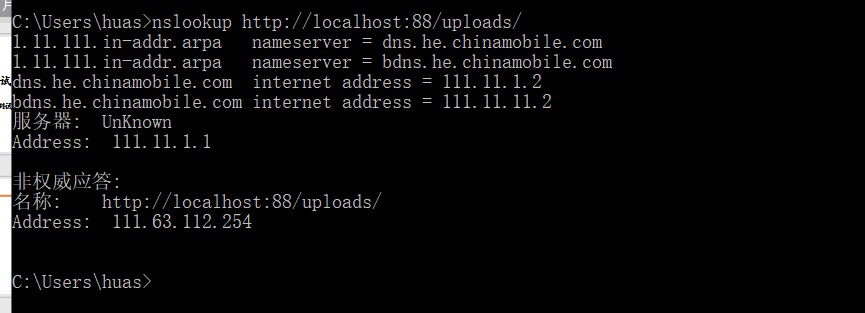
一．信息搜集：

1.域名信息：

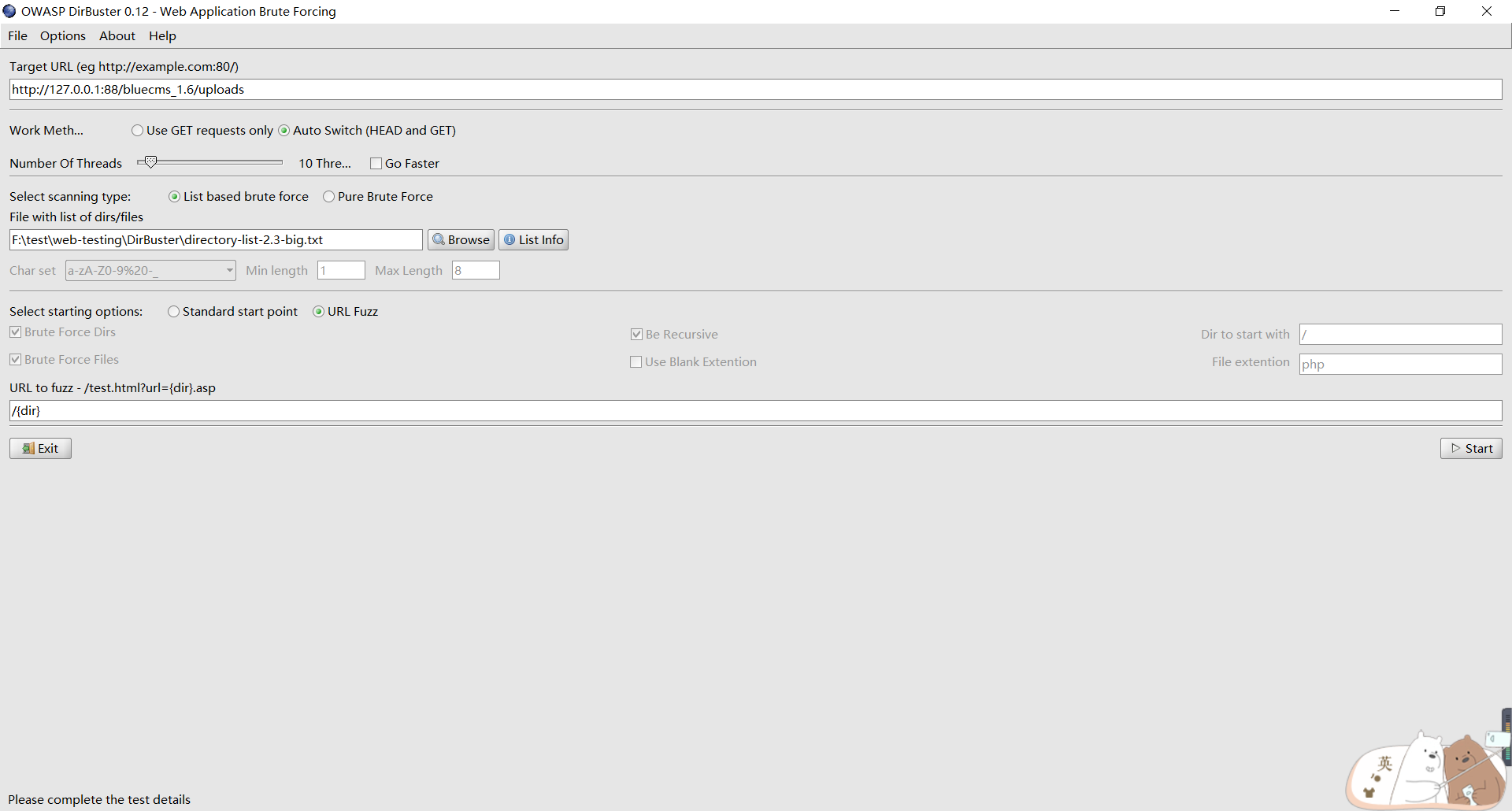
IP地址：

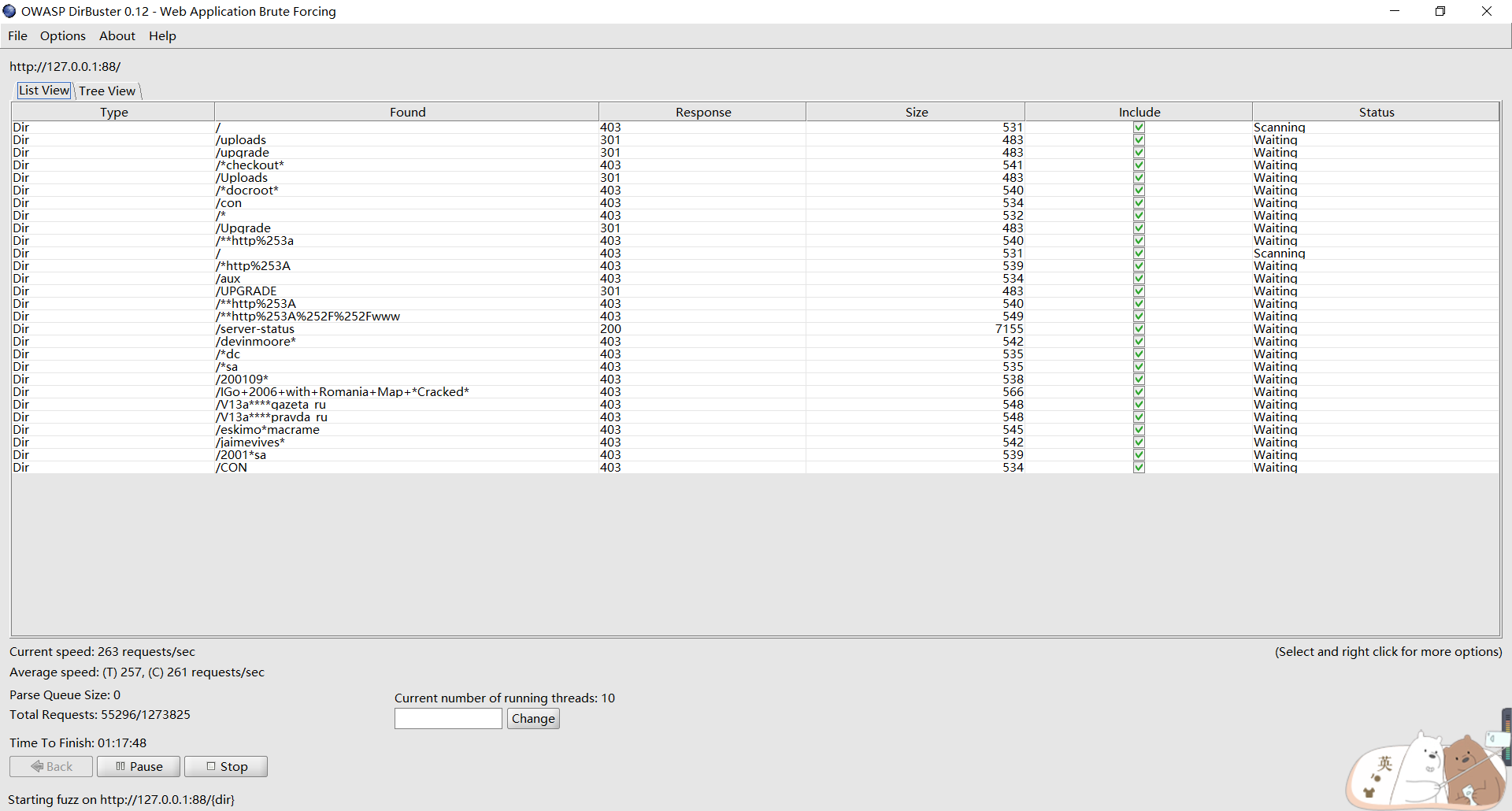




1. 敏感目录

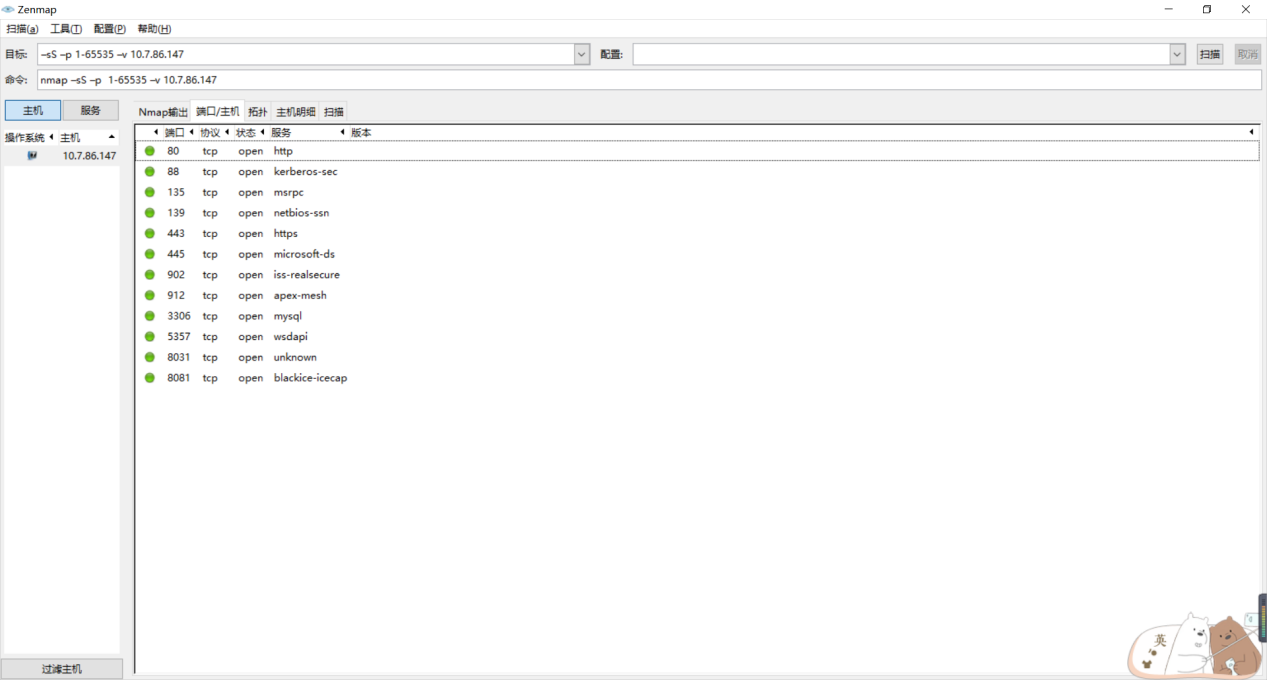
使用工具DirBuster





1. 端口扫描

使用工具Nmap



1. 整站分析

服务器的操作系统：Windows系统，url中某些字母改为大写，仍然能访问

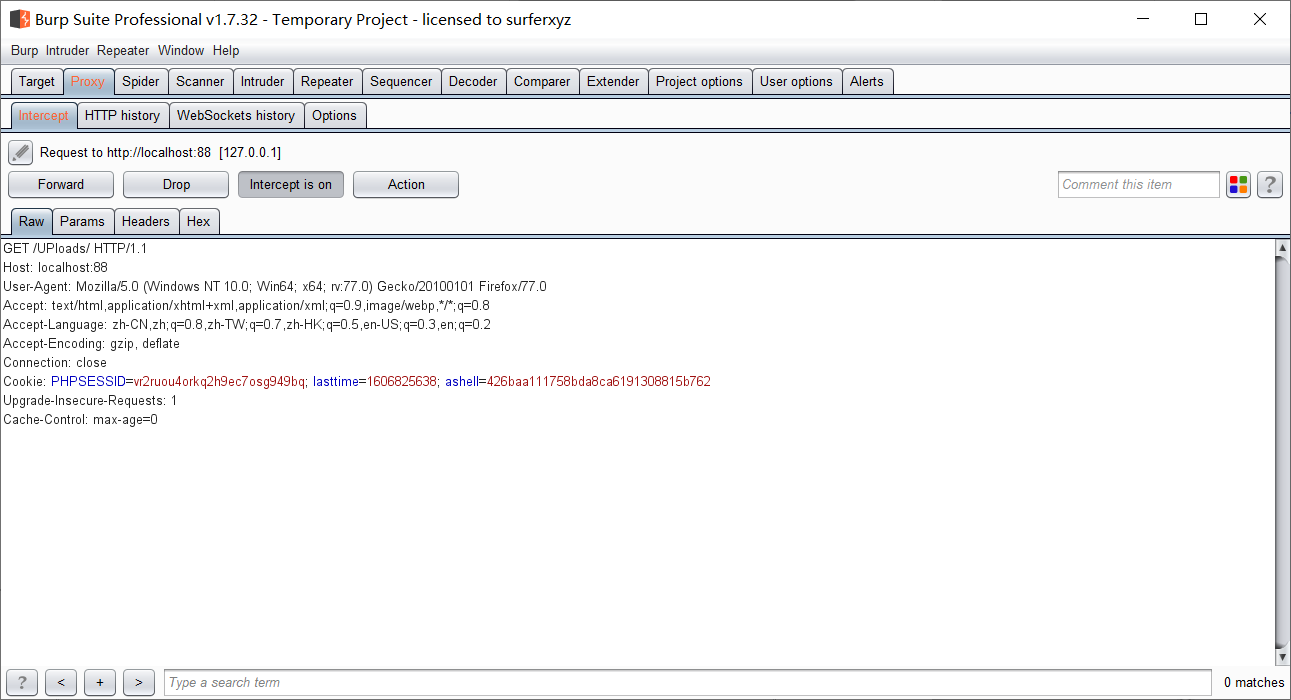
网站容器：Apache

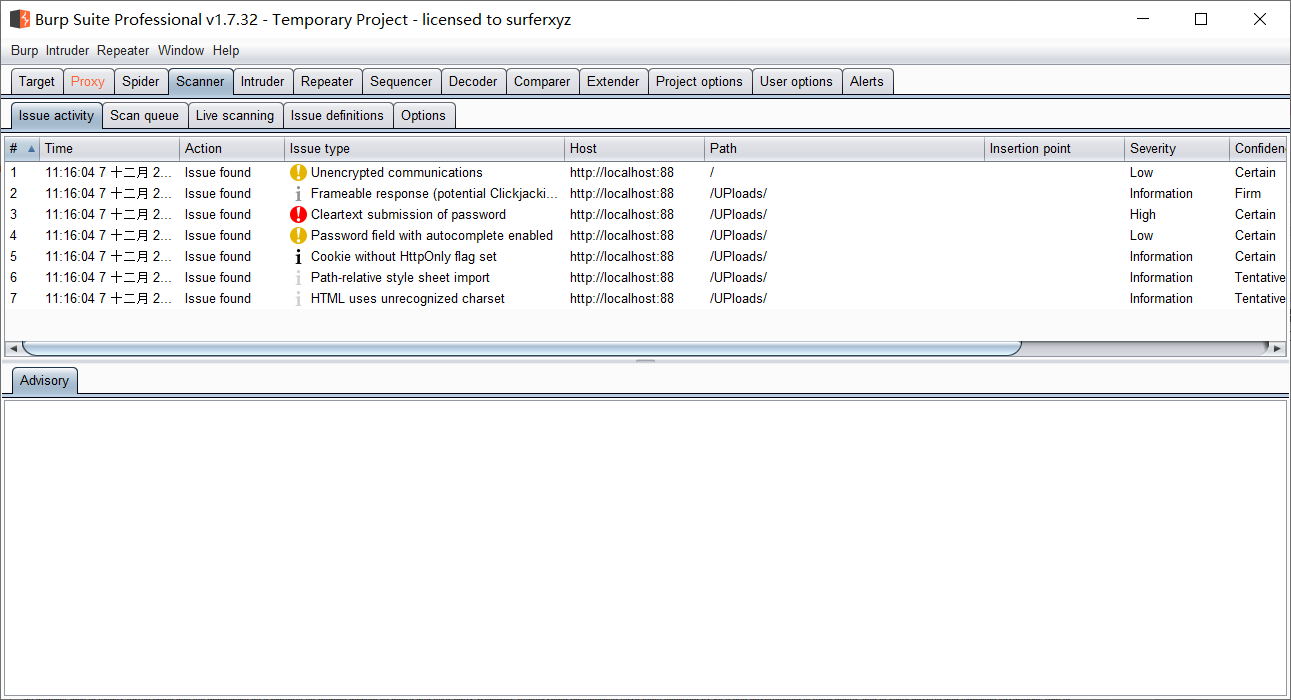
脚本类型：php，url后加 /index.php

数据库类型：Mysql，默认端口3306

1. 漏洞扫描（使用BurpSuite工具）

前台：http://localhost:88/uploads/





1. Unencrypted communications：未加密的通信

2.Frameable response (potential Clickjacking):框架响应(潜在点击劫持）

3.Cleartext submission of password：密码的明文提交

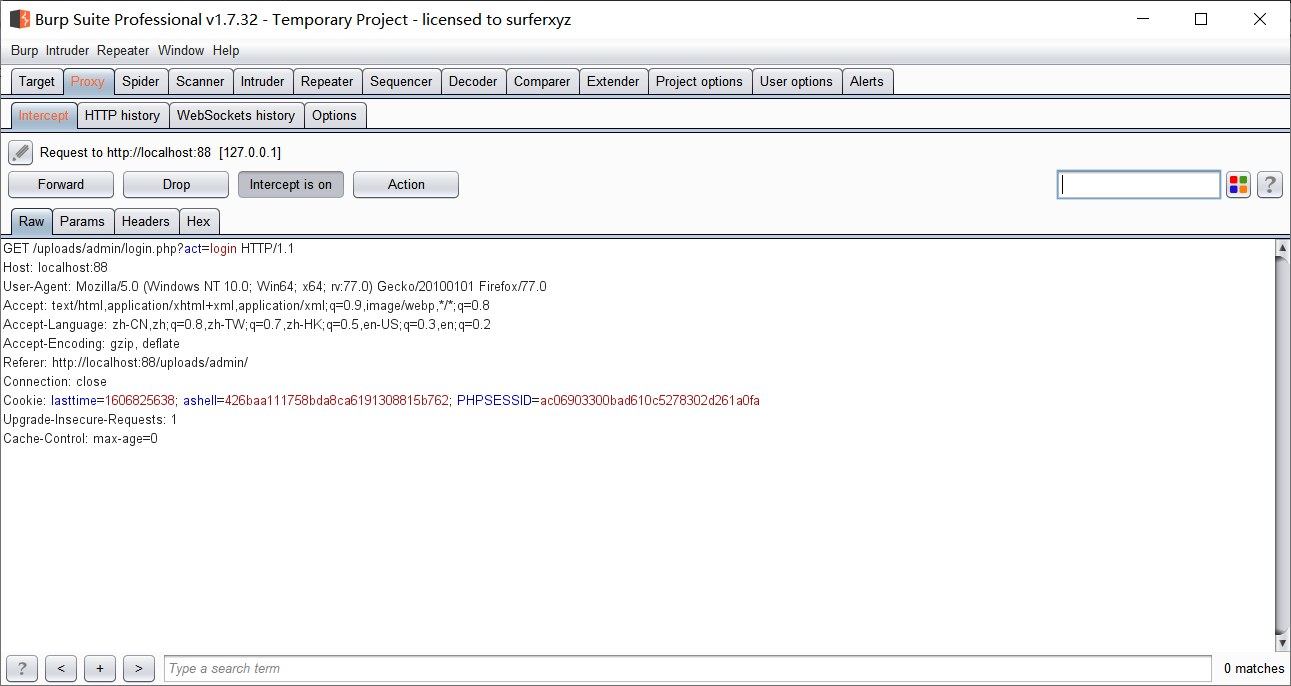
4.Password field with autocomplete enabled：启用自动完成的密码字段

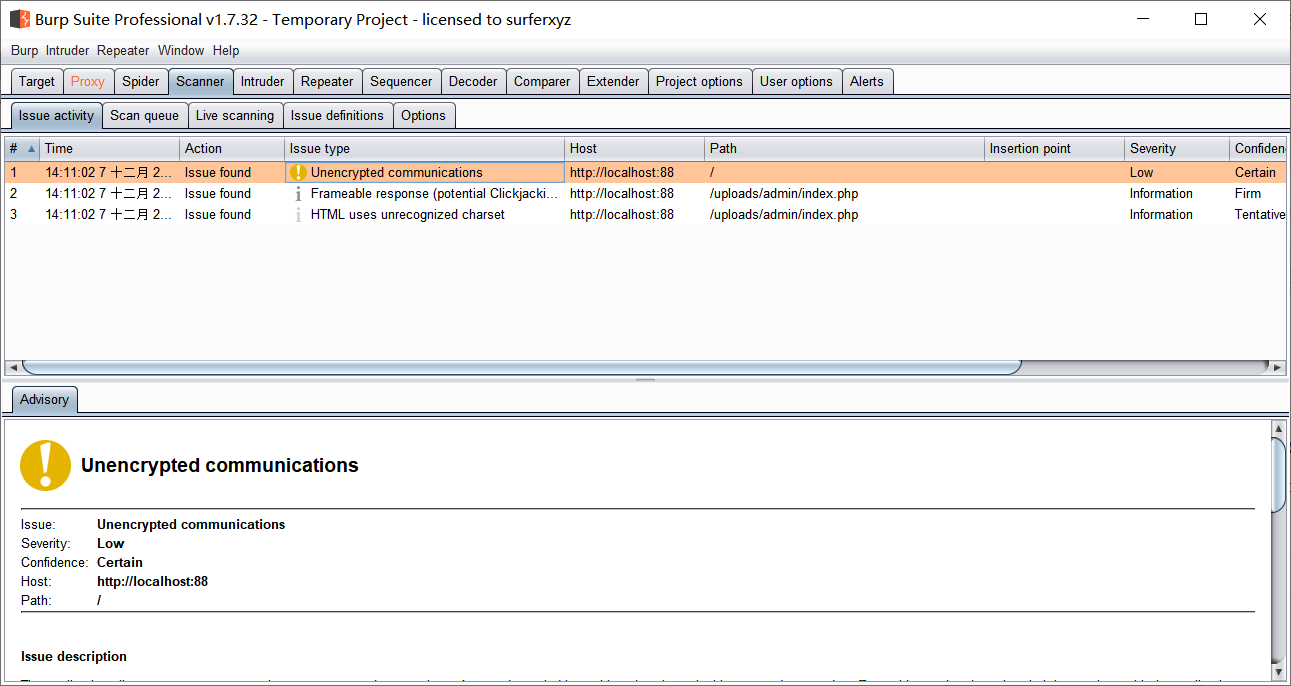
5.Cookie without HttpOnly flag set：没有设置HttpOnly标志的Cookie

6.Path-relative style sheet import：路径相关的样式表导入

7.HTML uses unrecognized charset：HTML使用无法识别的字符集

后台：http://localhost:88/uploads/admin





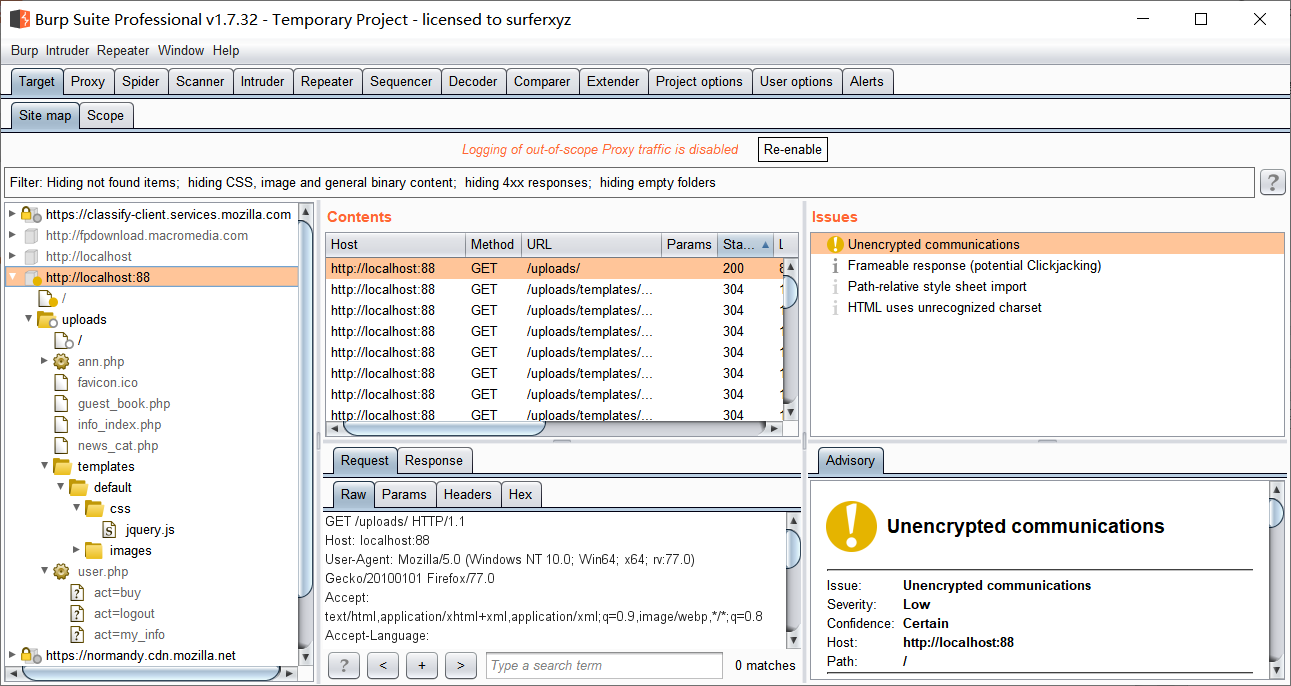
1. Unencrypted communications：未加密的通信

2.Frameable response (potential Clickjacking)：框架响应(潜在点击劫持)

3.HTML uses unrecognized charset：HTML使用无法识别的字符集

1. 爬取网站

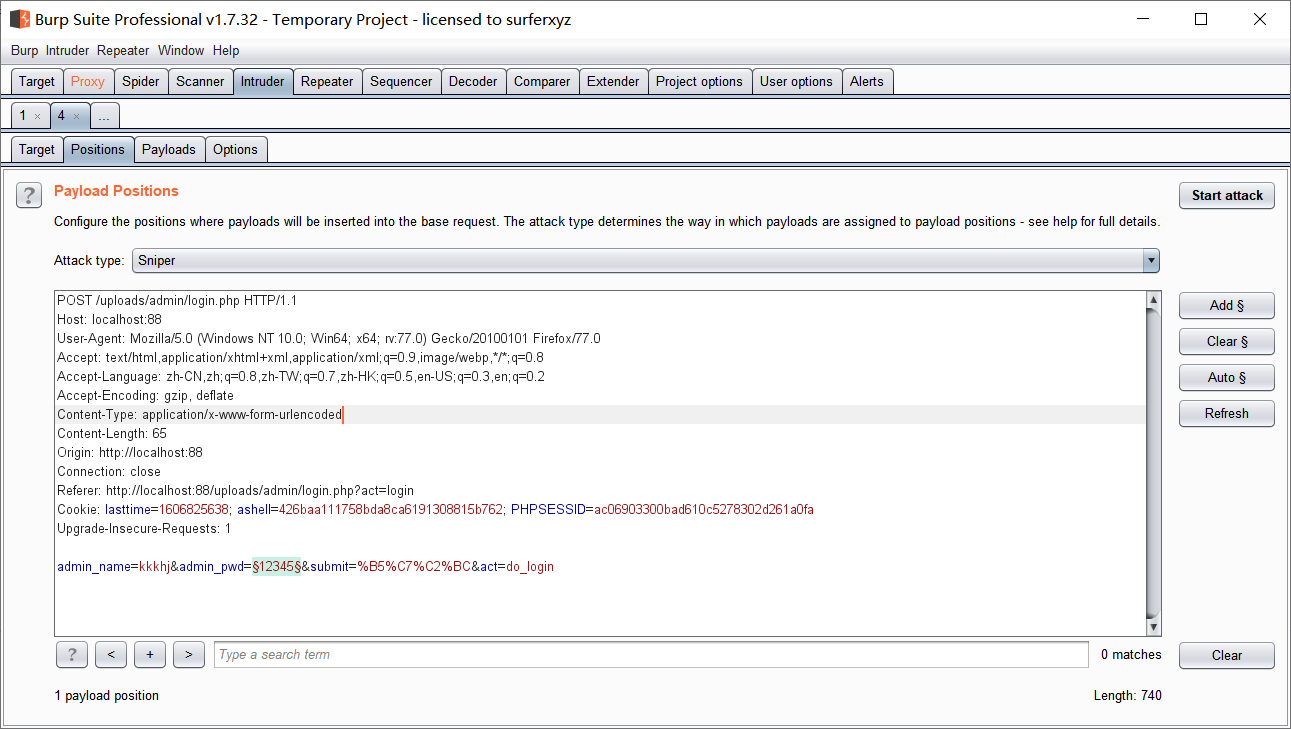
站点信息

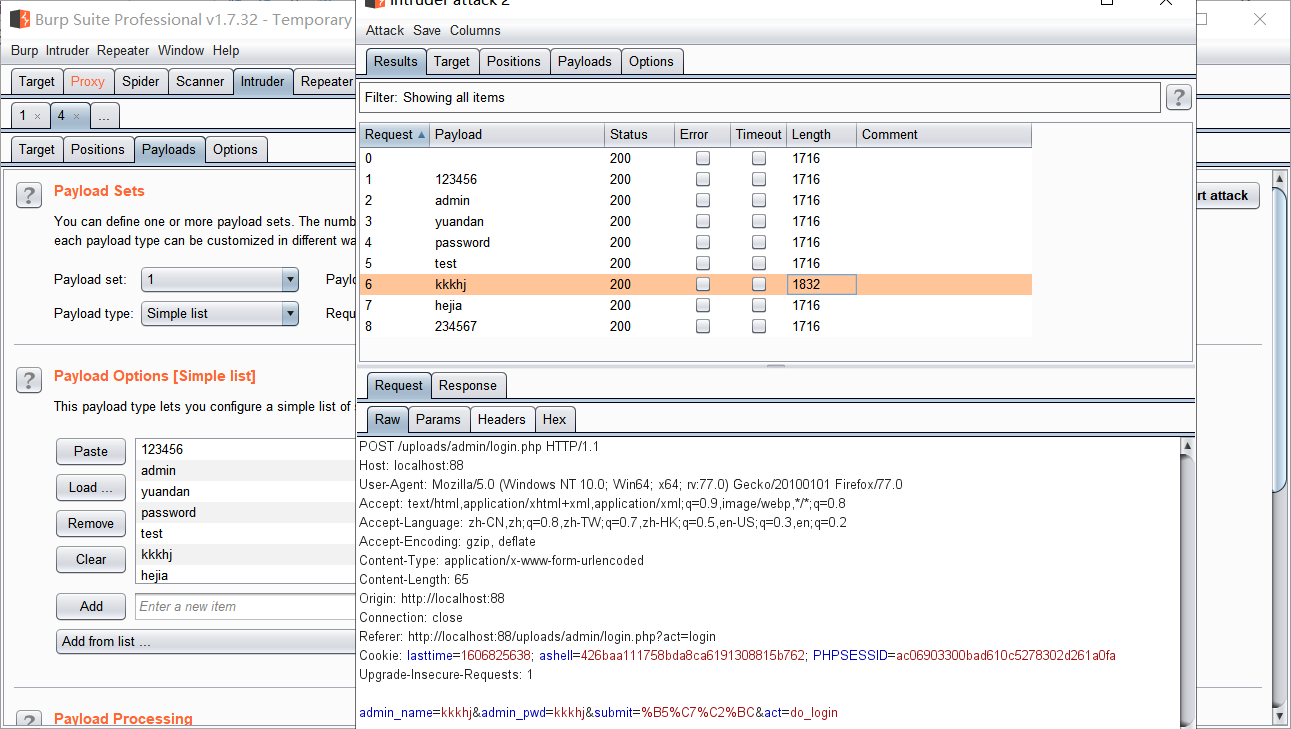


1. 自动攻击

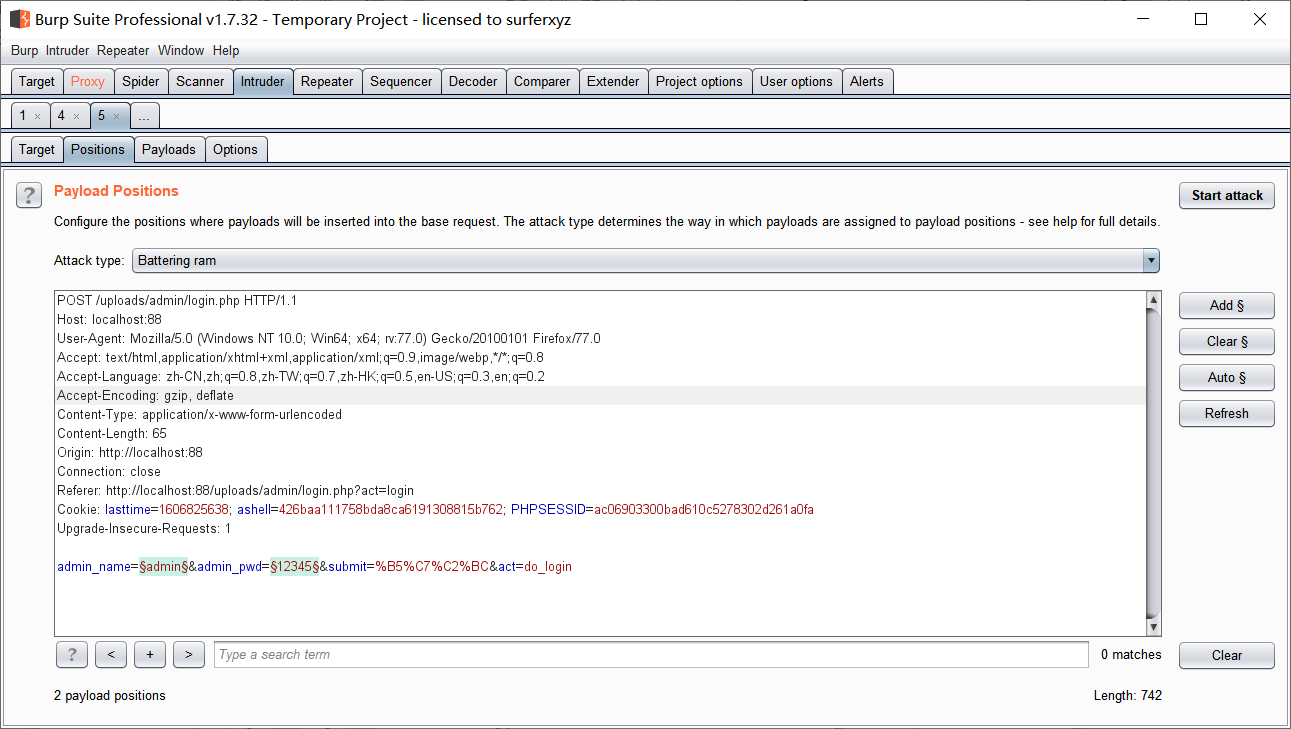
后台密码爆破

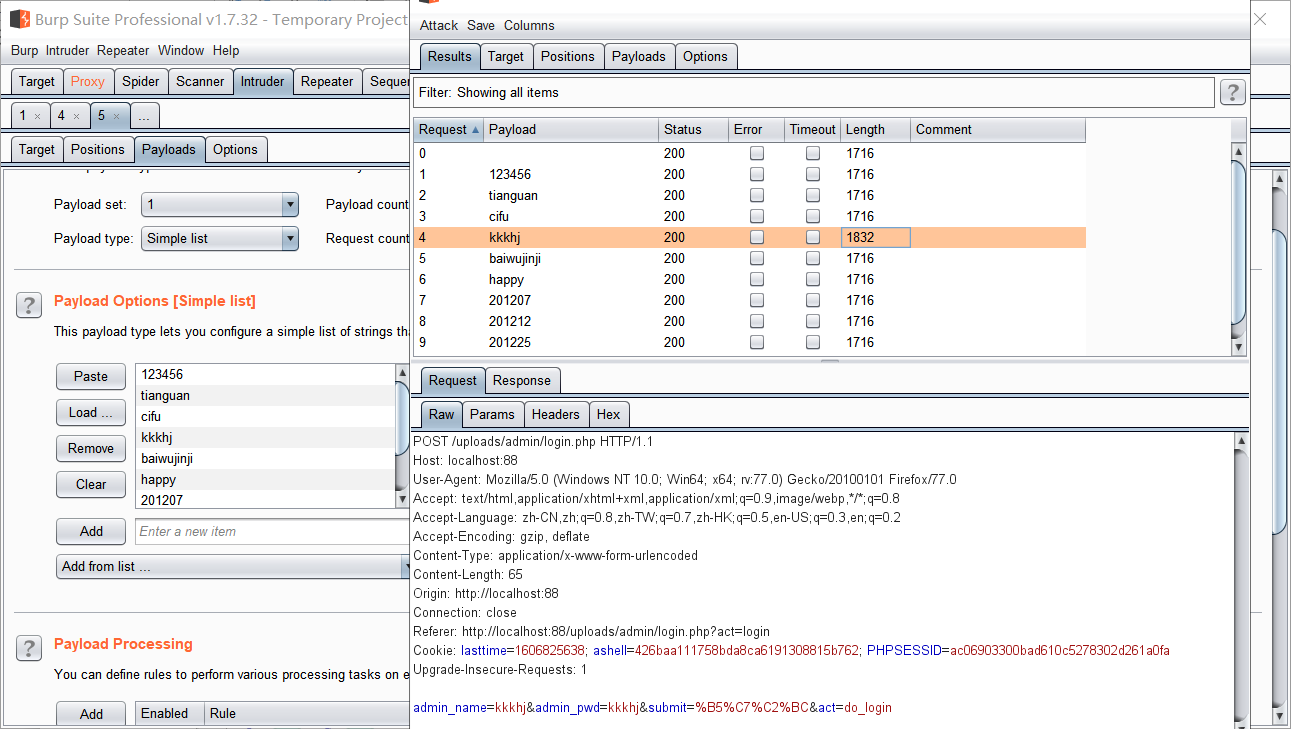
Sniper



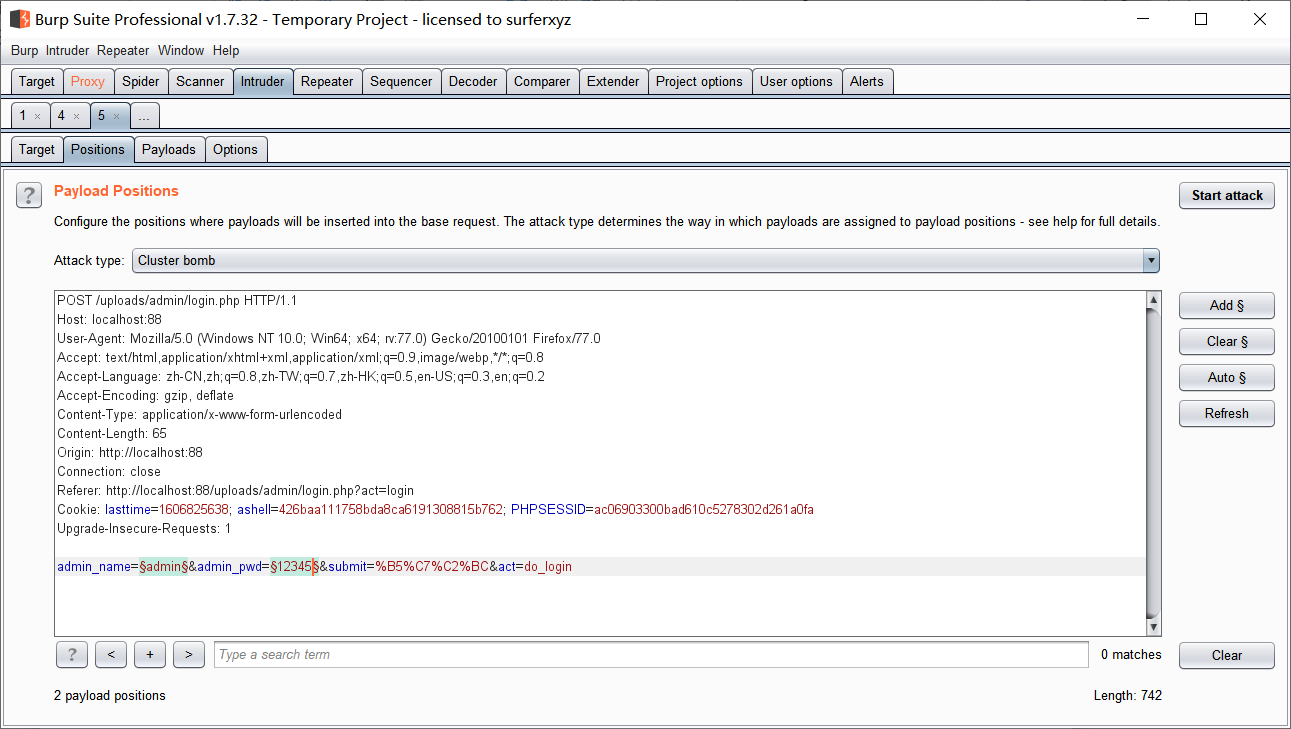


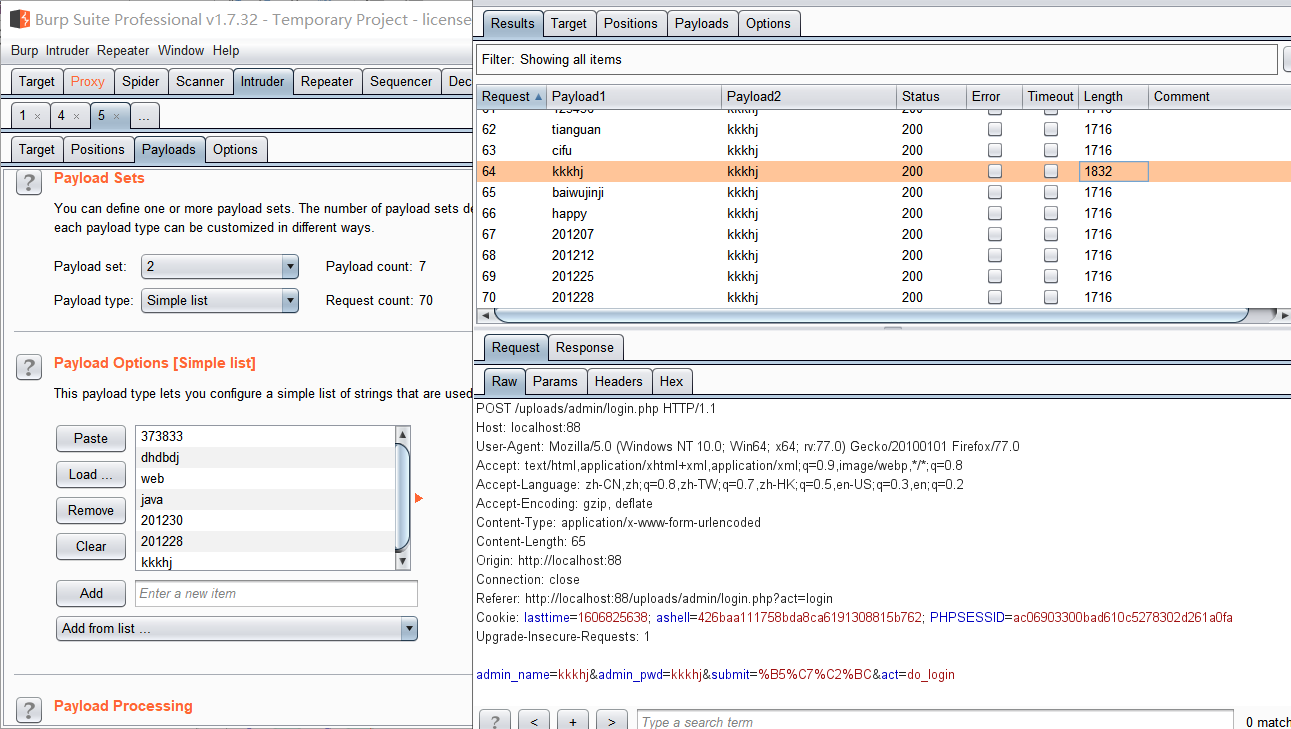
Battering ram：





Cluster bomb：



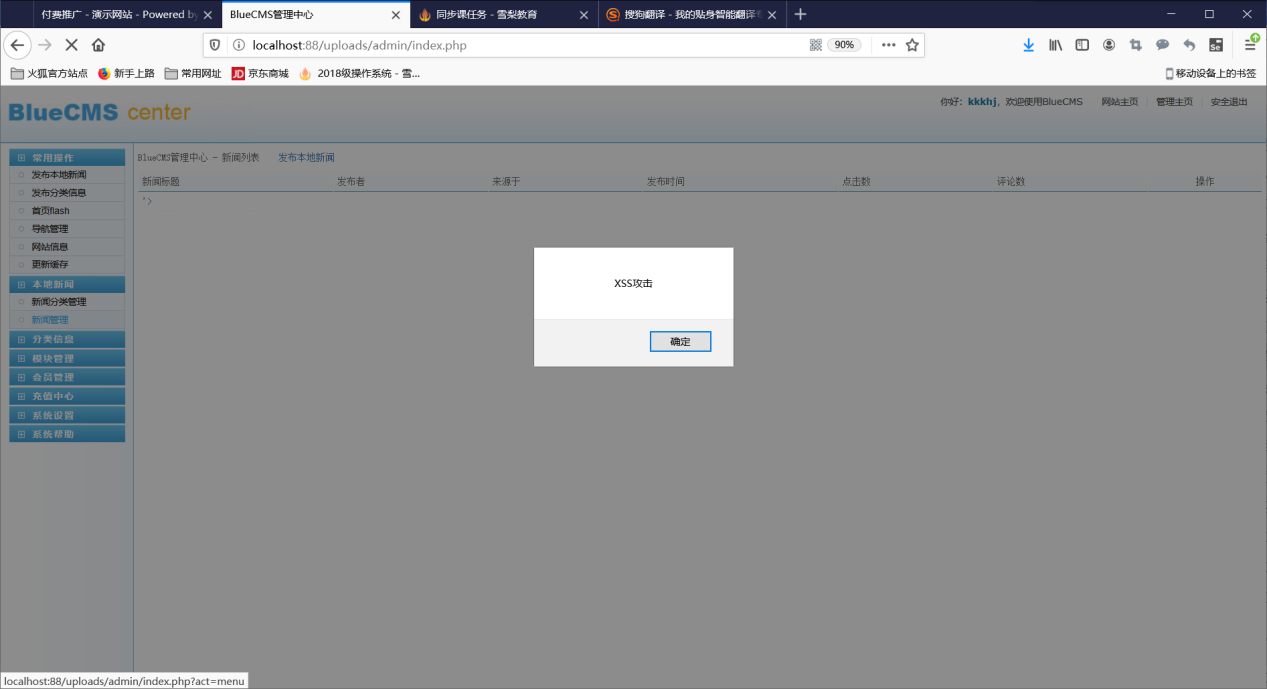


1. 手工测试

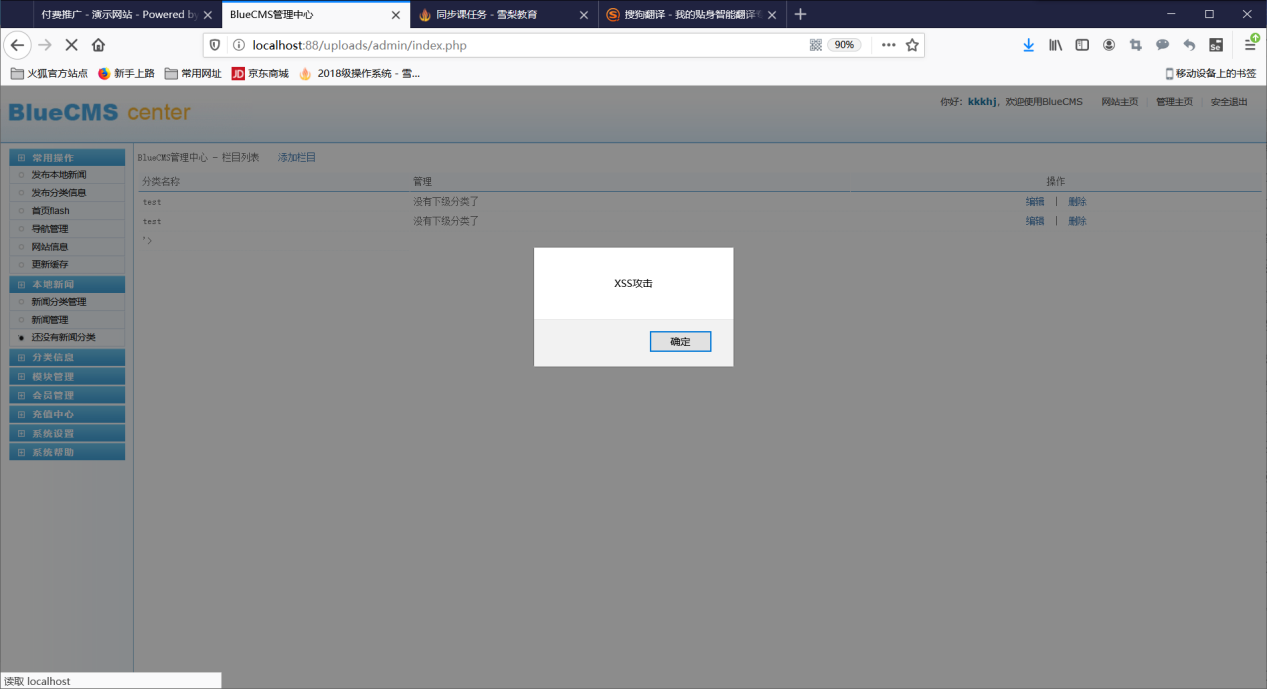
1.前后台登陆输入sql注入语句，如'or1=1--，登录失败，不存在sql注入漏洞



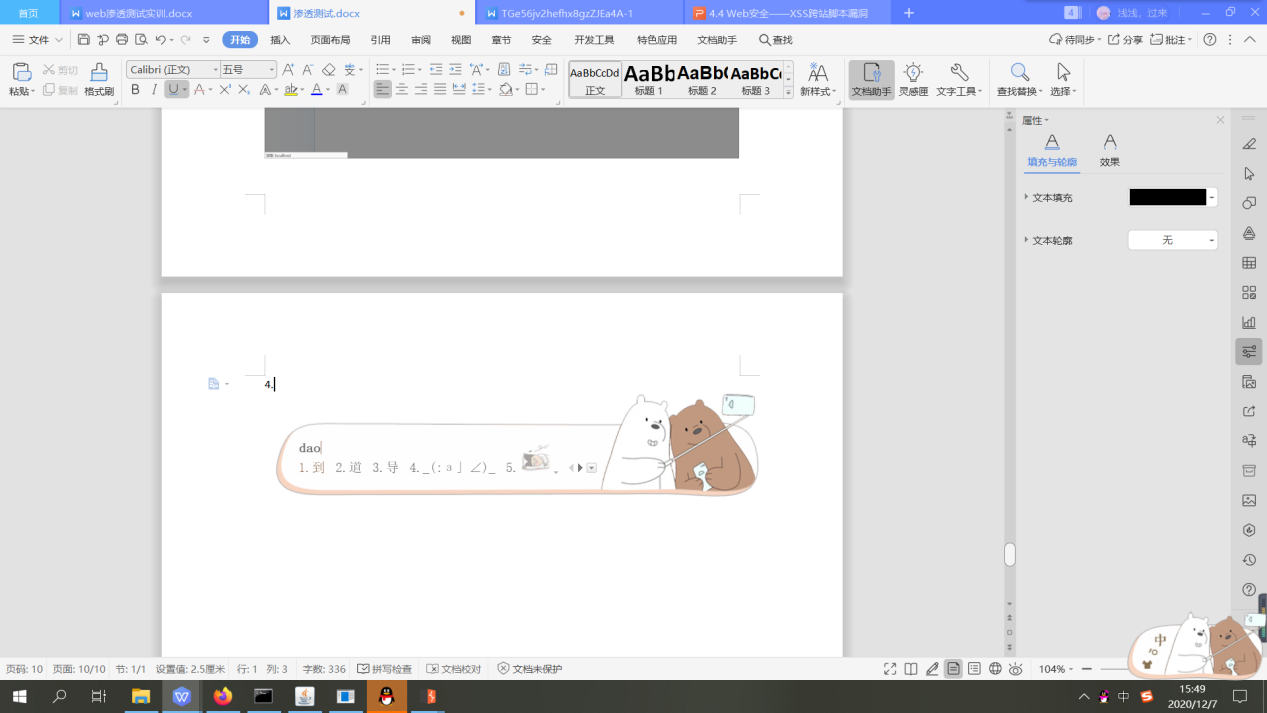
2.后台发布本地新闻存在反射型xss漏洞



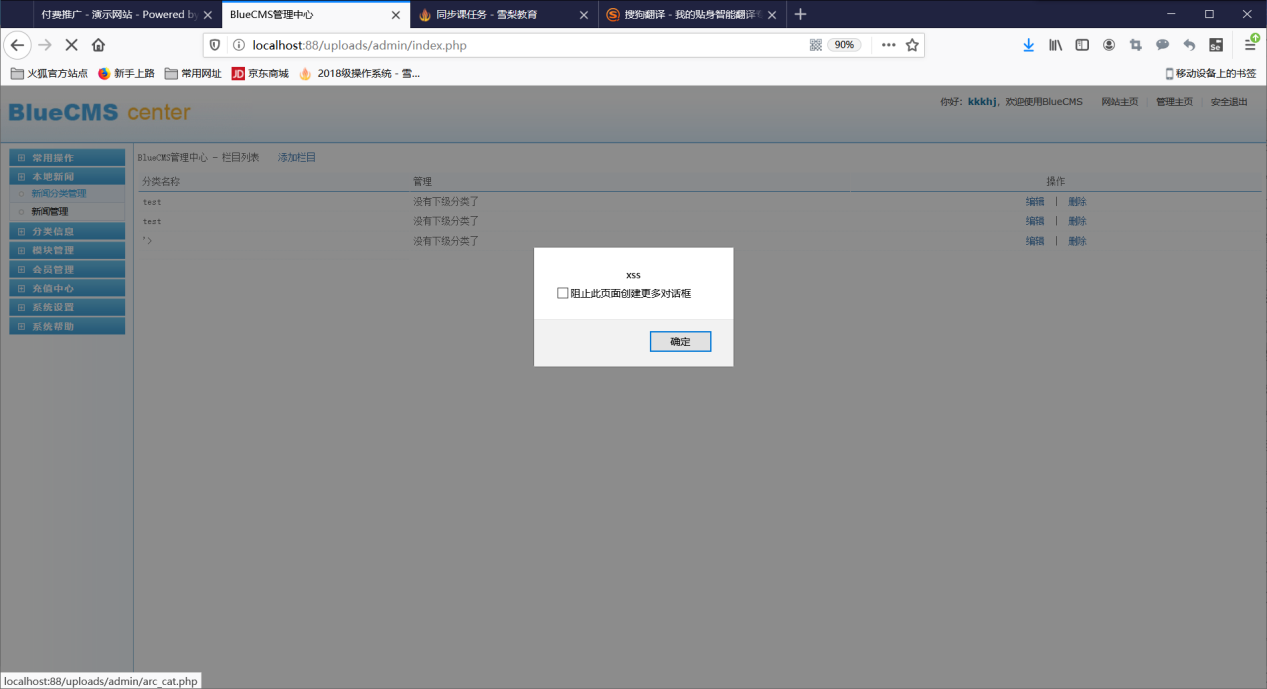
3.后台添加新栏目存在反射型小手术漏洞



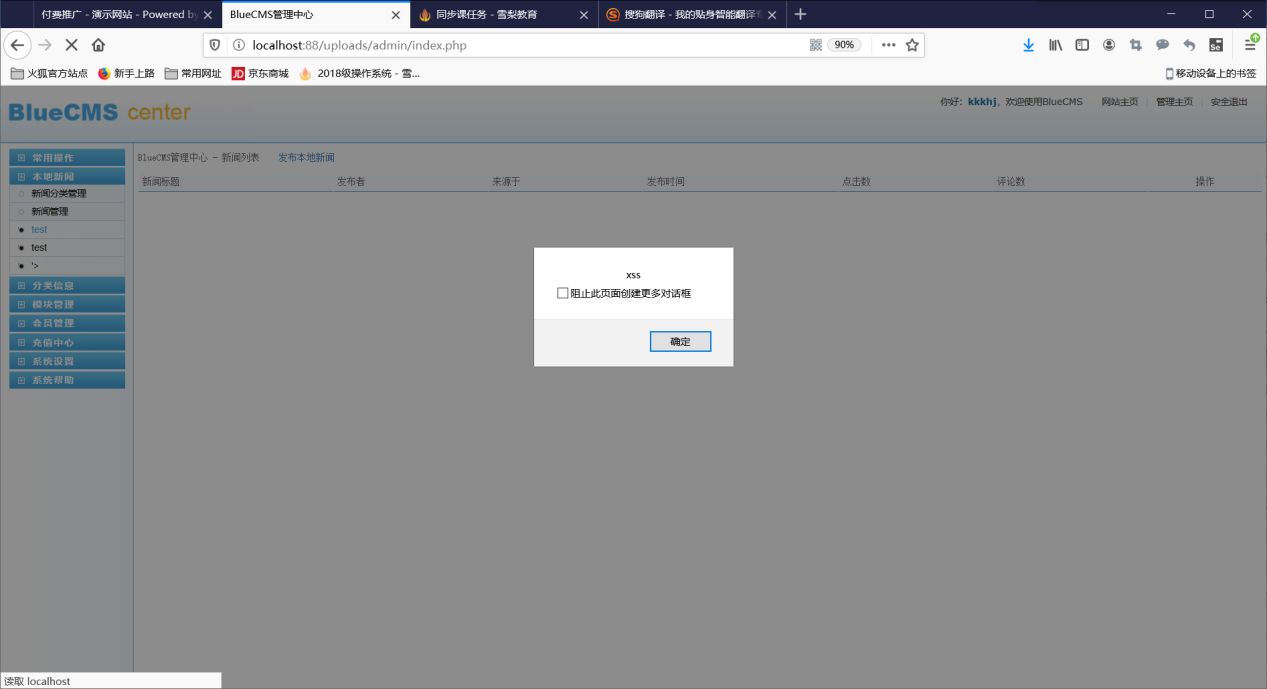
4.后台导航管理添加新链接存在存储型xss漏洞



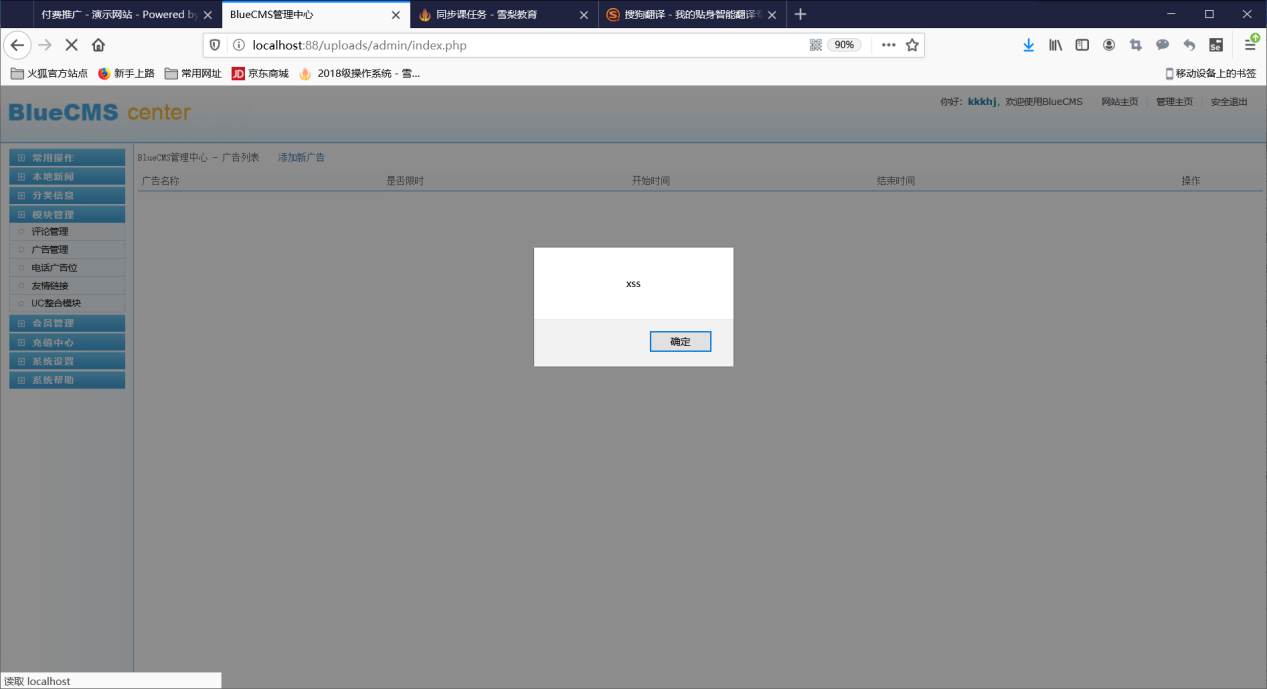
5.后台新闻分类管理添加栏目存在反射型，存储型xss漏洞



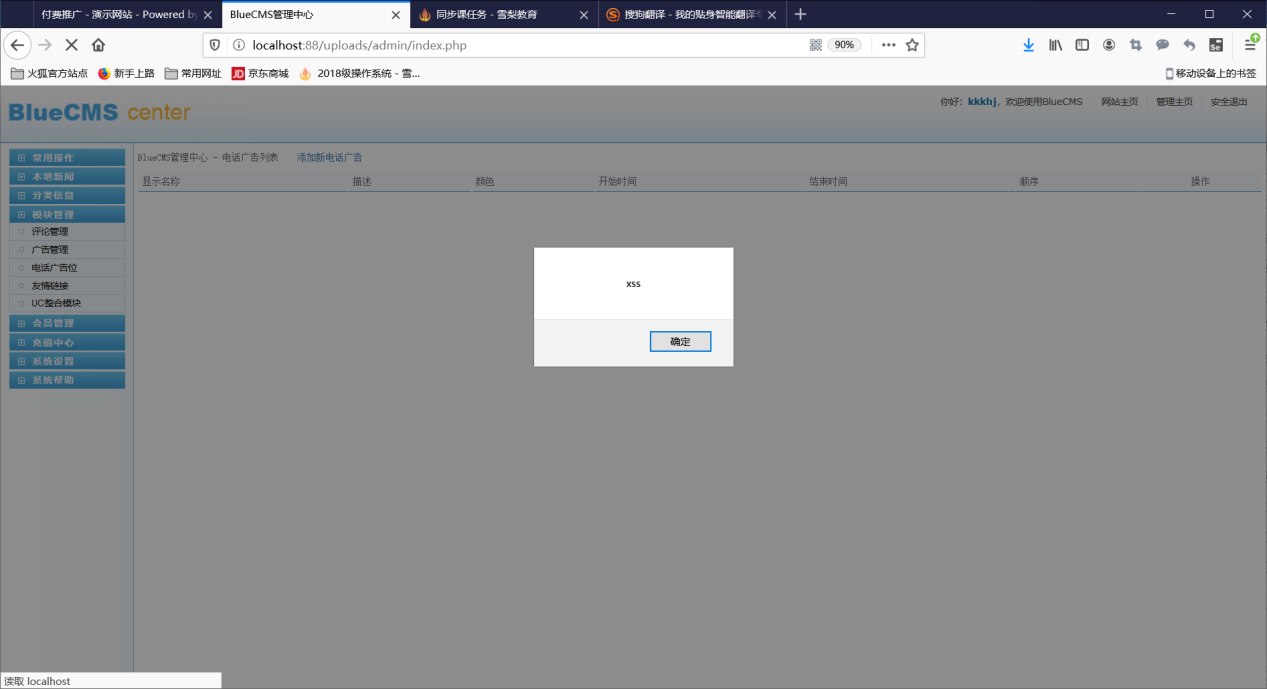
6.后台新闻管理存在存储型xss漏洞



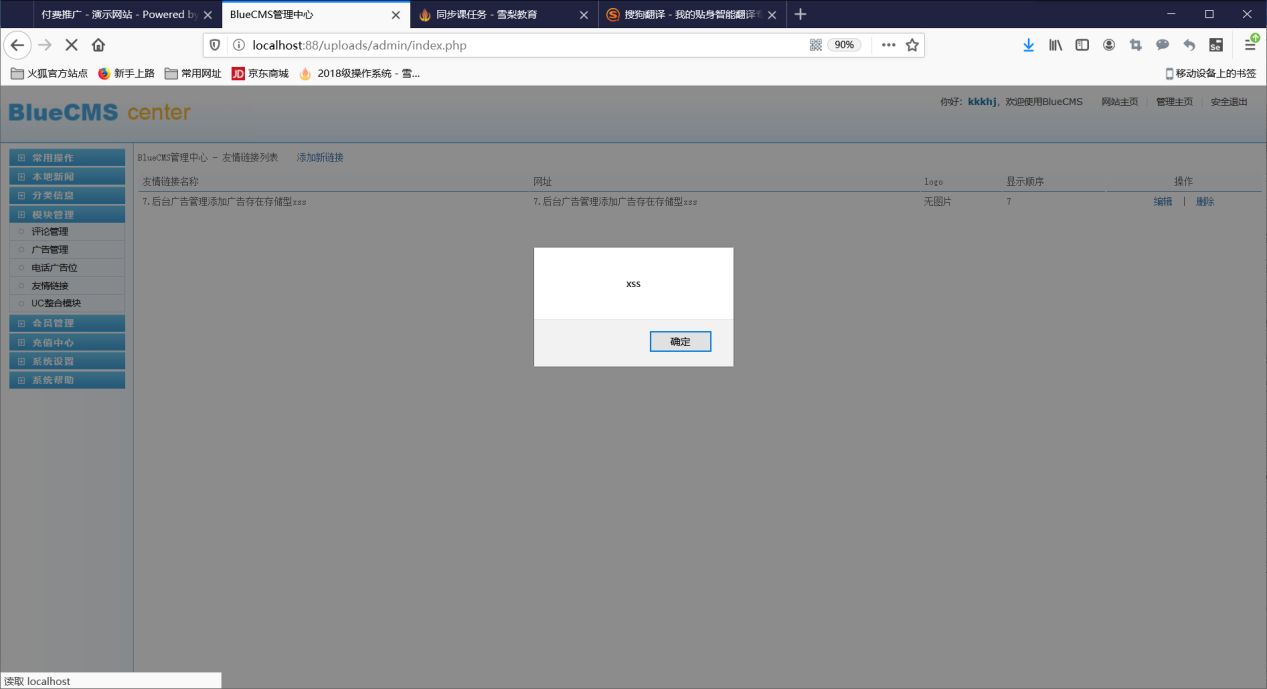
7.后台广告管理添加广告存在存储型xss



8.后台广告管理添加电话广告存在存储型xss



9.后台广告管理添加友情链接存在存储型xss



1. 后台会员管理会员列表存在存储型xss漏洞

