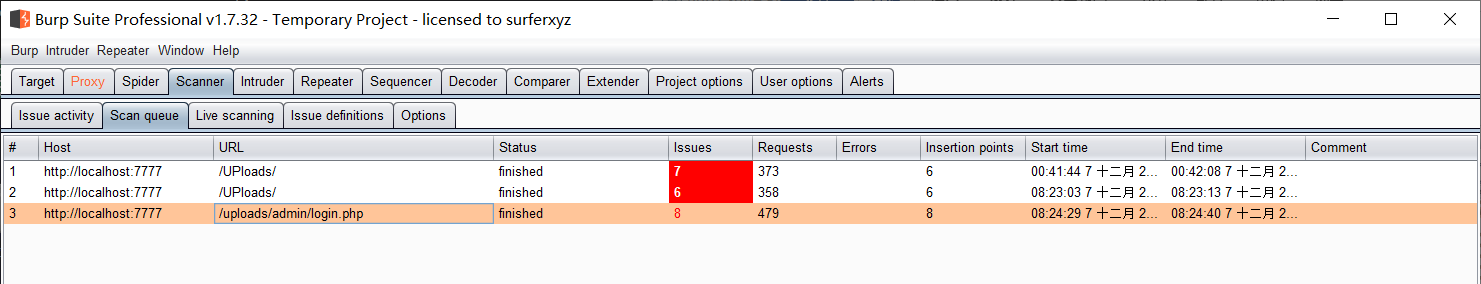
(一)前台：





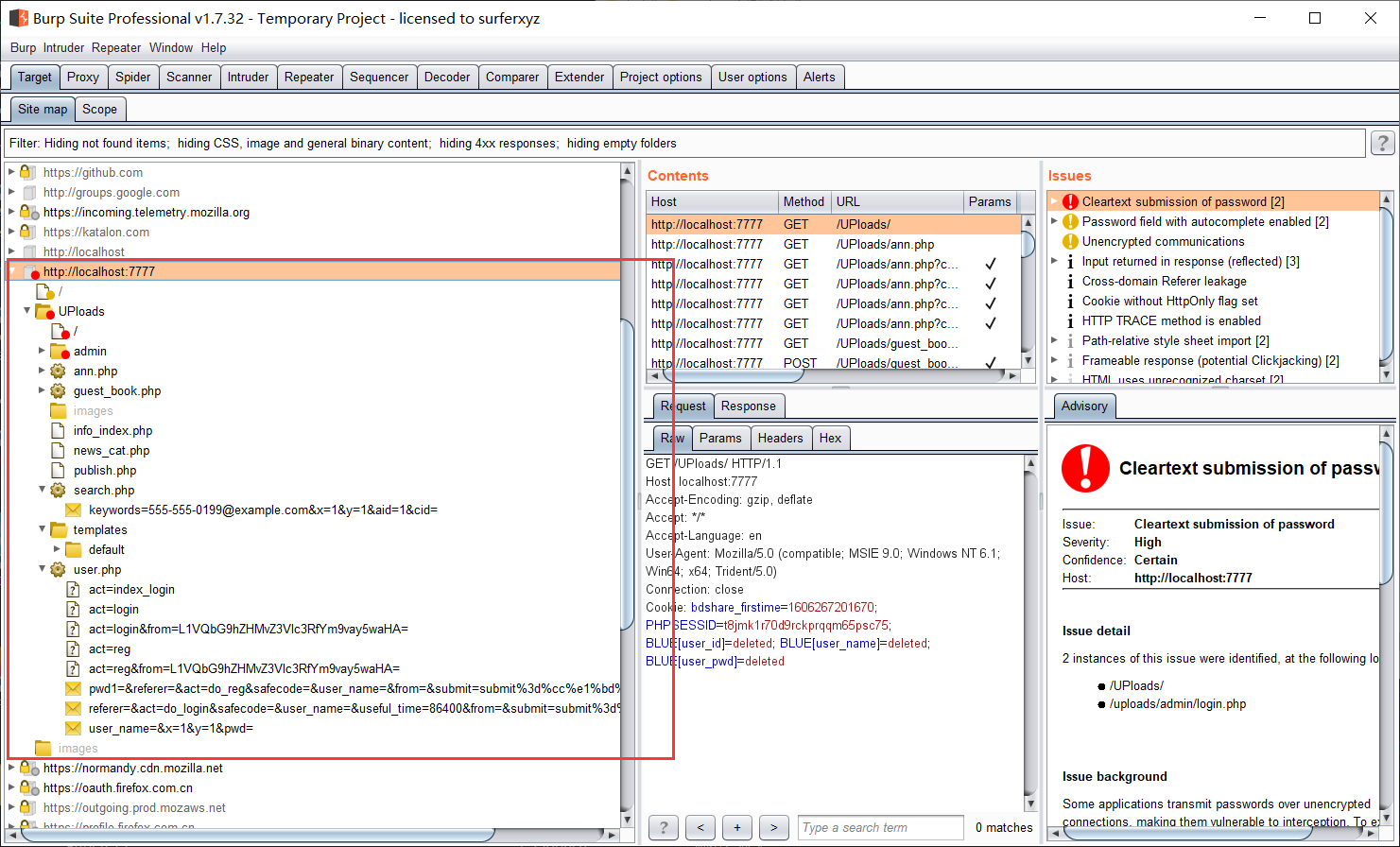
（二）后台：





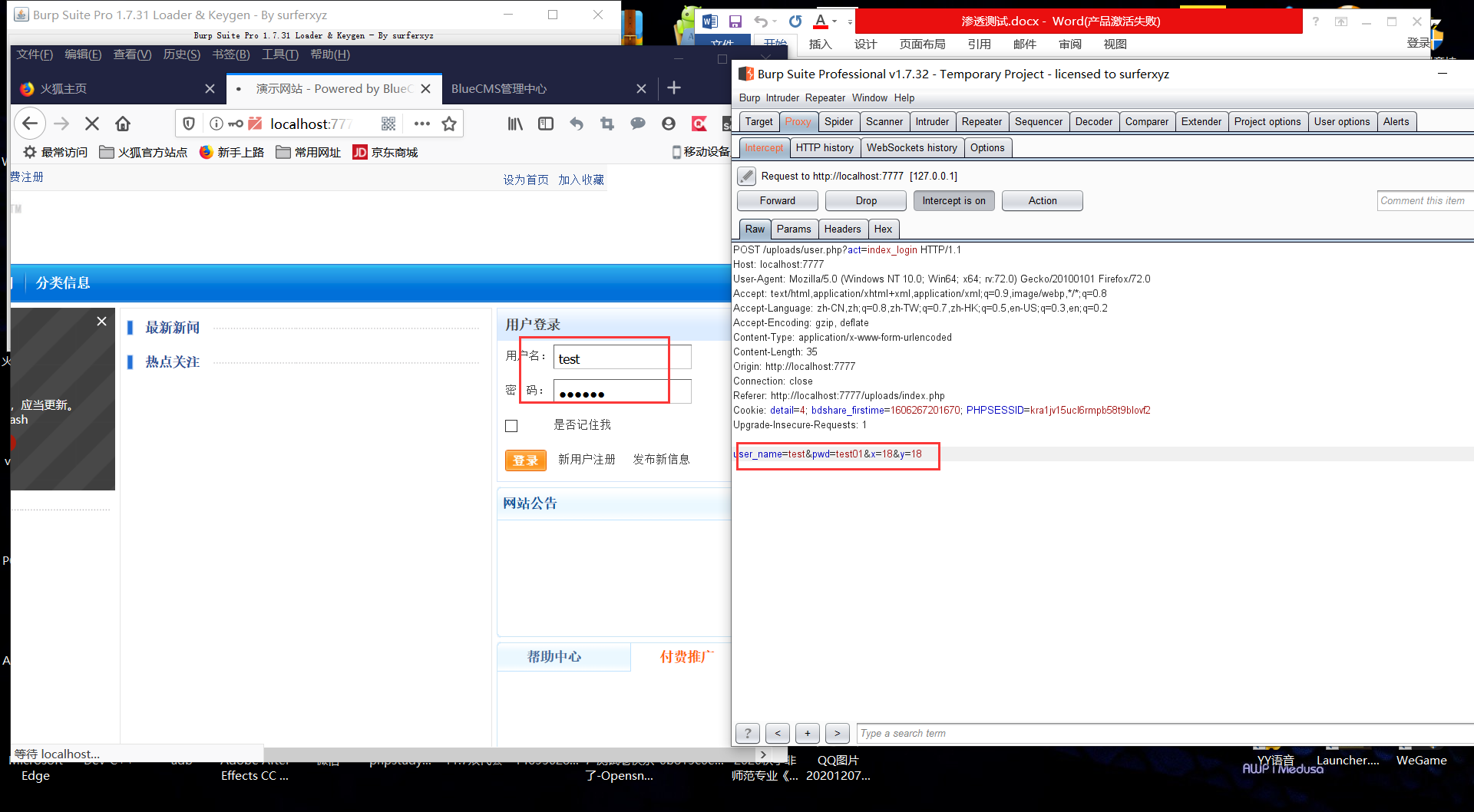
**三、爬取网站：**

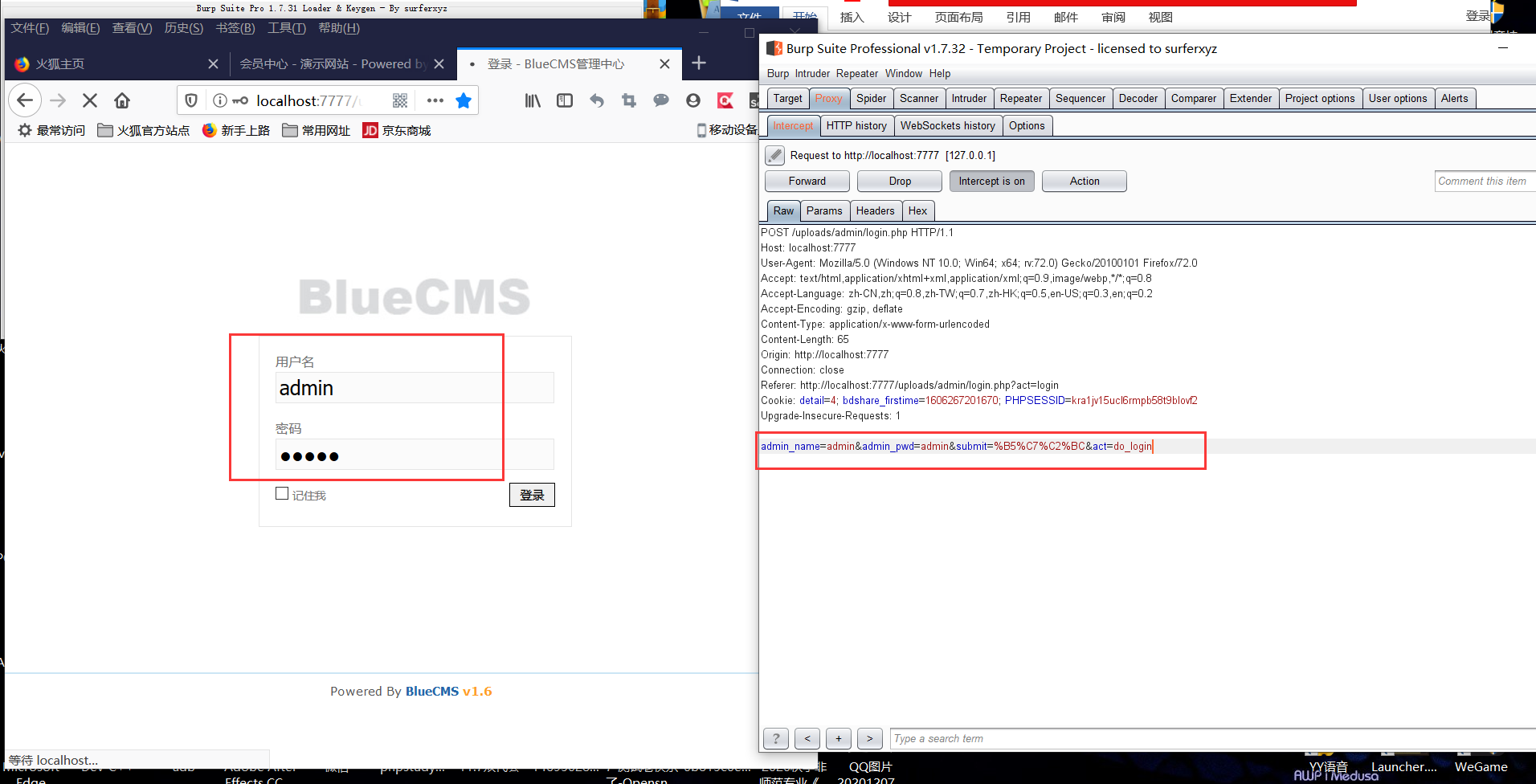
用WebRobot不能爬取，显示url格式错误，就使用Burp Suit进行爬取



**四、自动化攻击：**

1.密码明文传输：



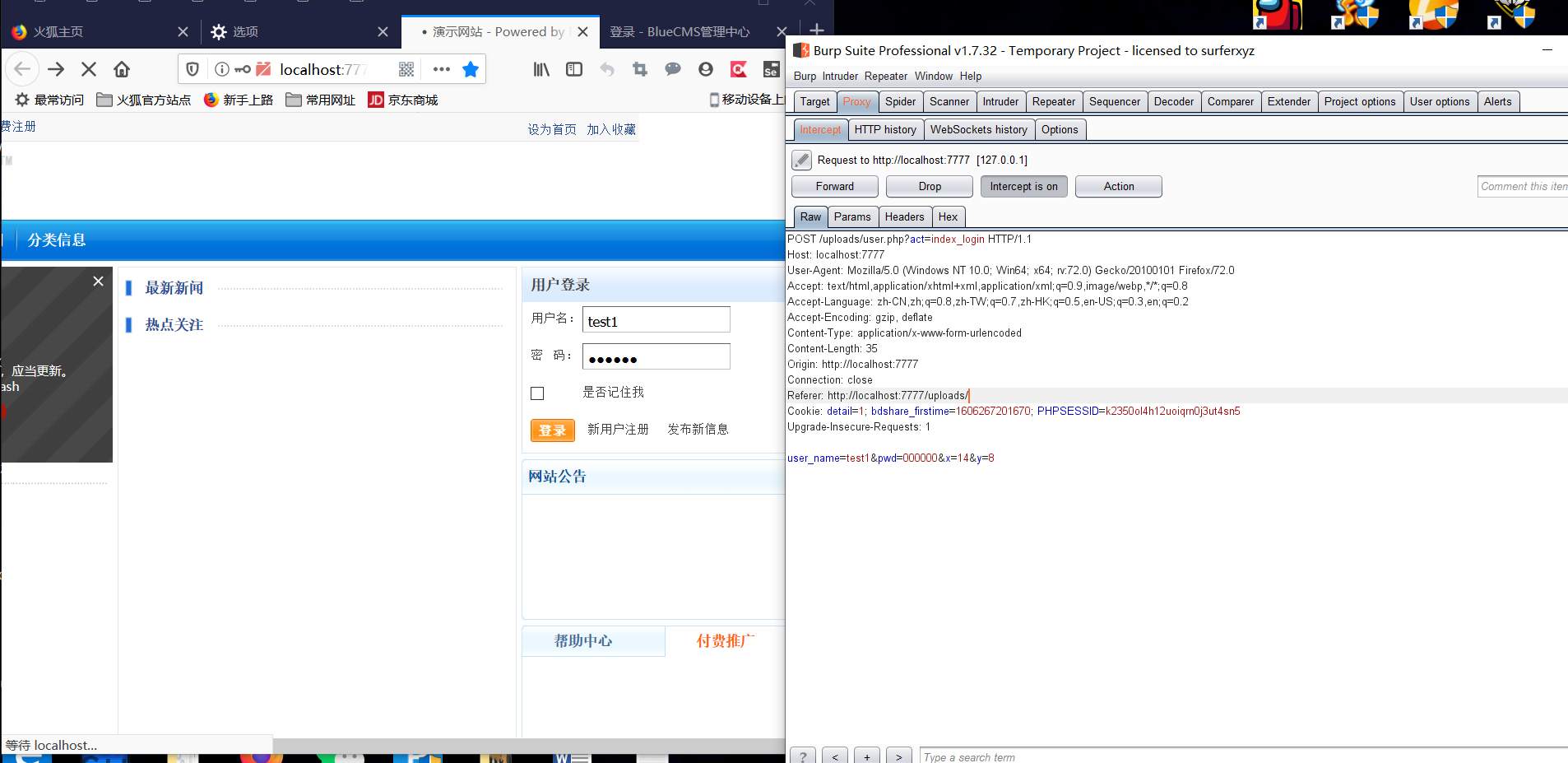


前后台都是密码明文传输

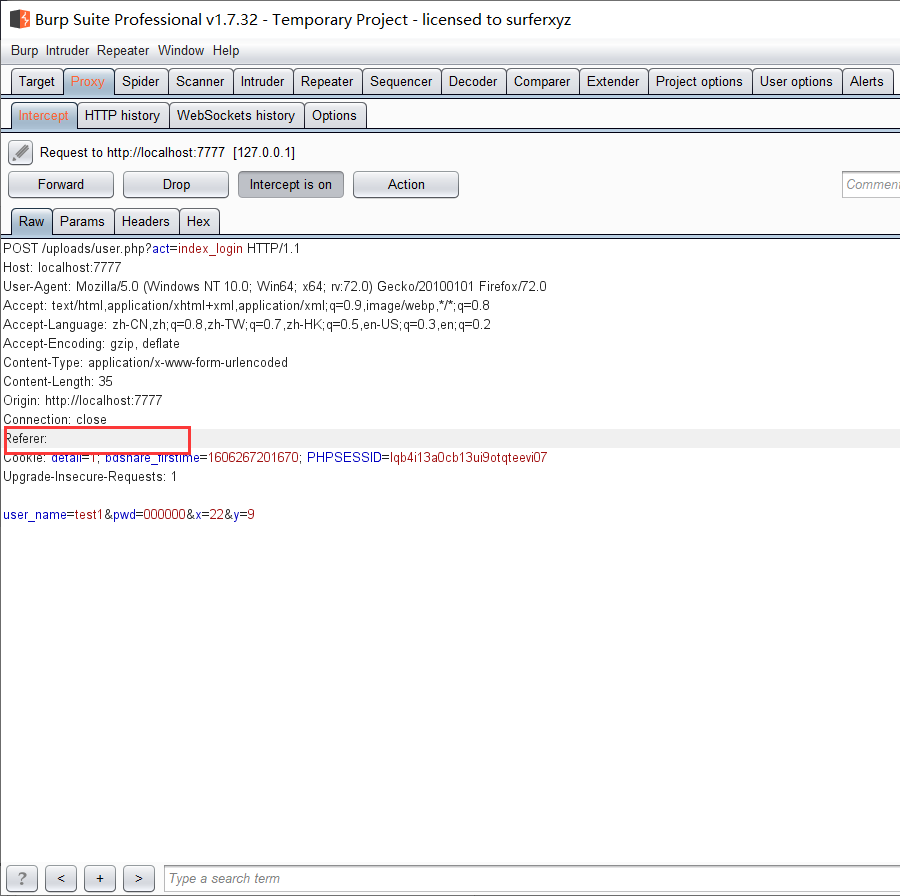
2.后台登录时我直接使用admin,admin就登录成功，弱密码

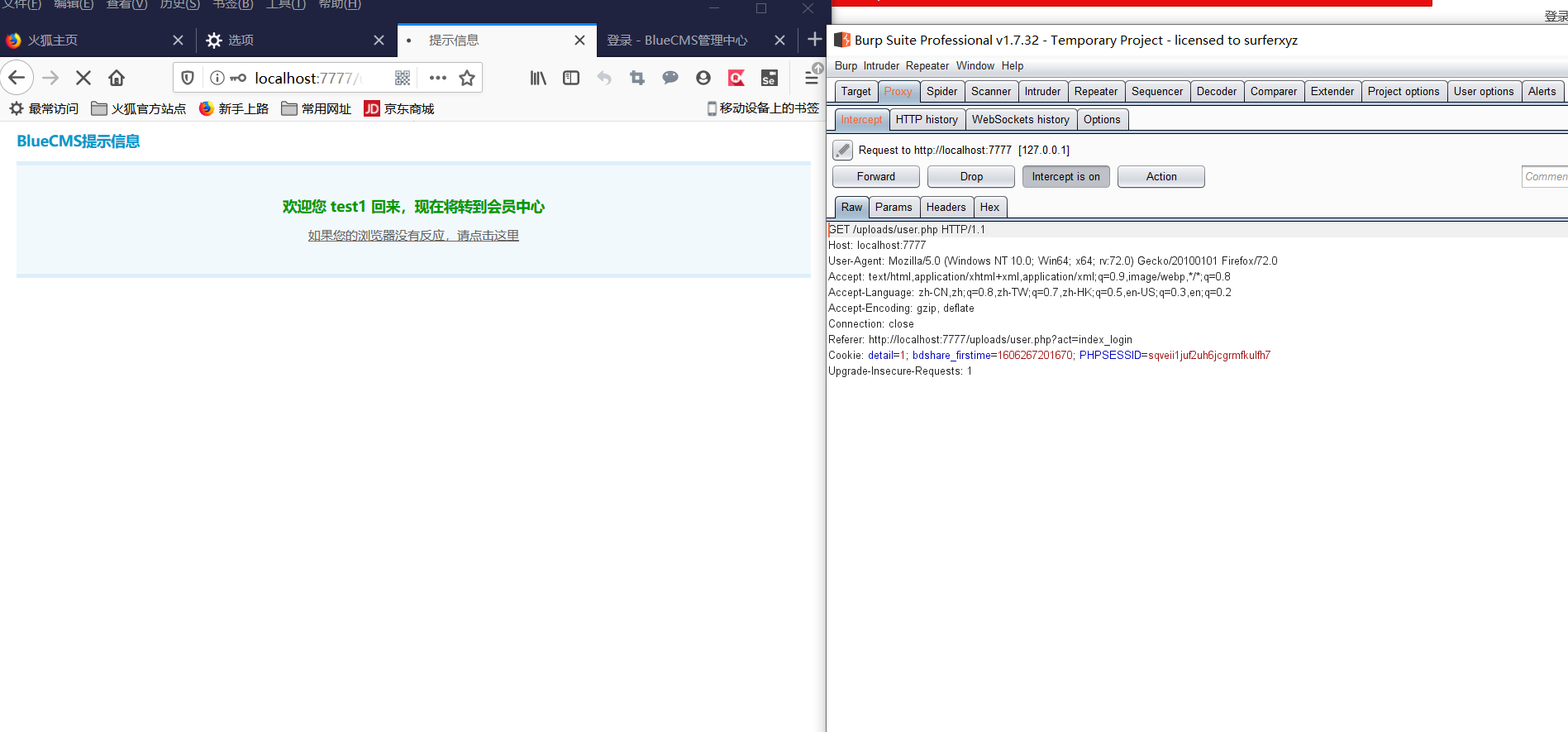
3.Csrf漏洞：

抓取请求：



去掉referer字段提交：





提交仍然有效：基本上可以确定存在CSRF漏洞

**五、对网站进行手工测试：**

Xss漏洞测试：

步骤：

1. 先进行登录
2. 然后在用户管理中点击我的个人资料
3. 在邮箱里面输入12345<script>alert('xss')</script>
4. 点击确认修改

结果：

弹出xss弹框，每次打开这个界面都会弹出xss弹框

存在xss存储型漏洞

