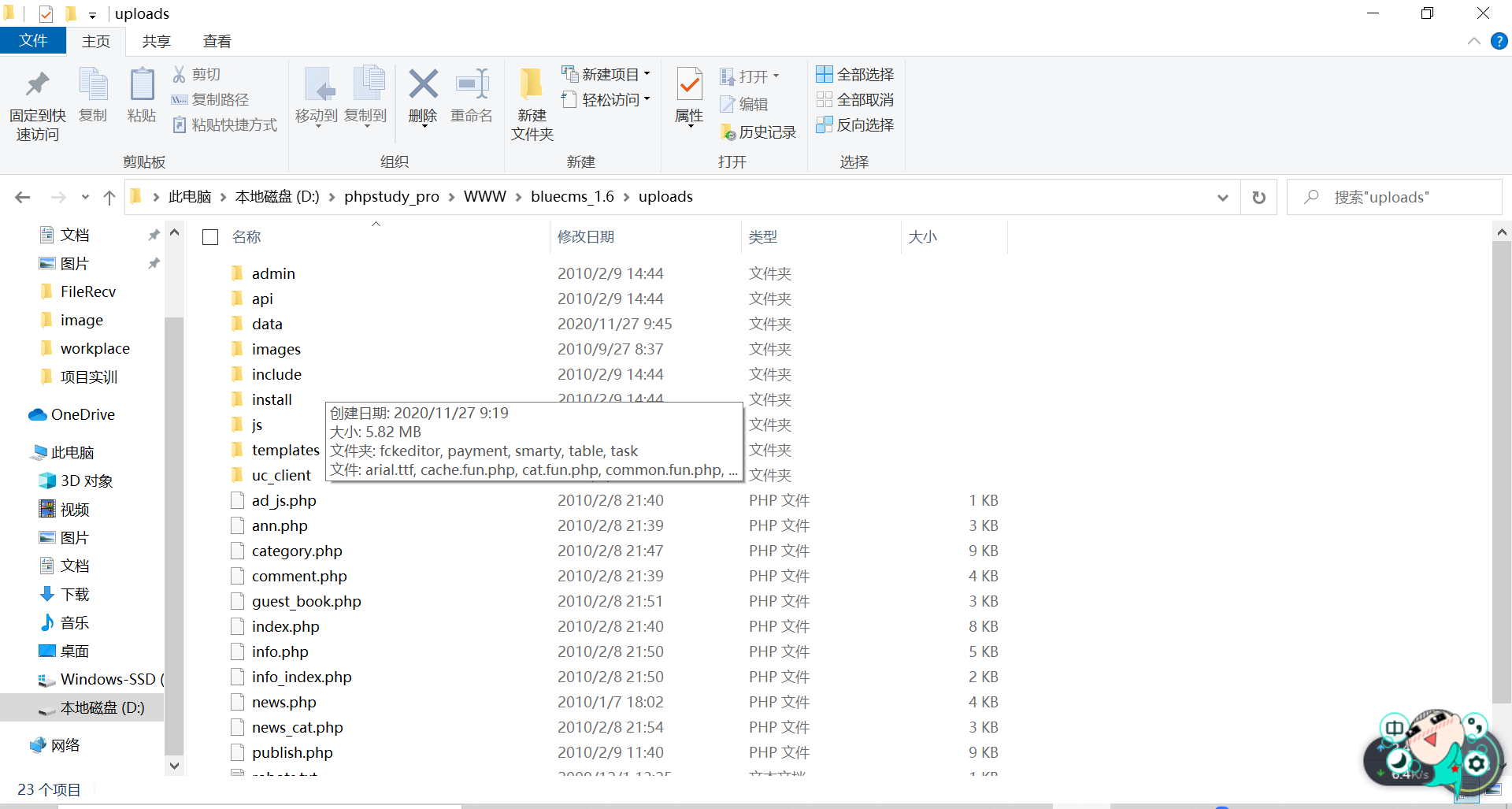
1.信息收集

Ip（本地ip）10.7.86.53

搭建的网站BLUECMS基于phpstudy\_pro的本地网站

观察基本的网站结构



2.漏洞扫描

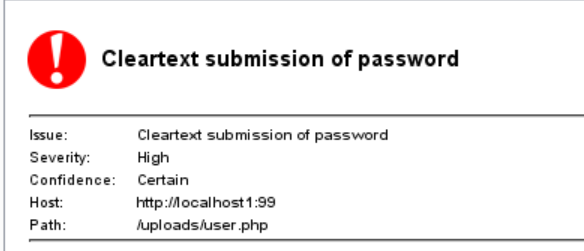
（1）利用burpsuit对网站bluecms\_1.6前台网站进行漏洞扫描：

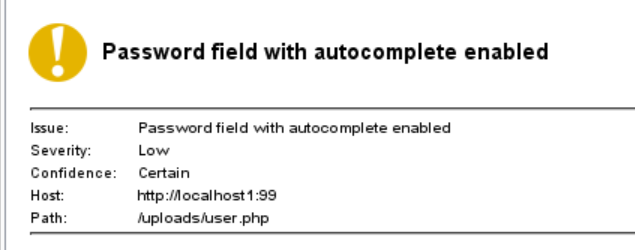
主要漏洞有：

1. 无加密通信



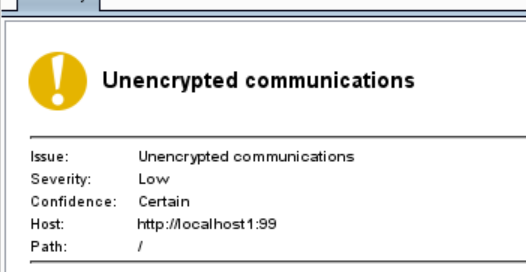
1. 明文提交密码



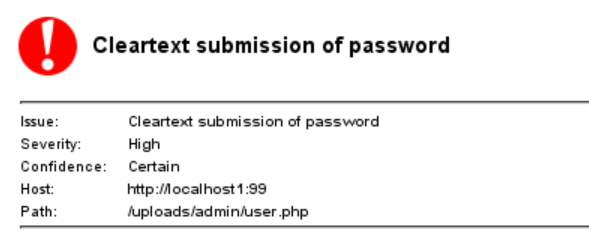
③启用自动完成的密码字段

1. 利用burpsuit对网站bluecms\_1.6后台网站进行漏洞扫描：

①未加密通信



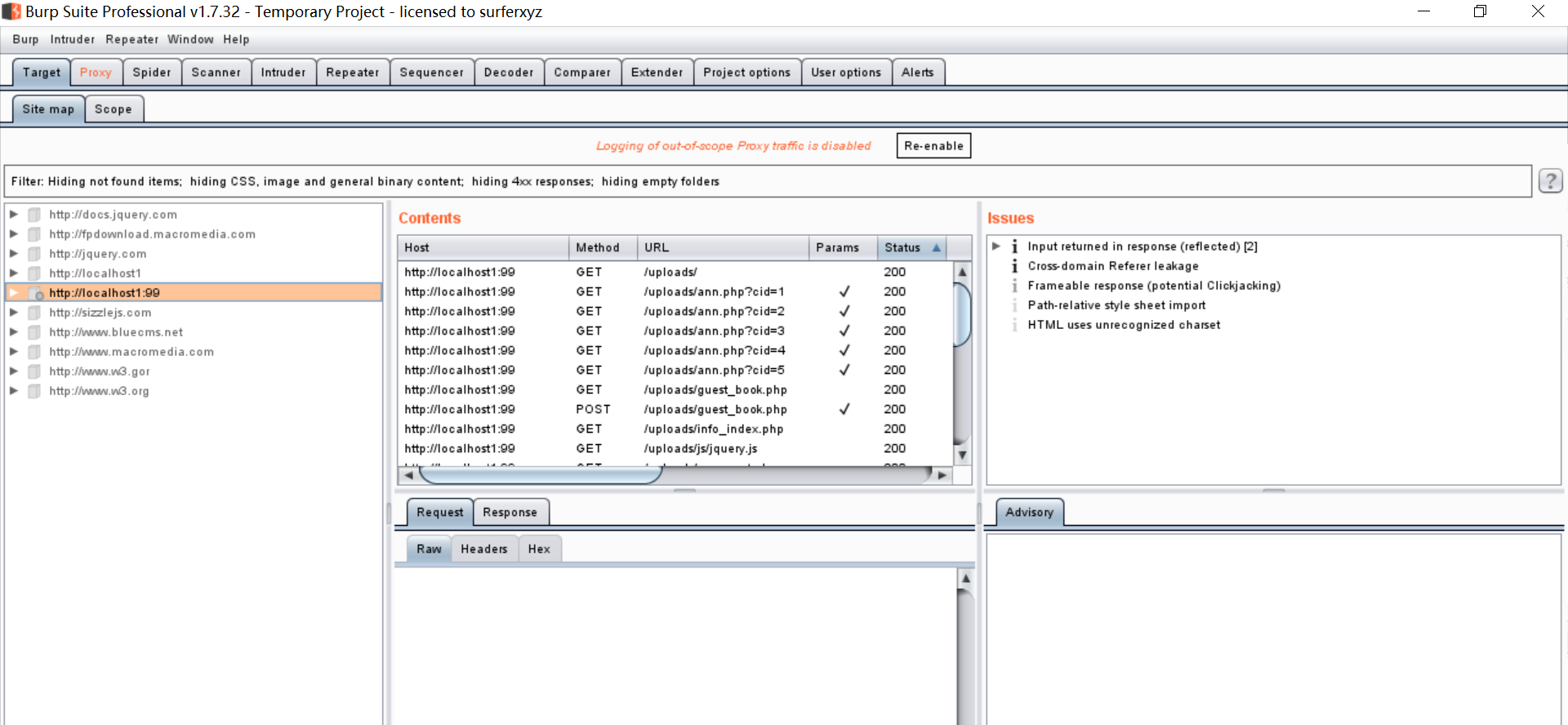
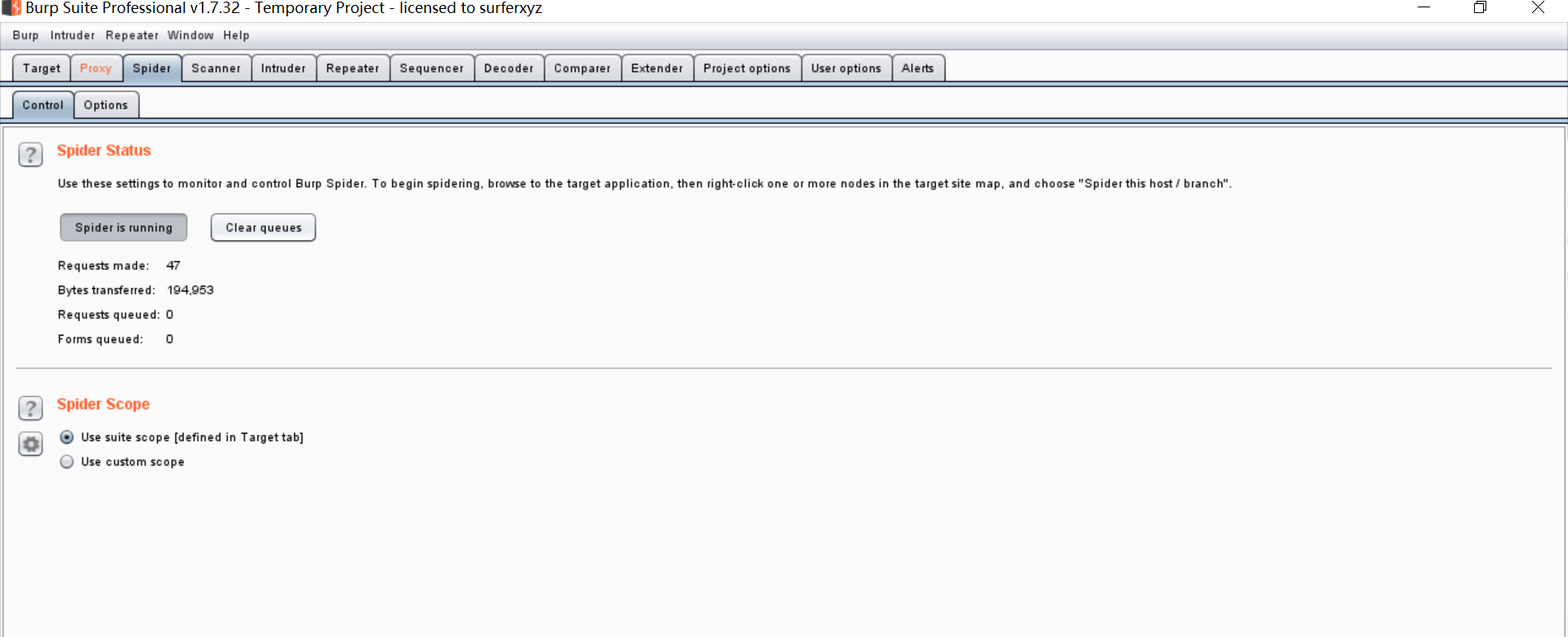
1. 明文提交密码



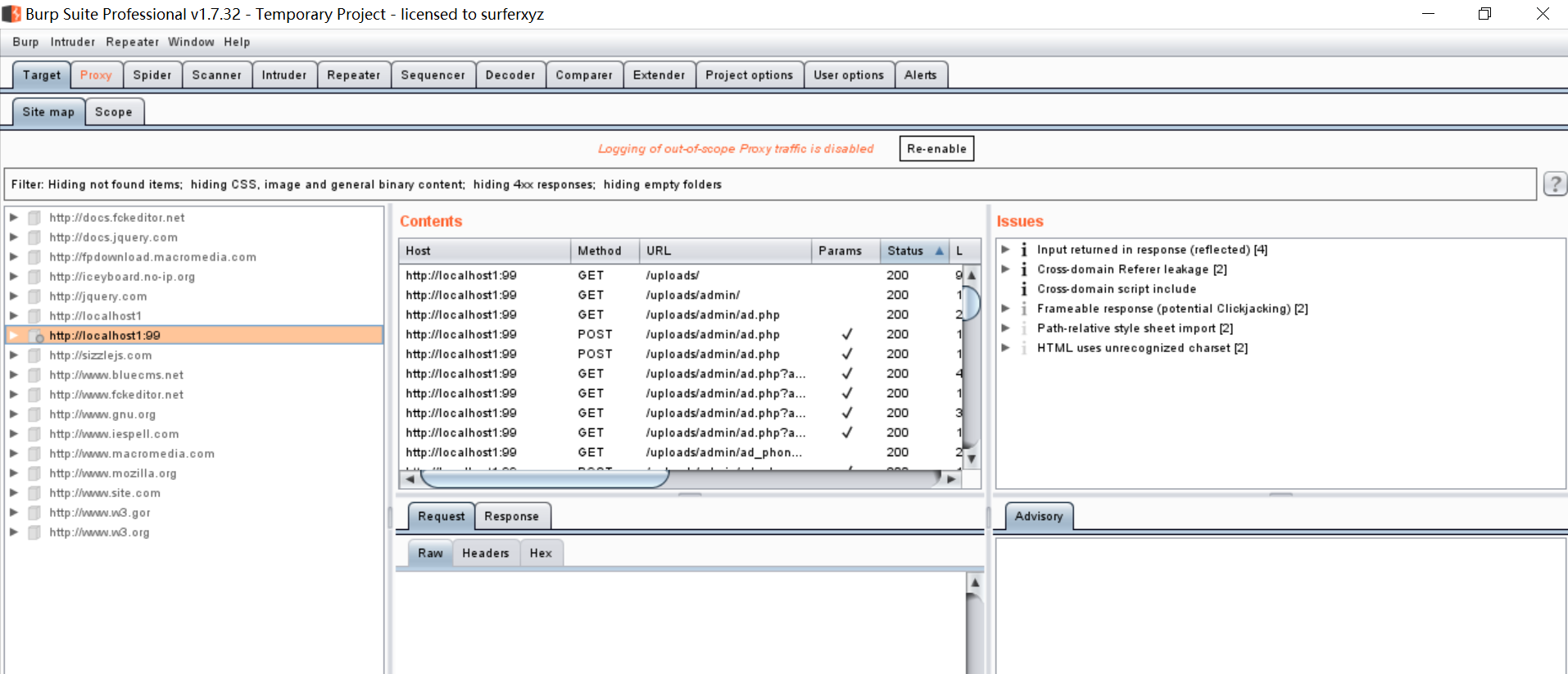
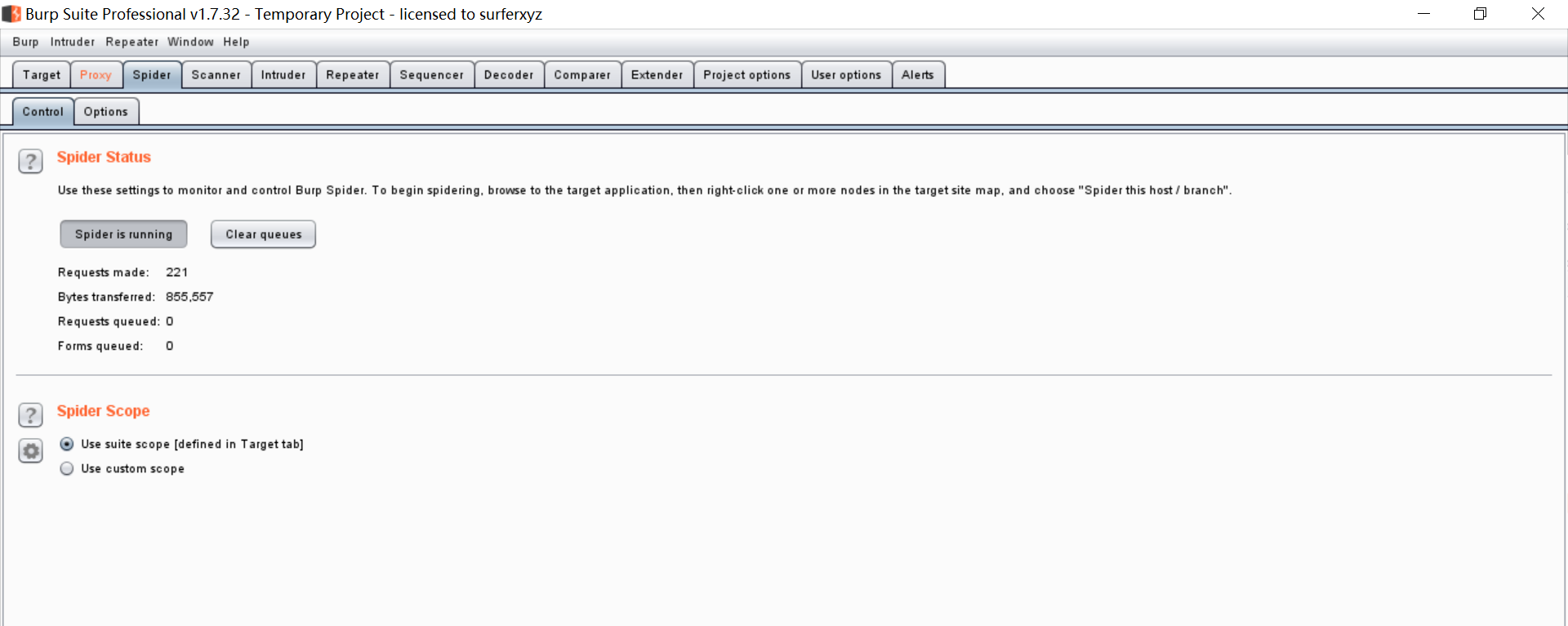
③启用自动完成的密码字段

3.网站爬取

（1）利用burpsuit进行爬取网站：前台网站

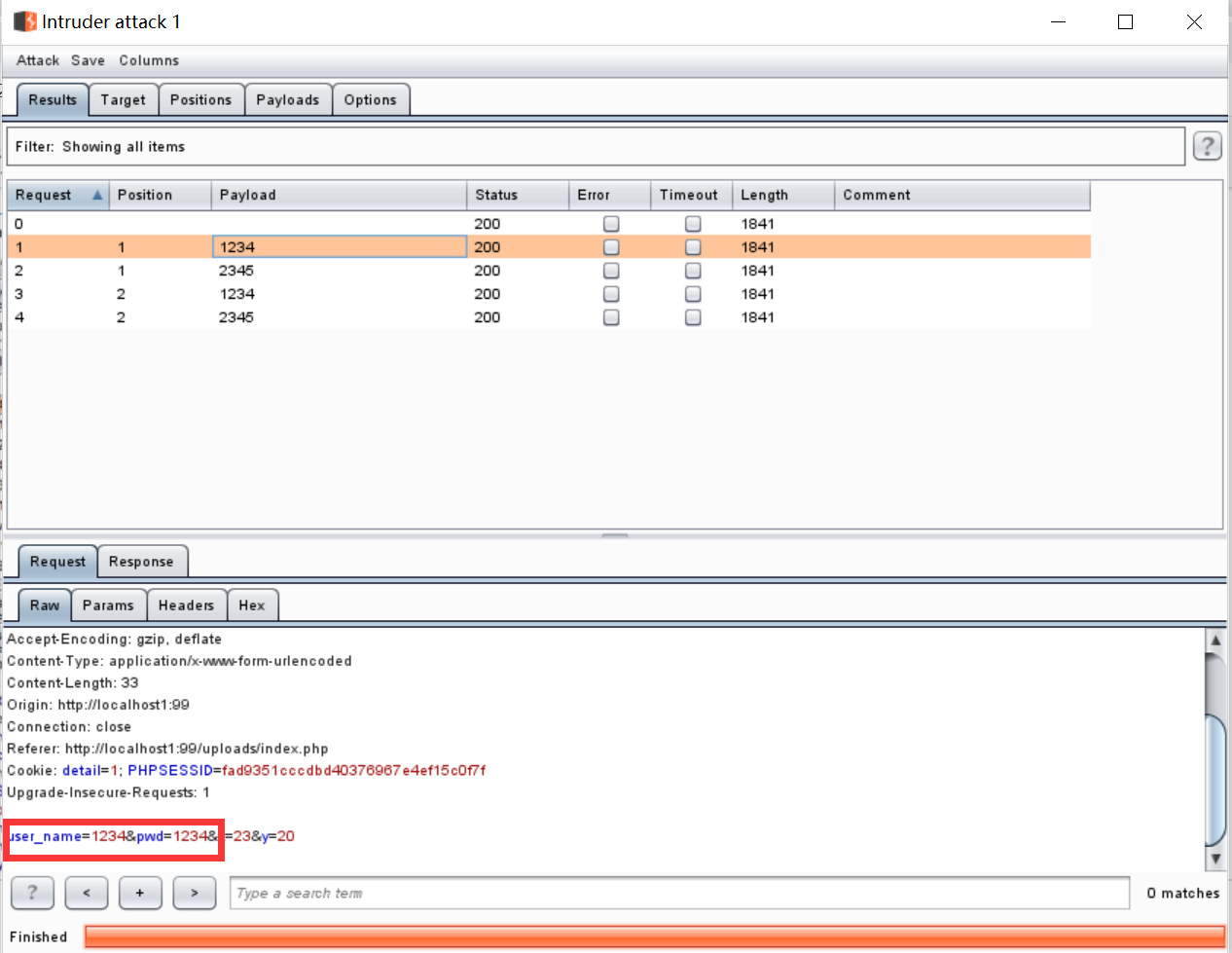
（2）利用burpsuit进行爬取网站：后台网站

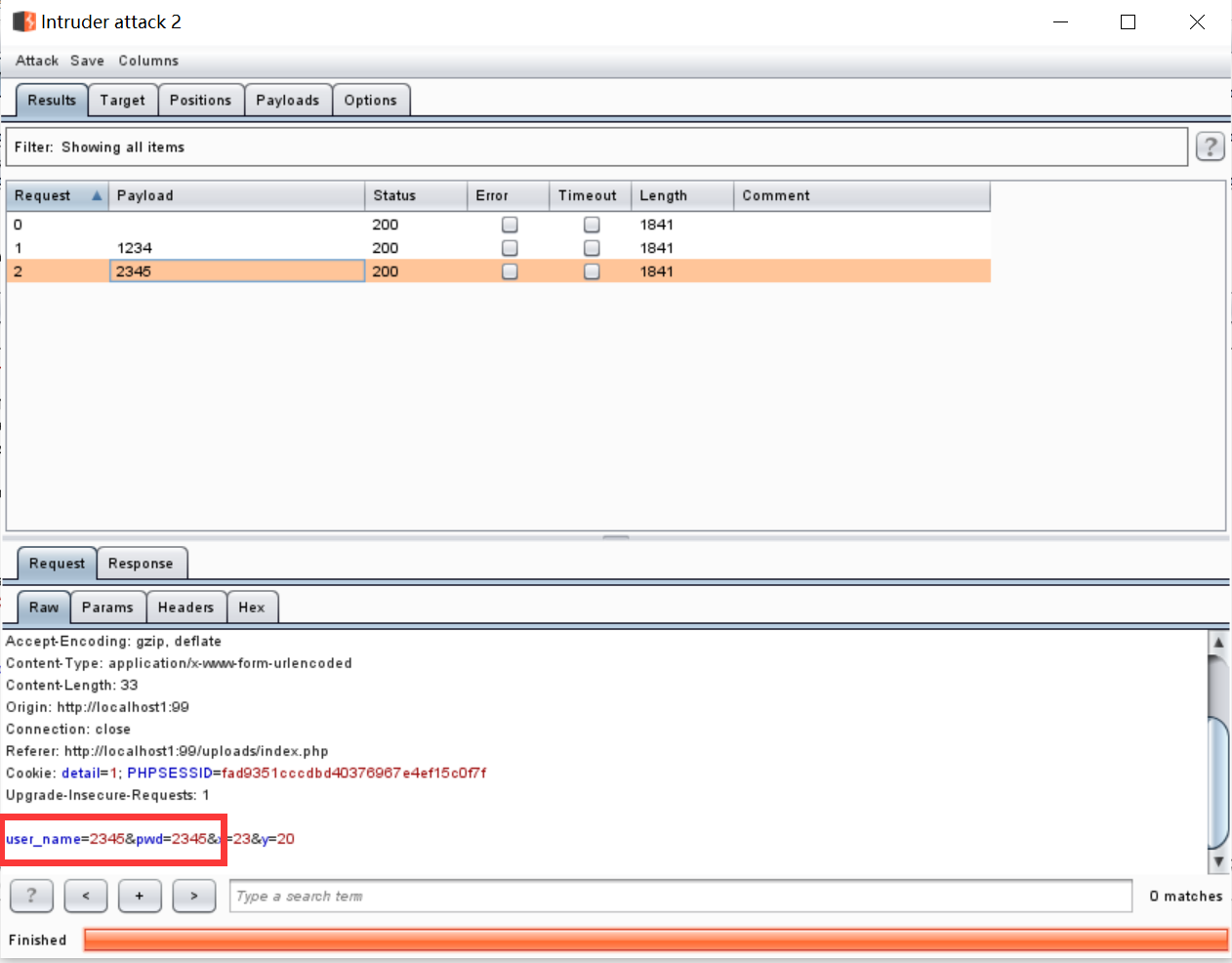
4.自动化攻击

（1）使用Intruder进行密码爆破

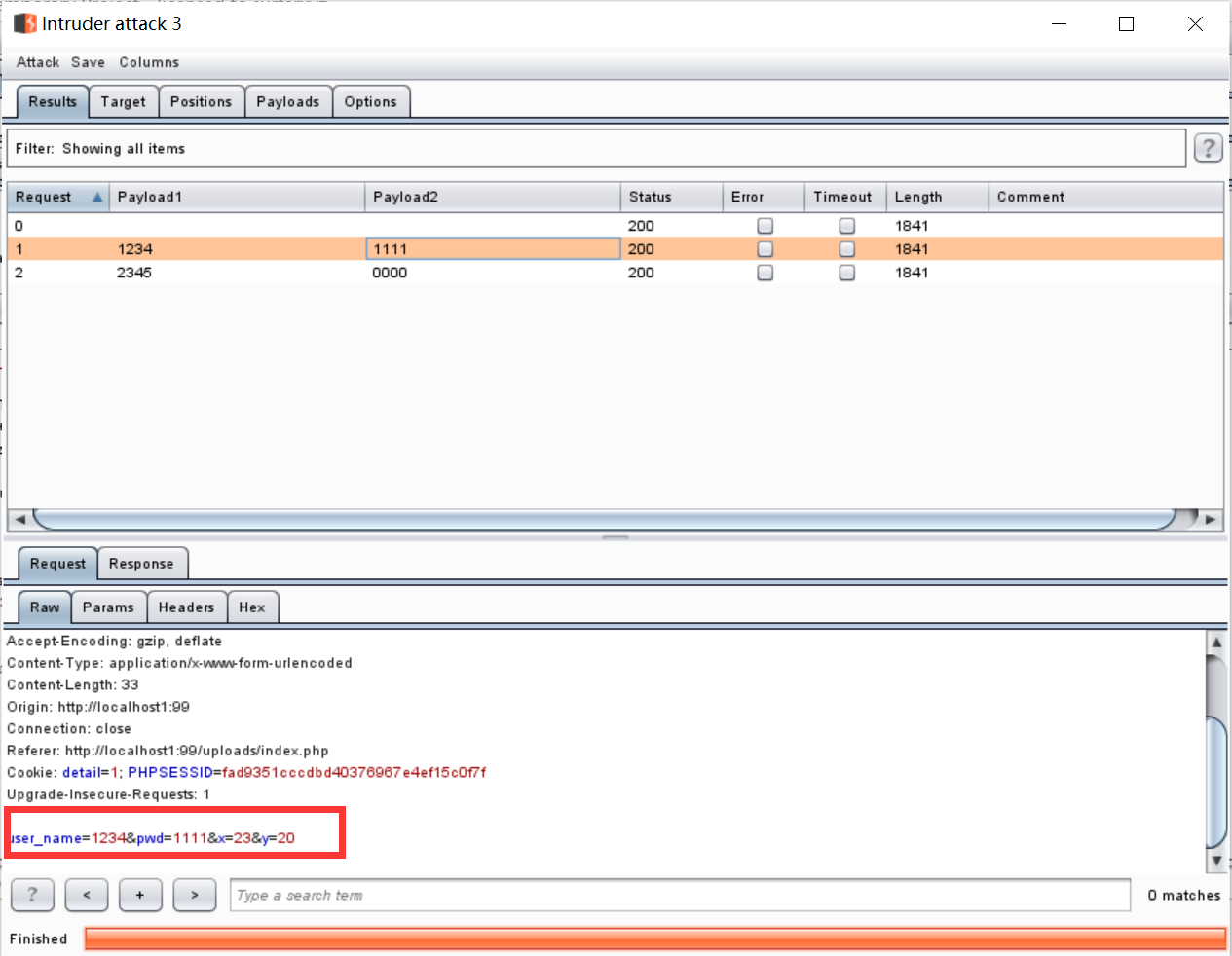
1. Sniper



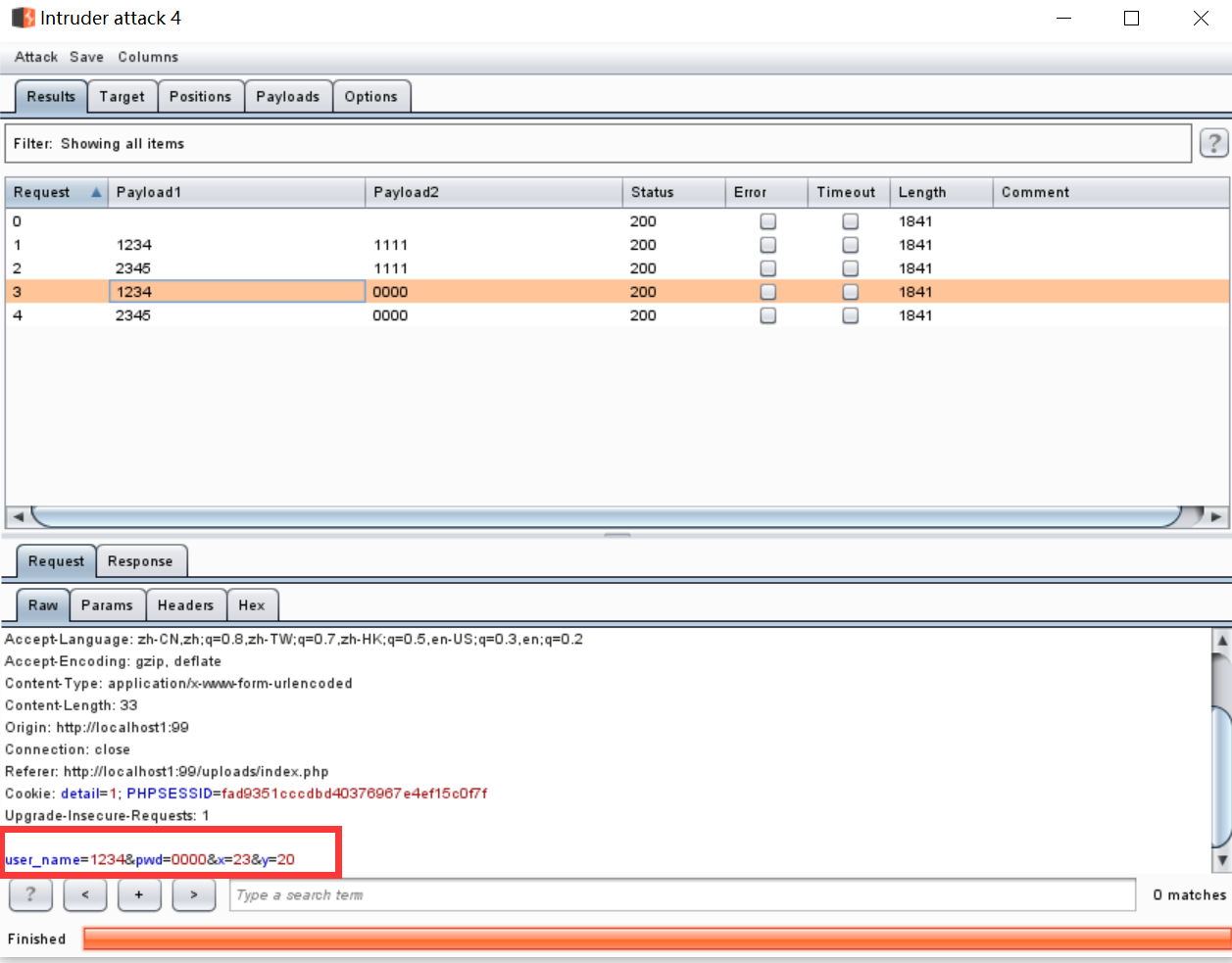
1. Battering ram



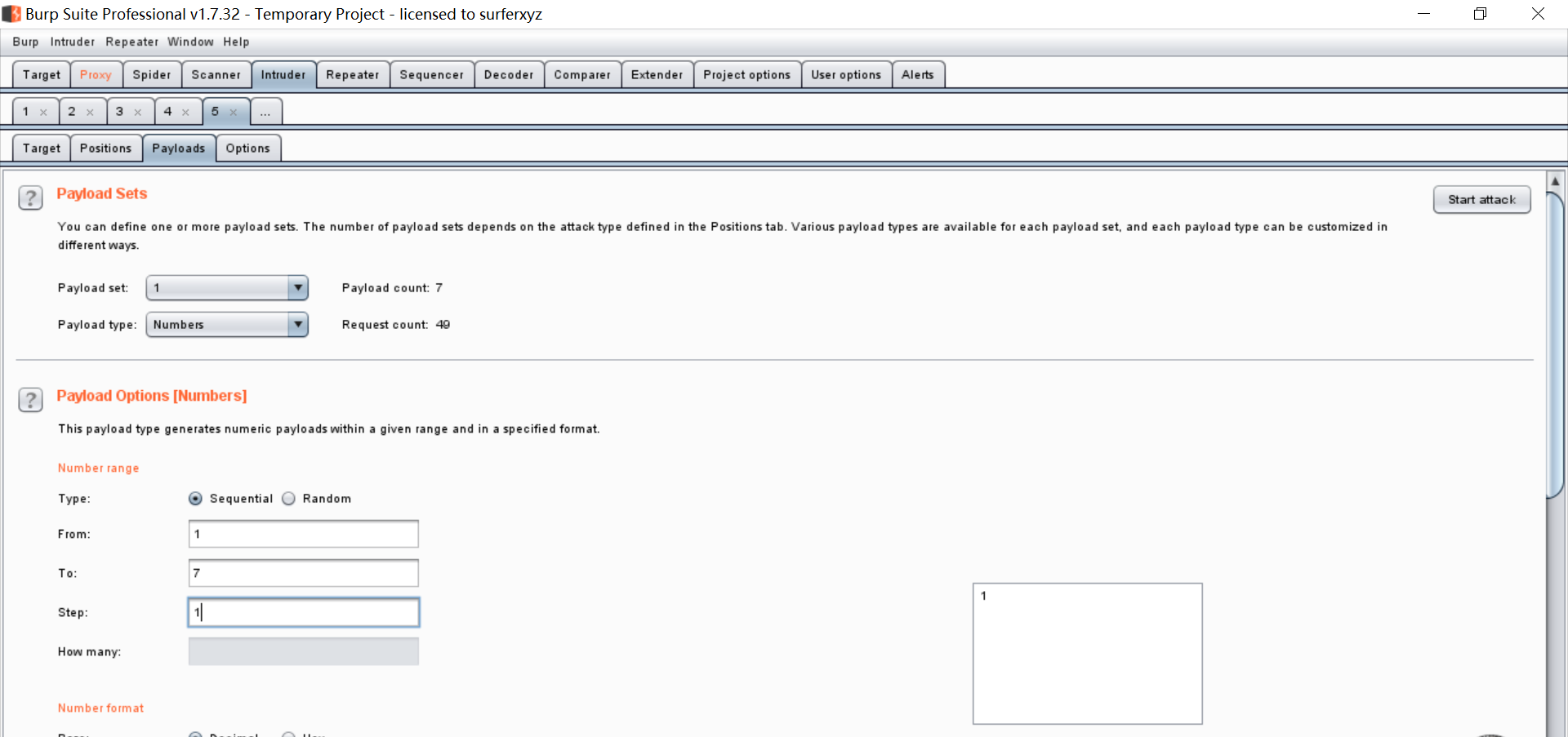
1. Pitchfork



1. Cluster bomb

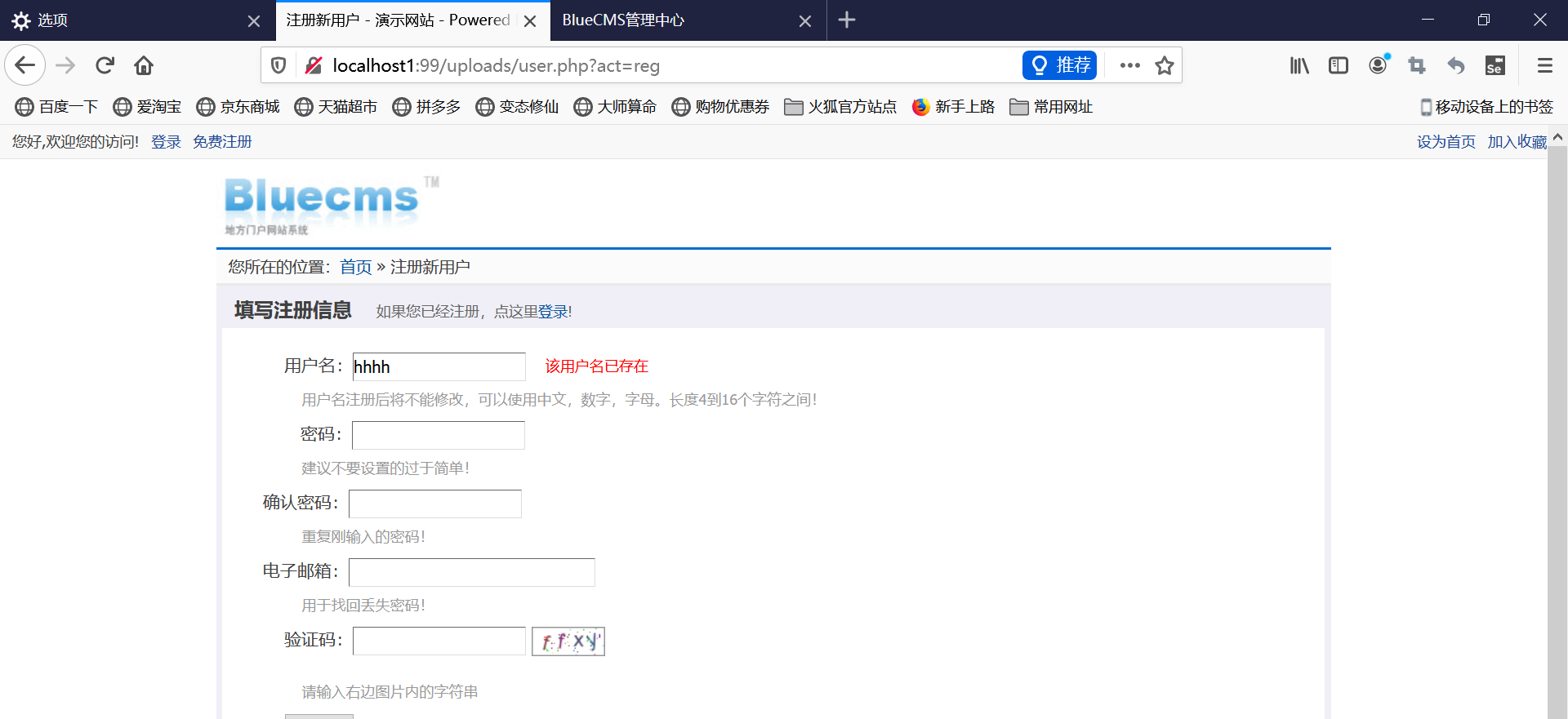


（2）使用Intruder进行sql注入

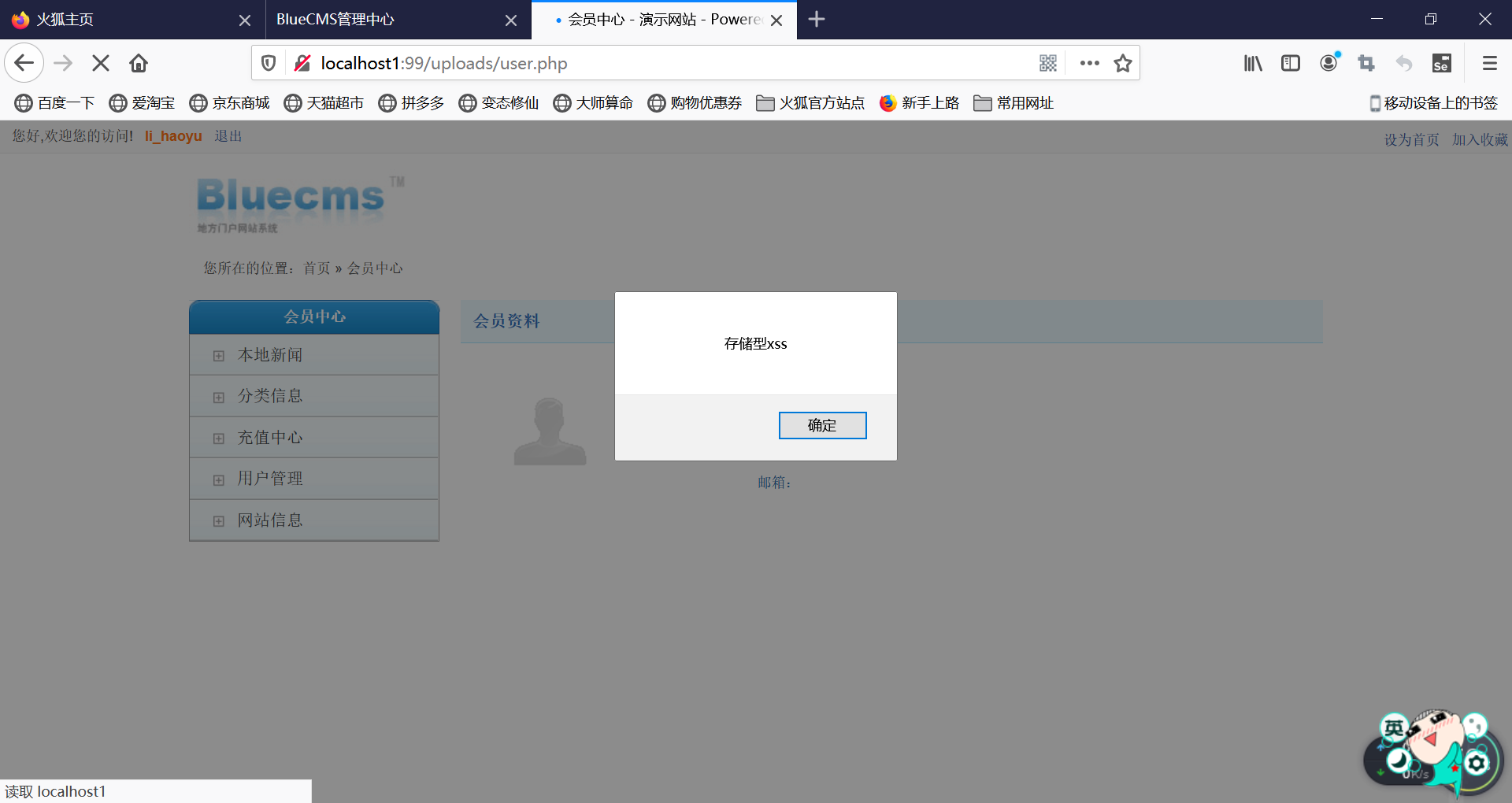


5.手工测试

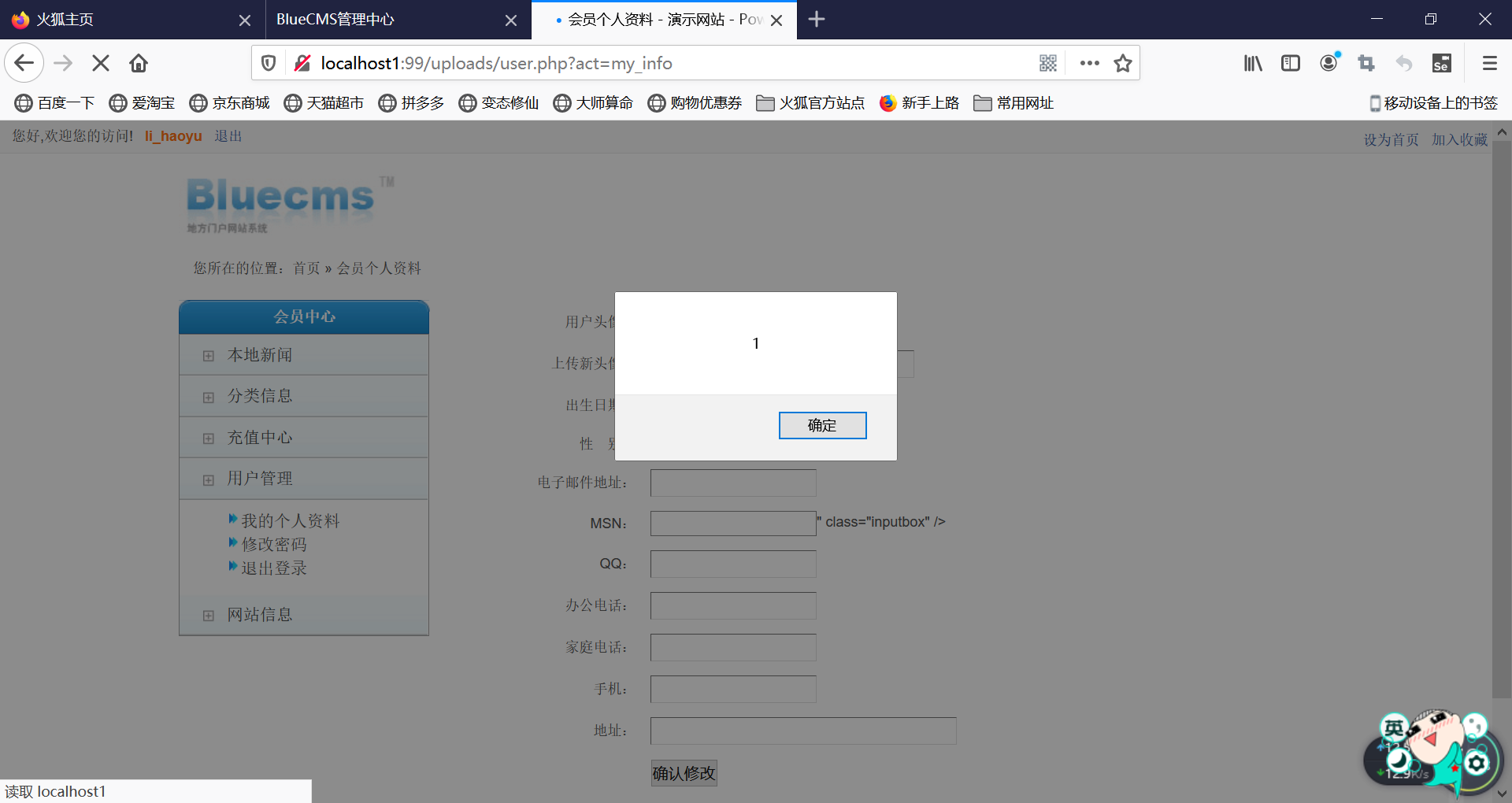
（1）注册时名字不区分大小写

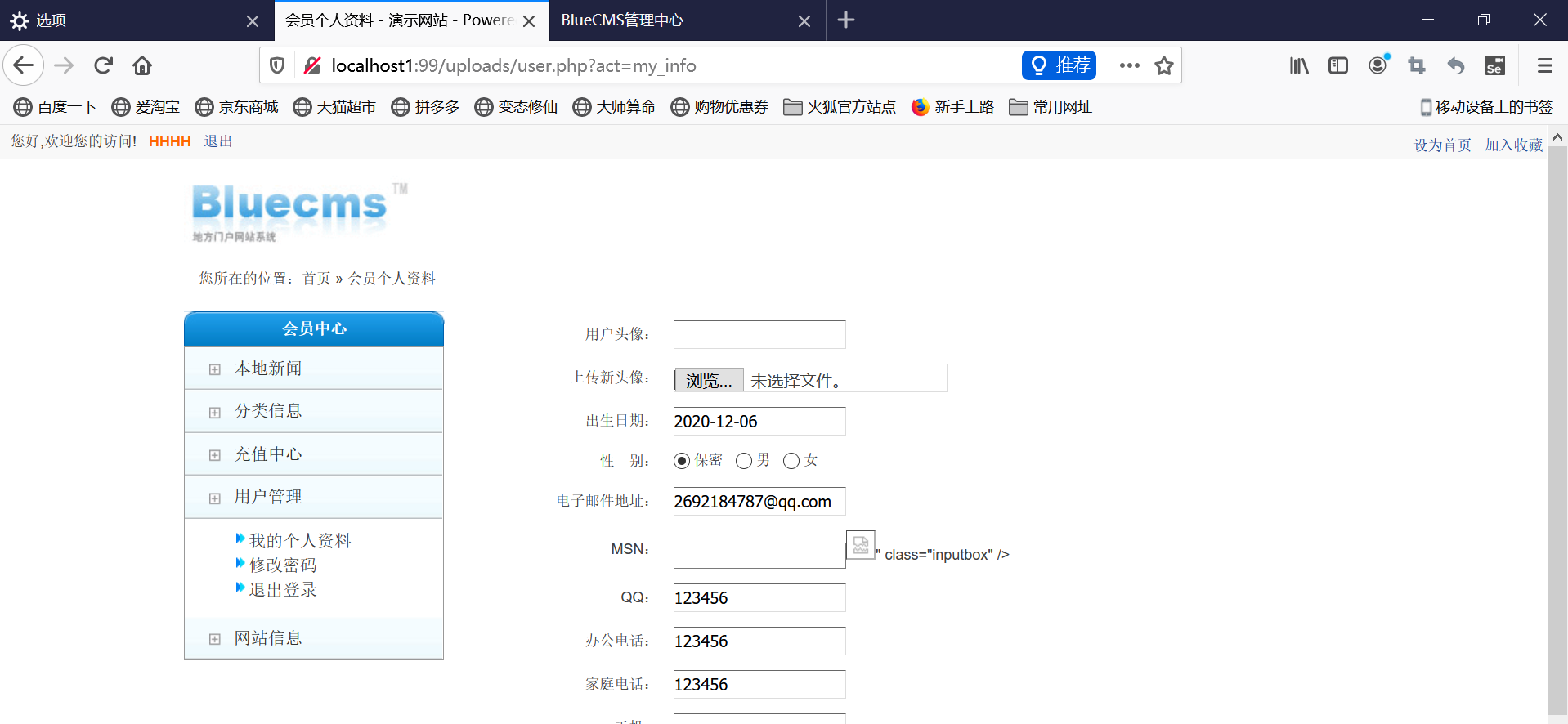
（2）在电子邮件地址中 输入<script>alert(“存储型xss”;)</script>，点击确认修改会出现弹框

（3）在MSN中插入"><img src=&apos;&apos; onerror=alert(1)>，更改成功后再次点击个人信息资料会出现弹框：

点击确定后MSN后会出现字符，点击检查元素时，网页代码中出现不该出现的代码

（4）新闻发布后，刷新页面新闻消失