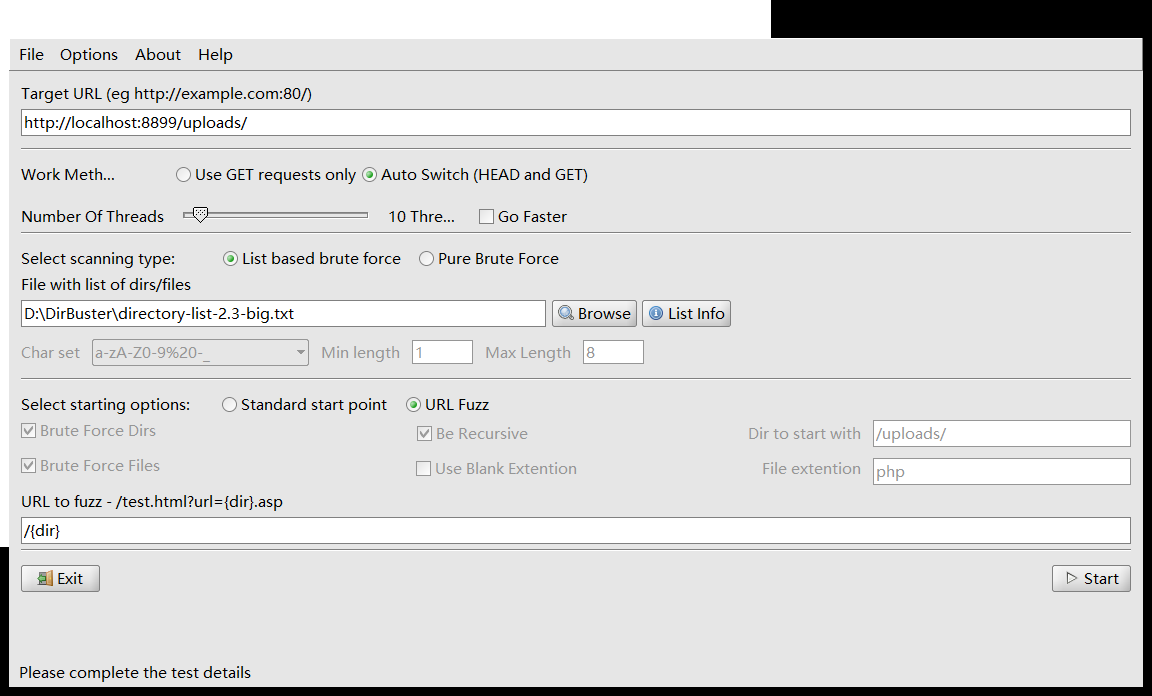
### 1、信息收集

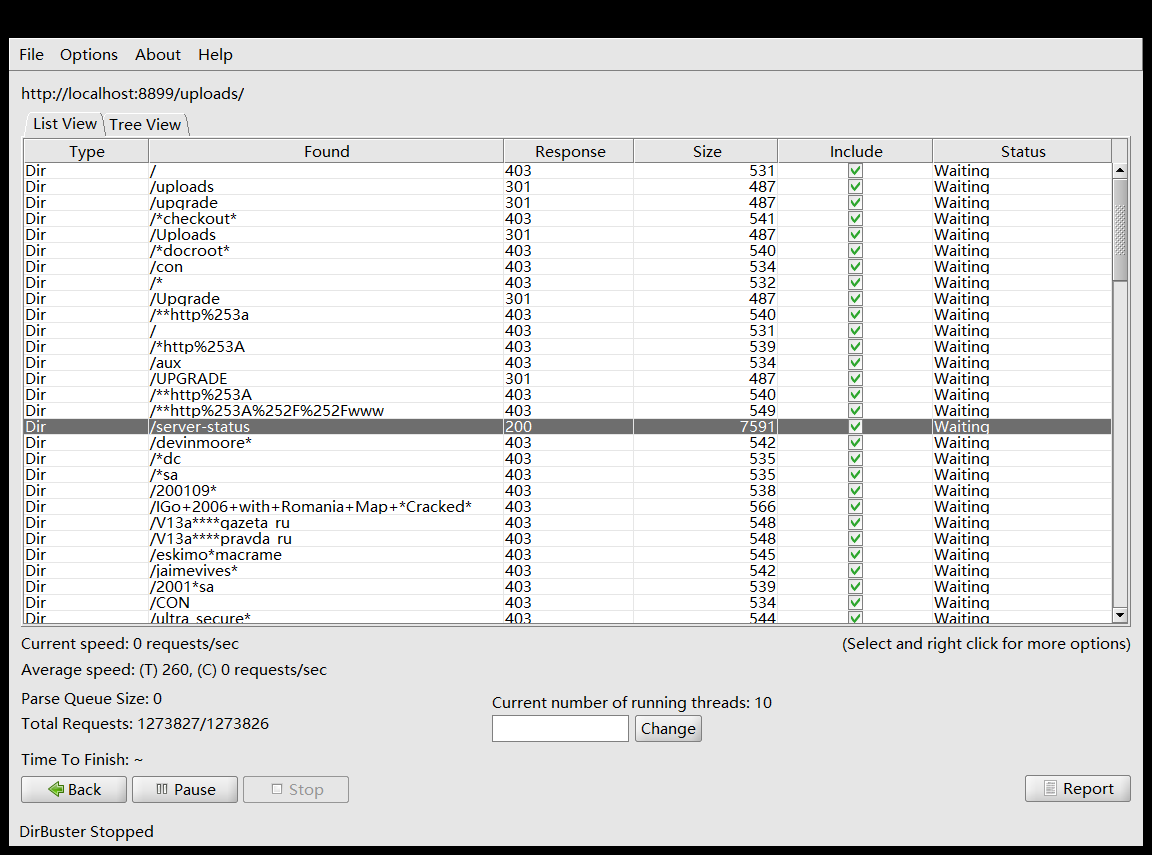
**1.1域名信息**

本地localhost

10.7.86.172

**1.2.使用DirBuster扫描敏感目录**

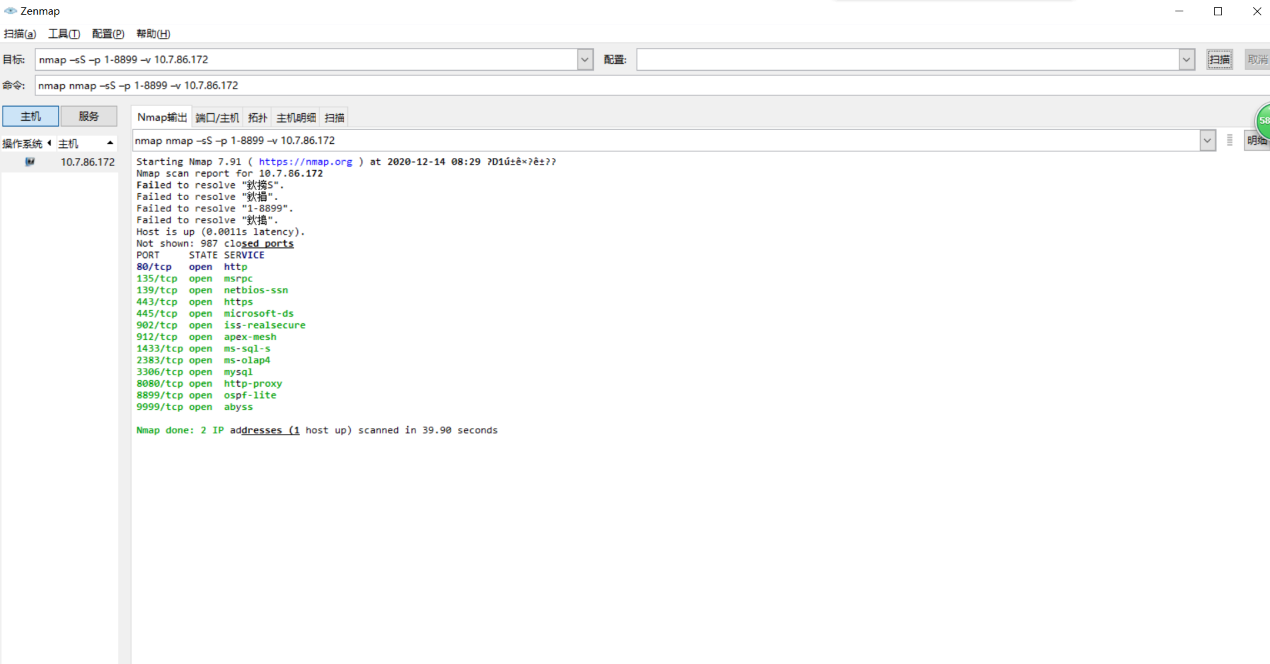




**1.3**.**端口扫描：**

**1.4.旁站C段：**

1.扫描指定ip所开放的端口：

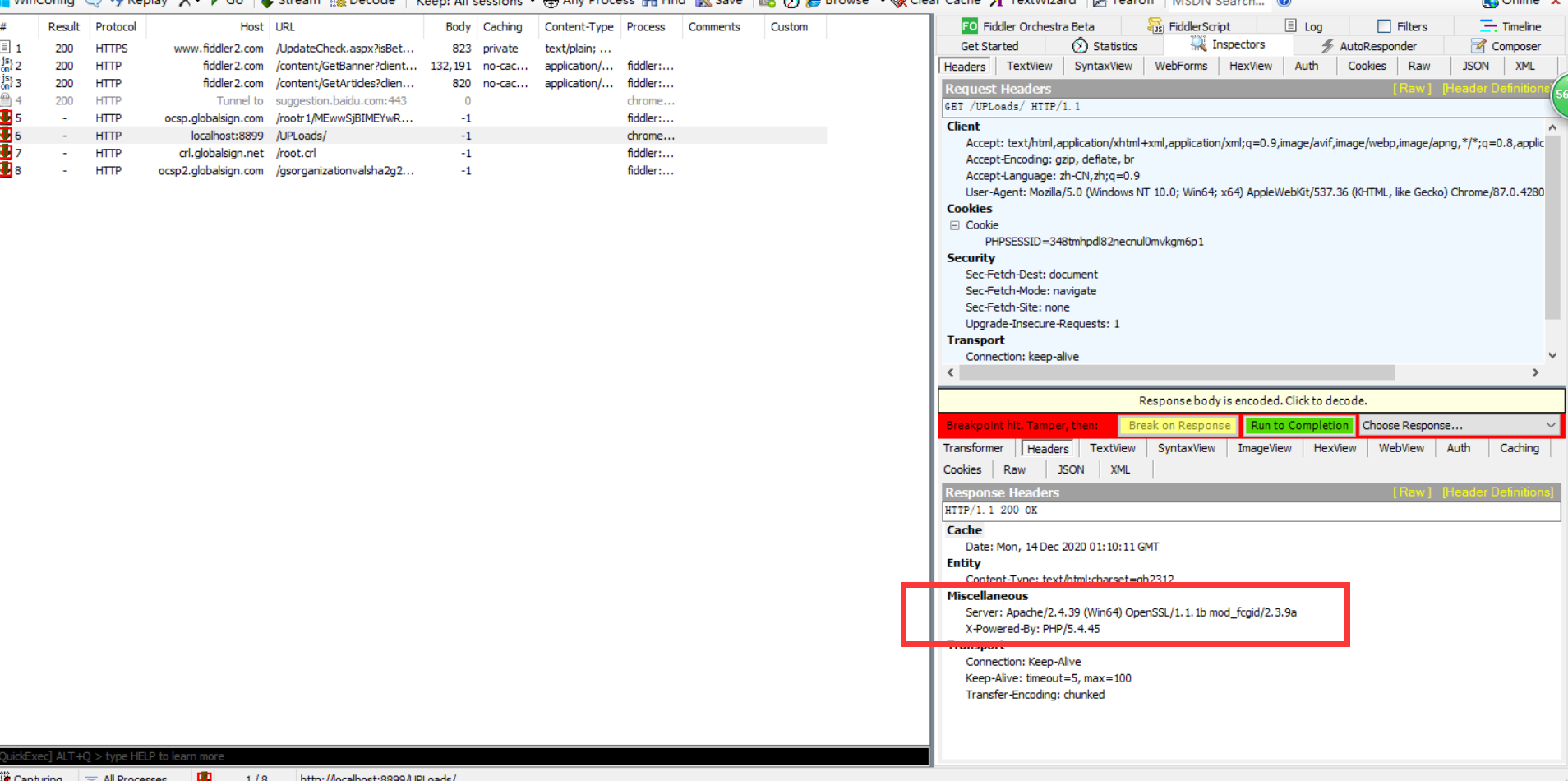


**1.5.整站分析：**

1.5.1服务器的操作系统：

URL中某些字母改为大写，仍能访问，则判断其是WINDOWS系统，如果不能，是linux系统，访问，<http://localhost:8899/UPLoads/>,仍然能够访问，所以是Windows系统

1.5.2网站容器：**Apache**

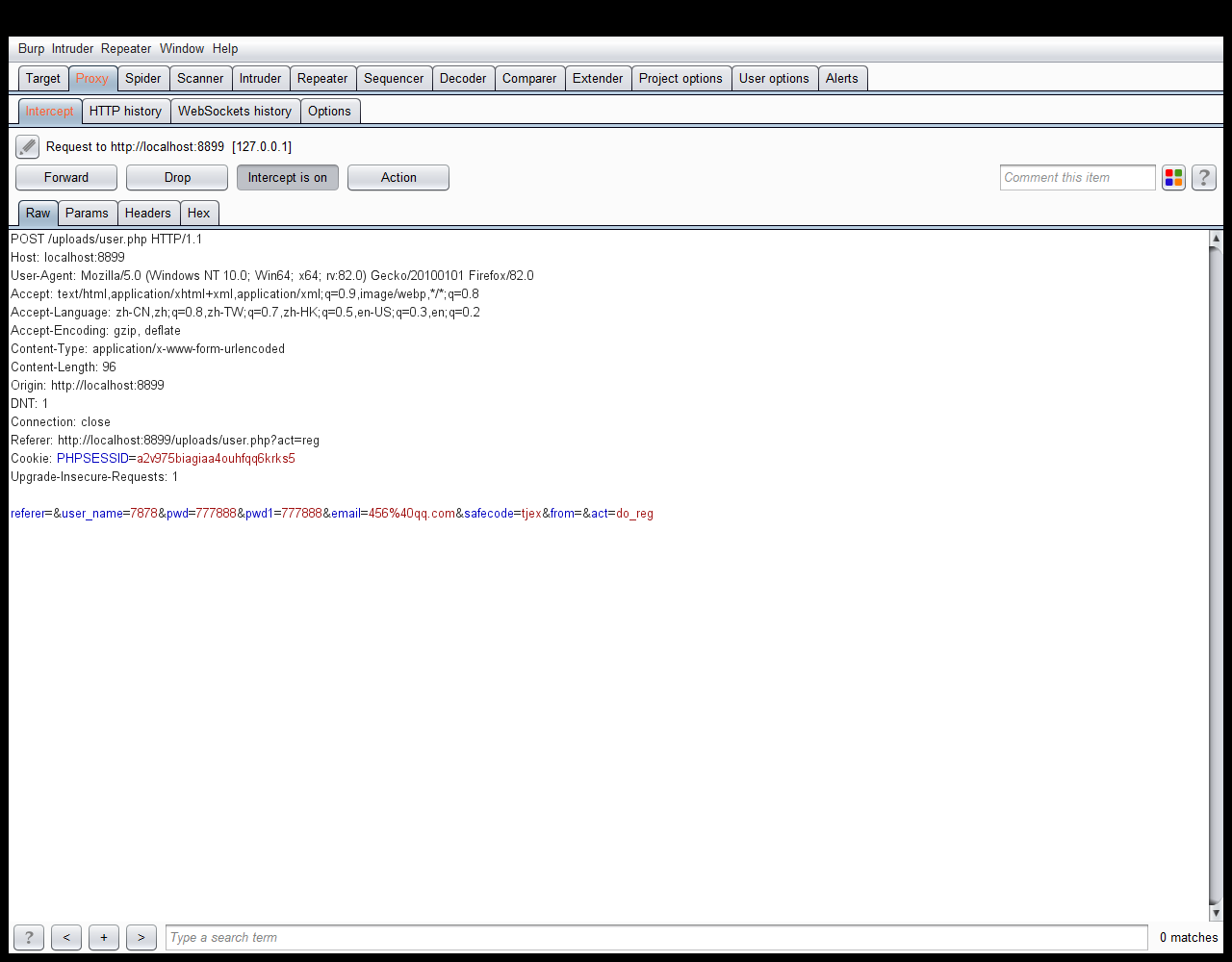


**1.5.3分析脚本类型为php**

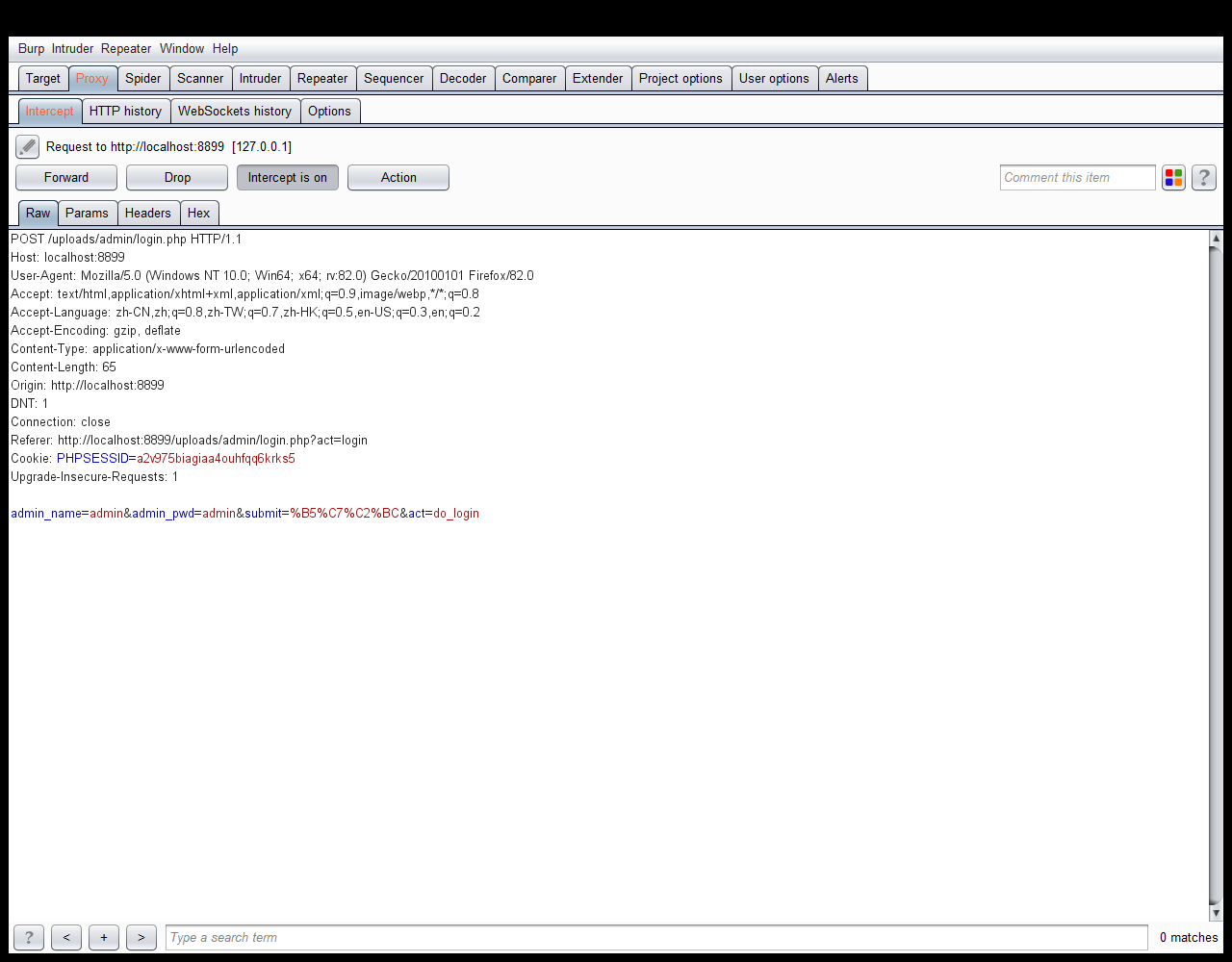
**1.5.4数据库：Mysql**

### 2、Burpsuit扫描前台和后台

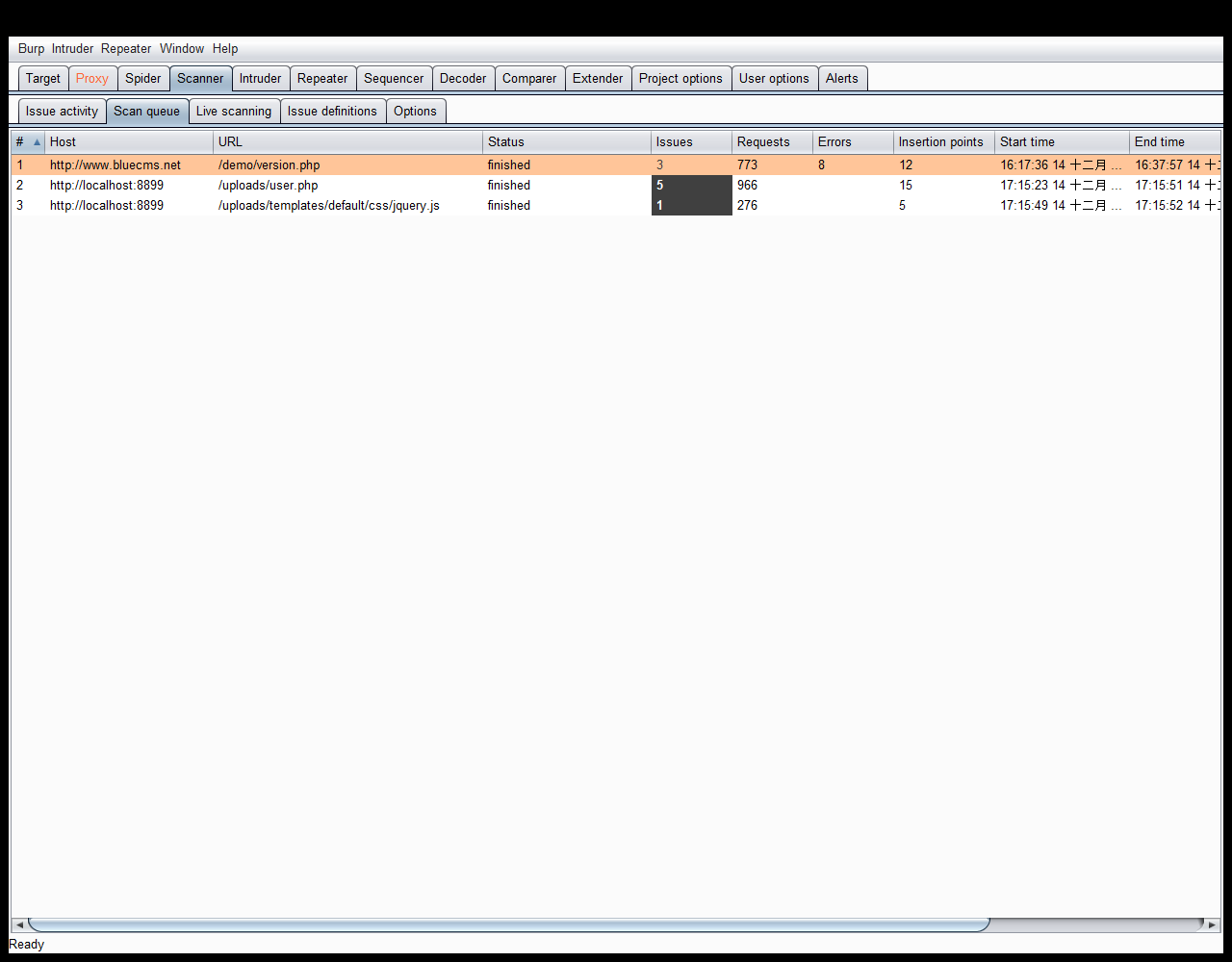
2.1扫描前台注册：



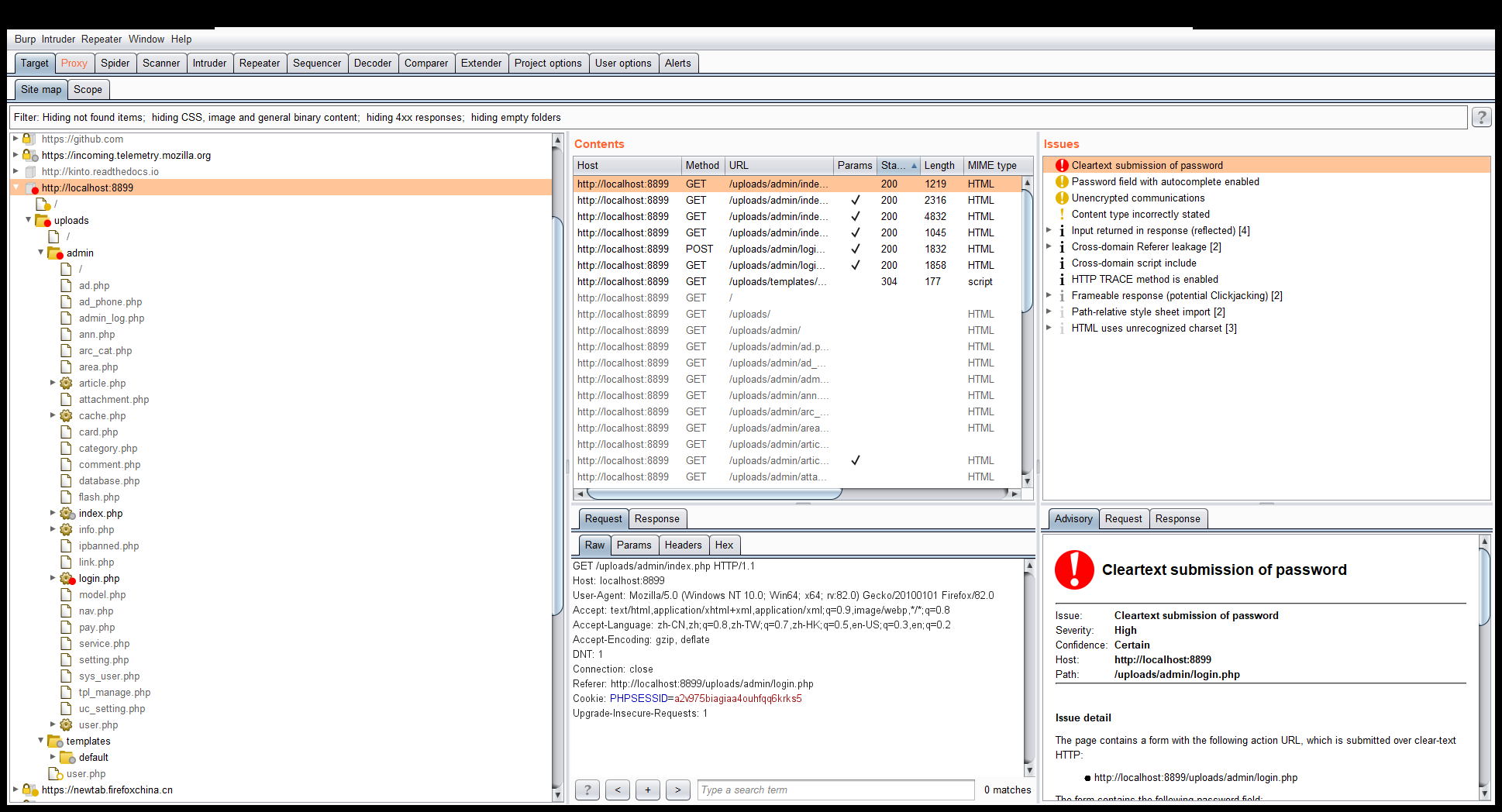
2.2扫描后台登录：



2.3扫描队列

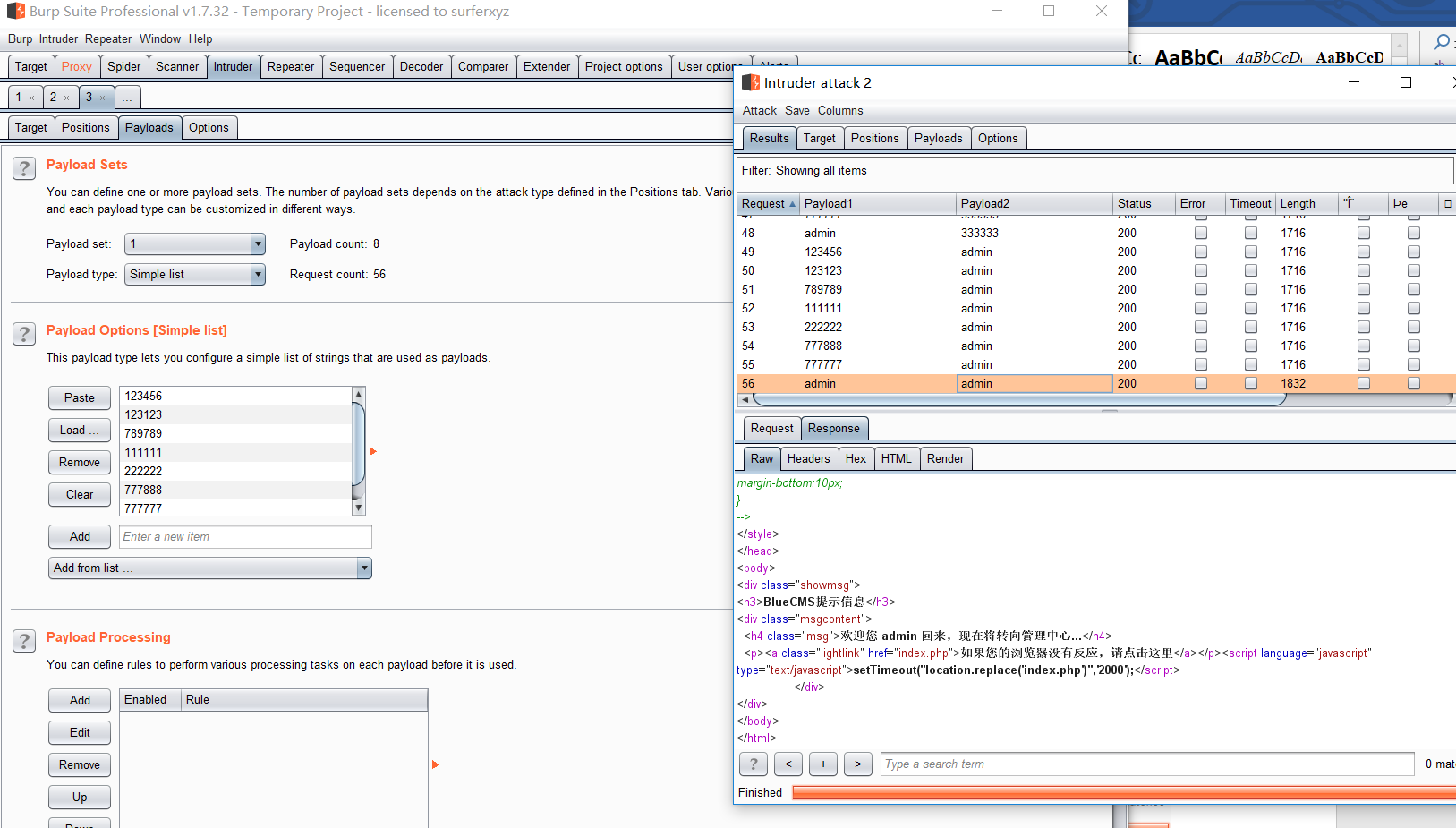


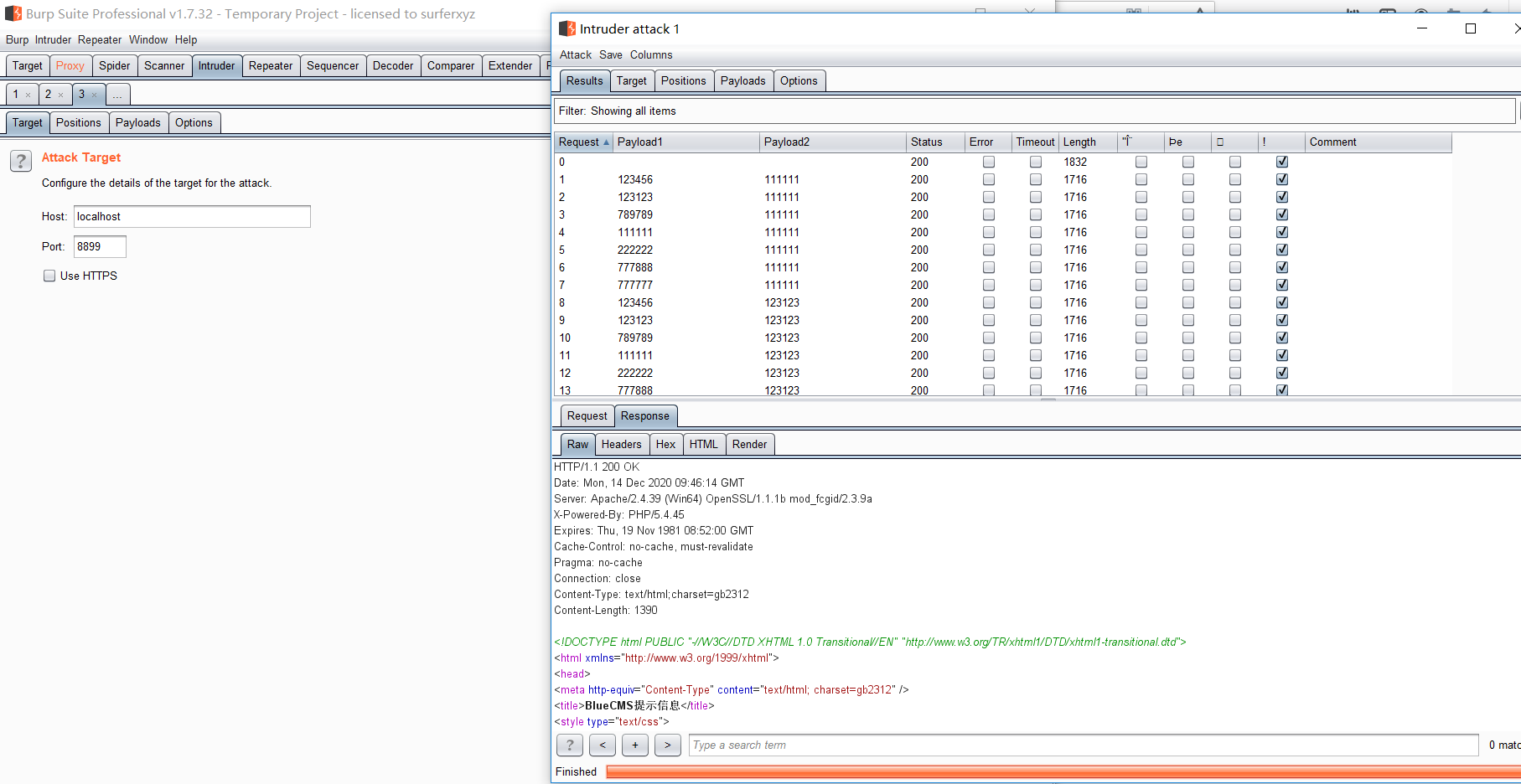
2.4爬取网站



# 3.自动化攻击

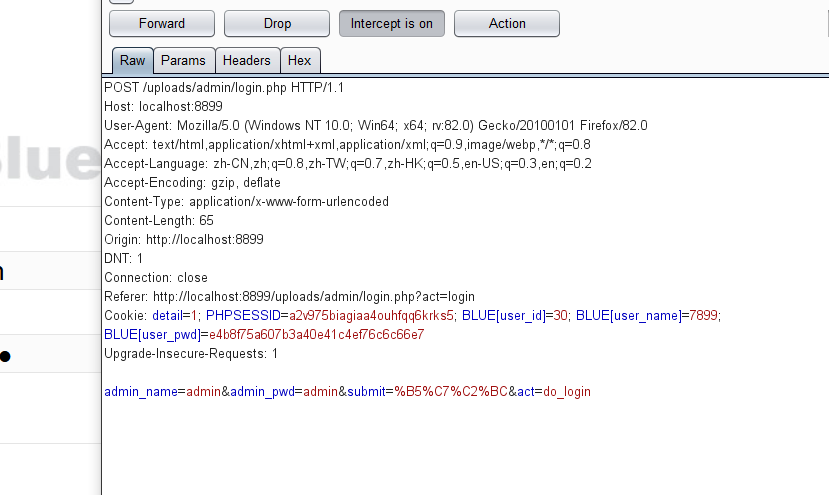
3.1暴力破解





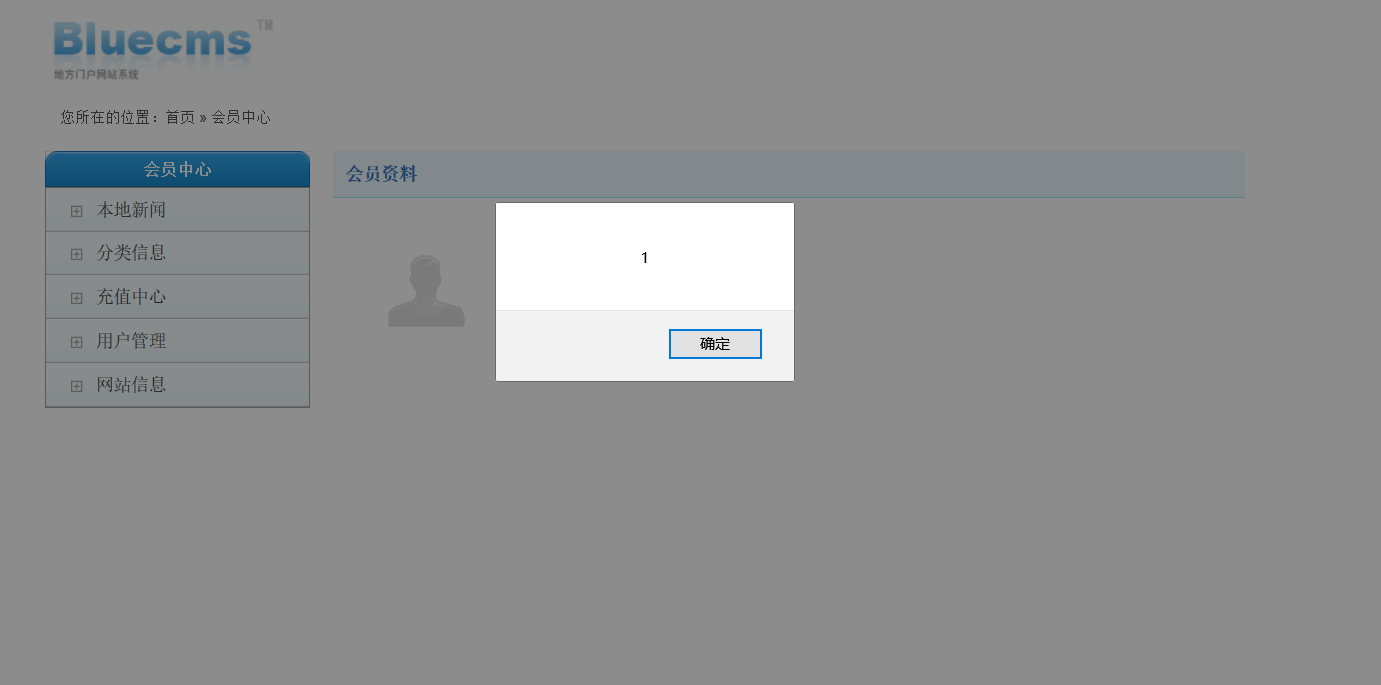
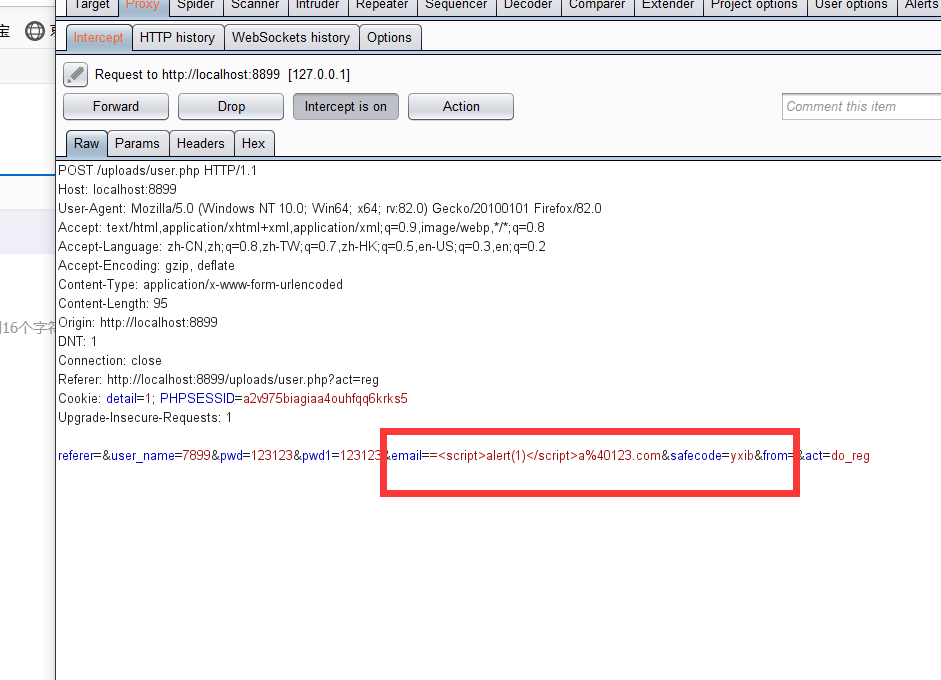
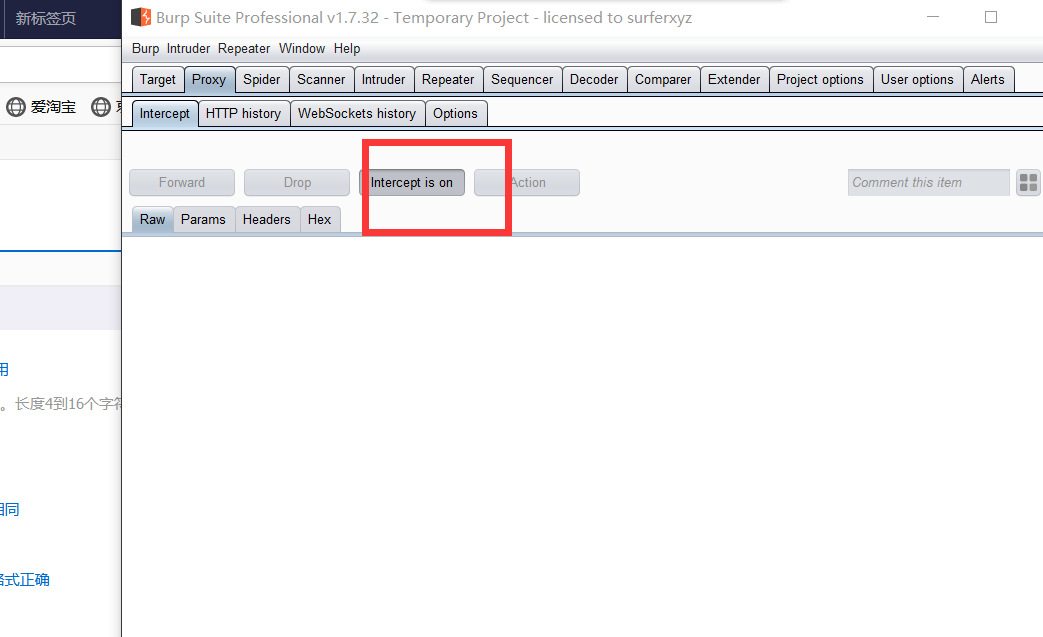
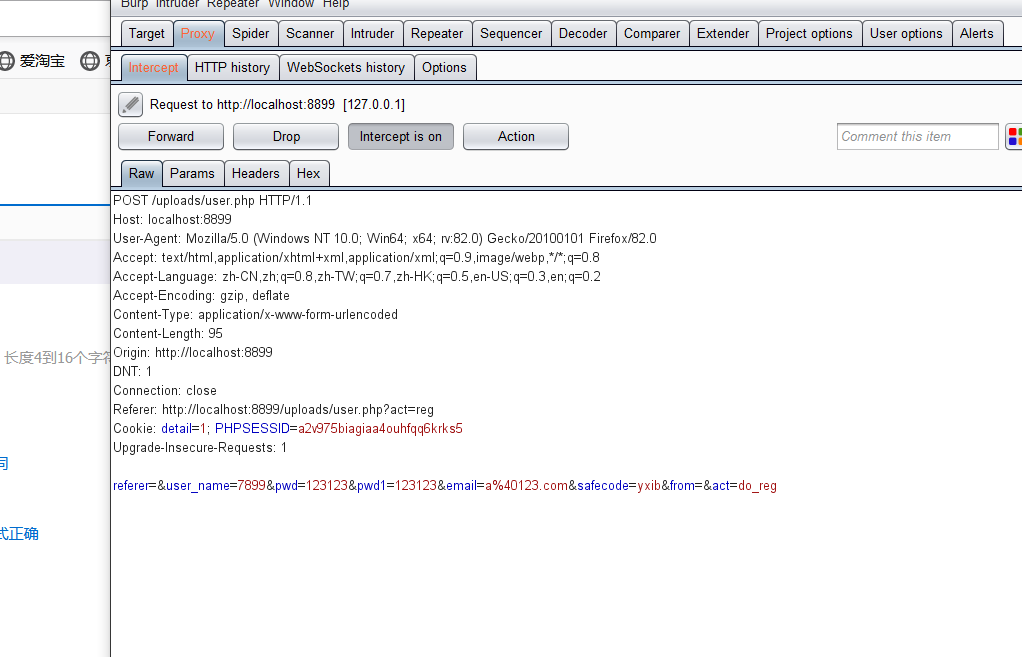
# 4.手工测试

4.1明文传输

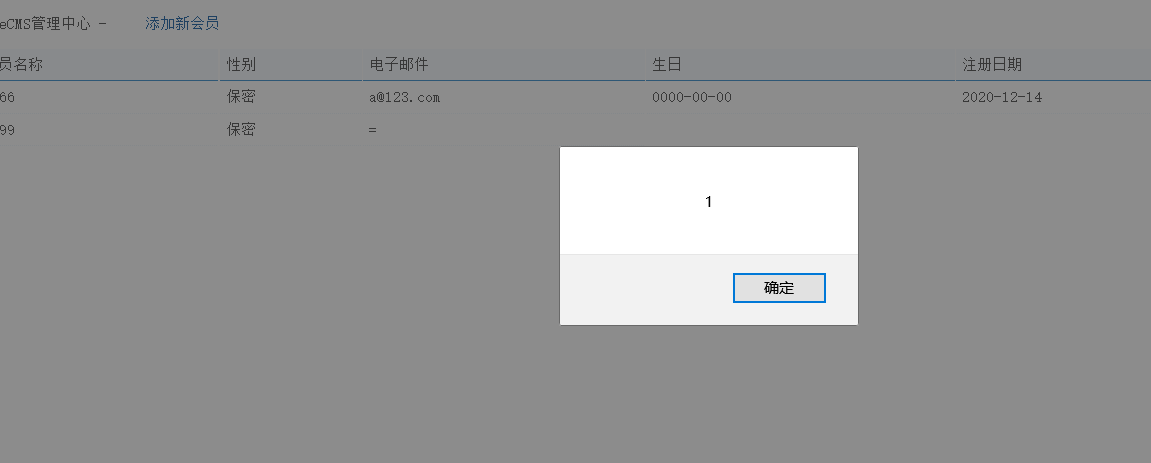


4.2xss漏洞

4.2.1前台注册邮箱拦截并修改加入语句



4.2.2 在后台管理添加会员，也会出现弹窗，漏洞为存储型漏洞



4.3登录界面的CSRF攻击

