# bluecms\_1.6网站渗透测试报告

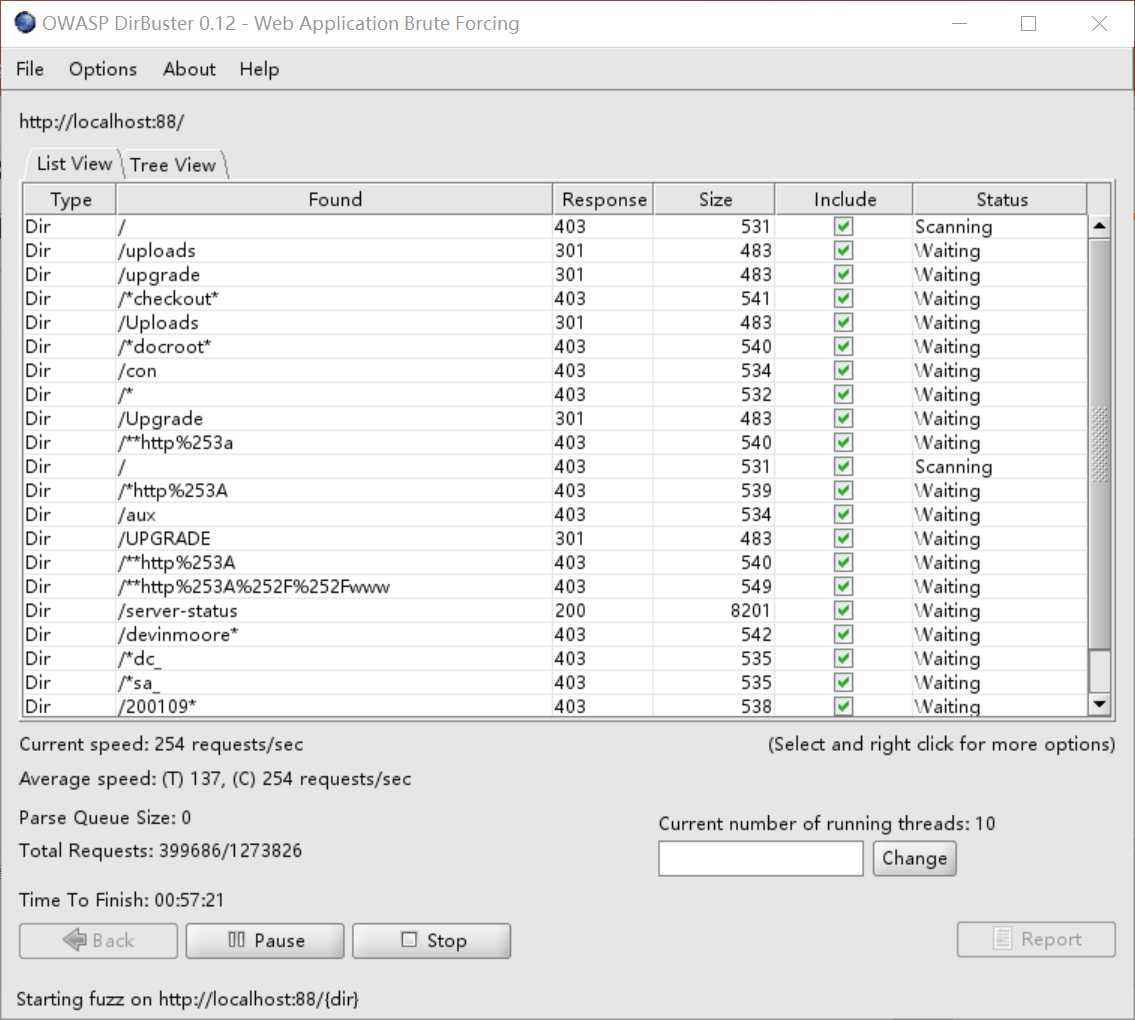
**分为五个部分：**

1. 信息收集
2. 利用burpsuit进行漏洞扫描
3. 爬取网站
4. 自动化攻击
5. 对网站进行手工测试
6. **信息收集**

域名信息

环境搭建在本机，无域名信息

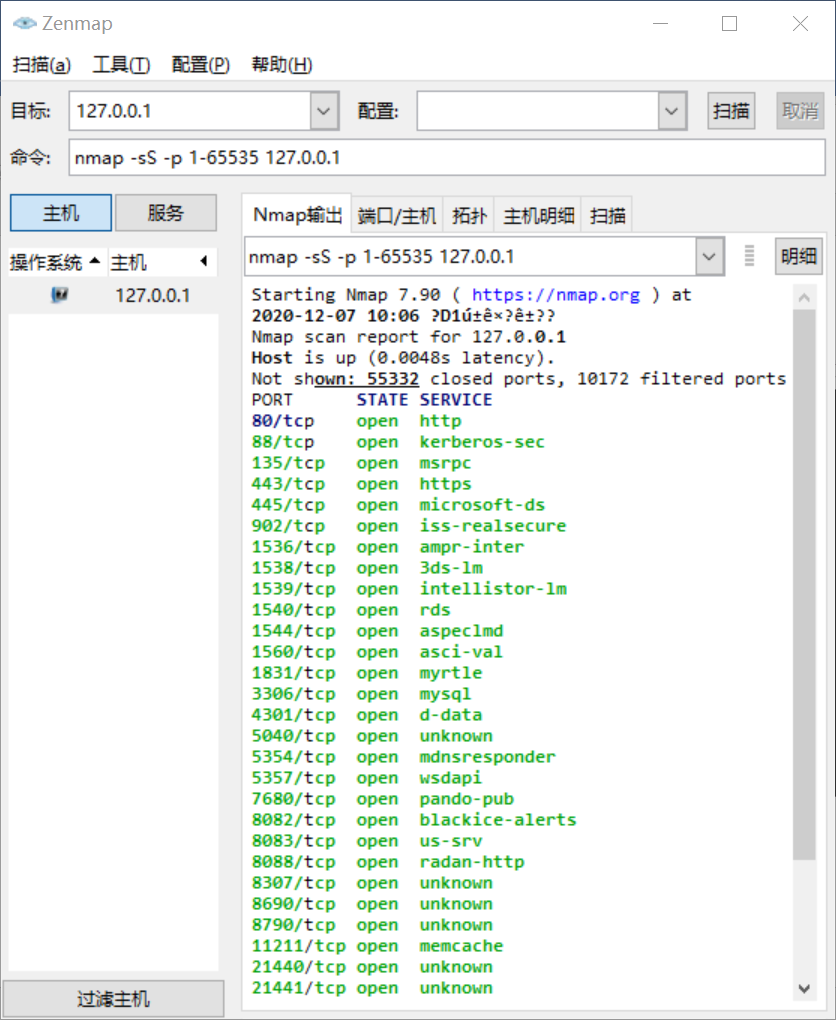
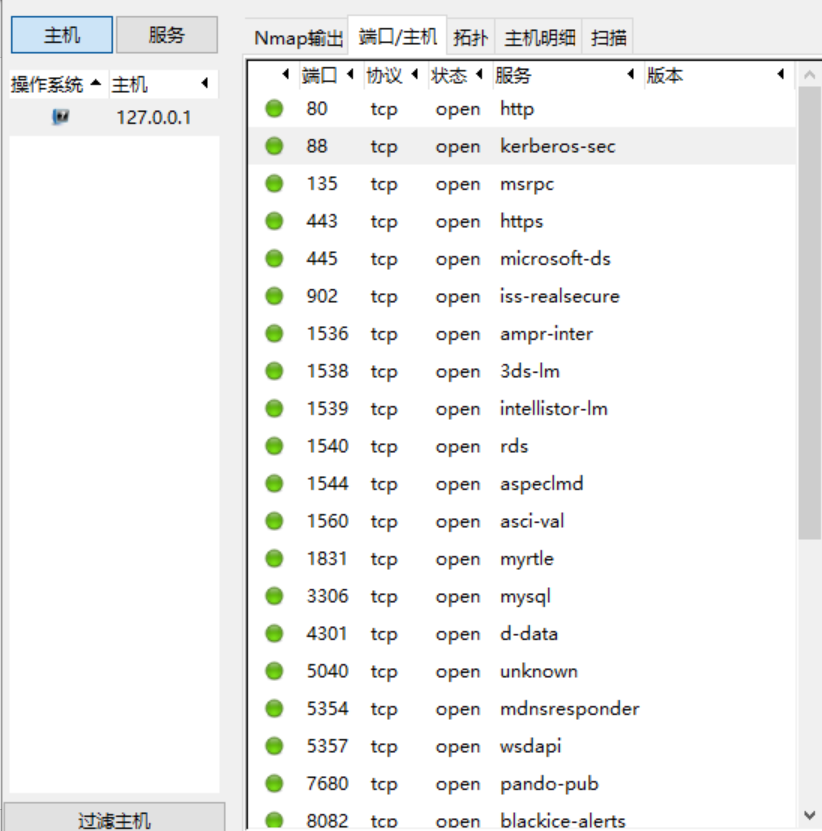
敏感目录



配置端口



扫描端口



扫描操作系统



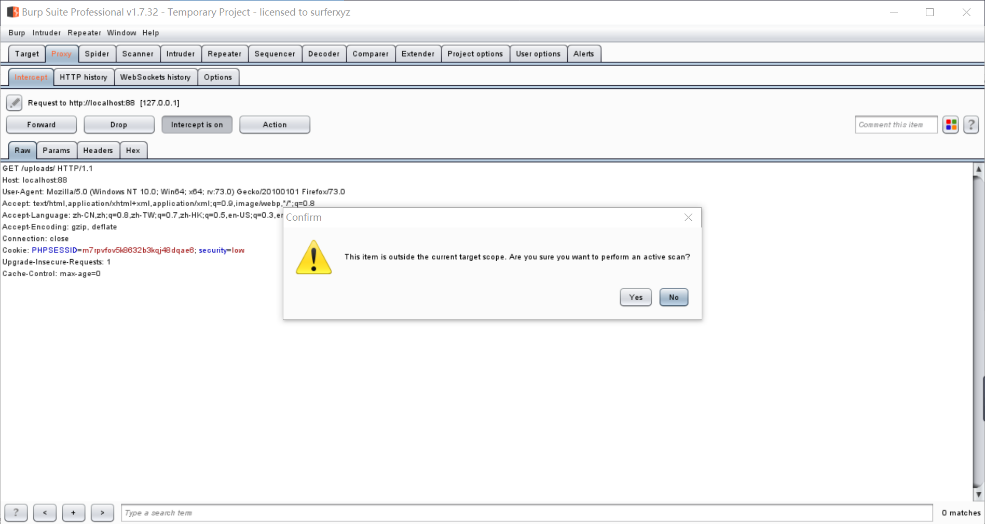
操作系统是Microsoft Windows 10 1809 – 1909

脚本类型php

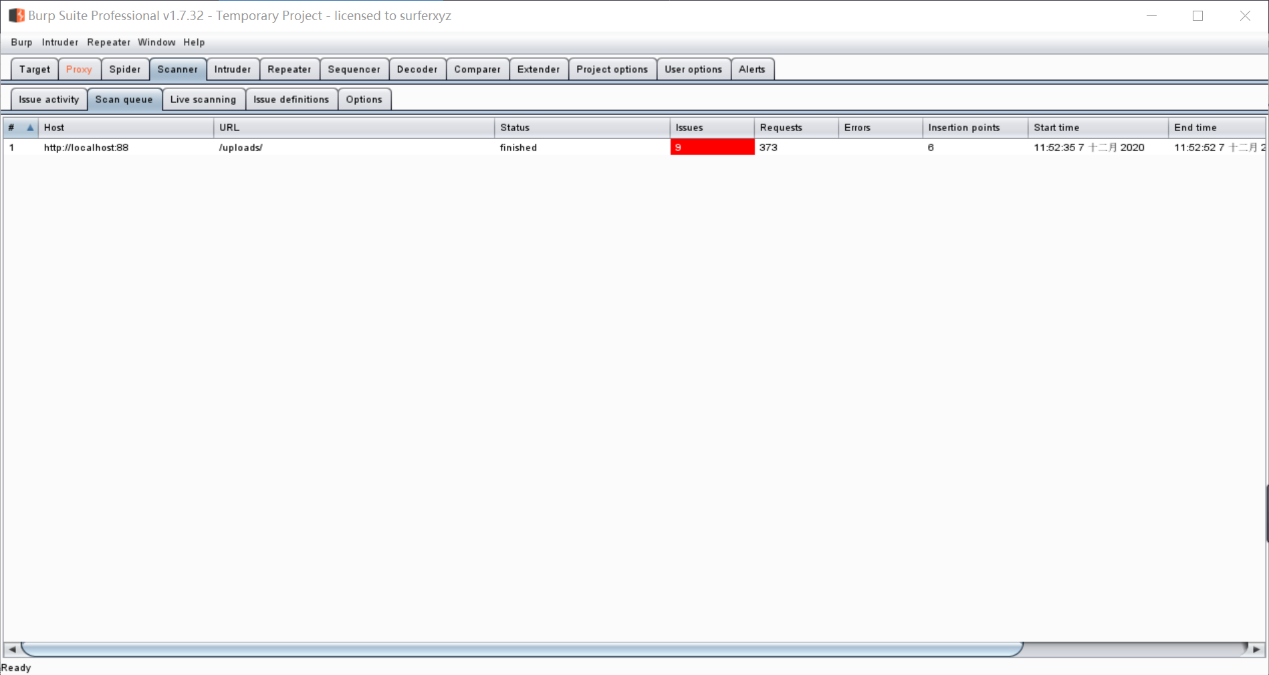
数据库类型mysql

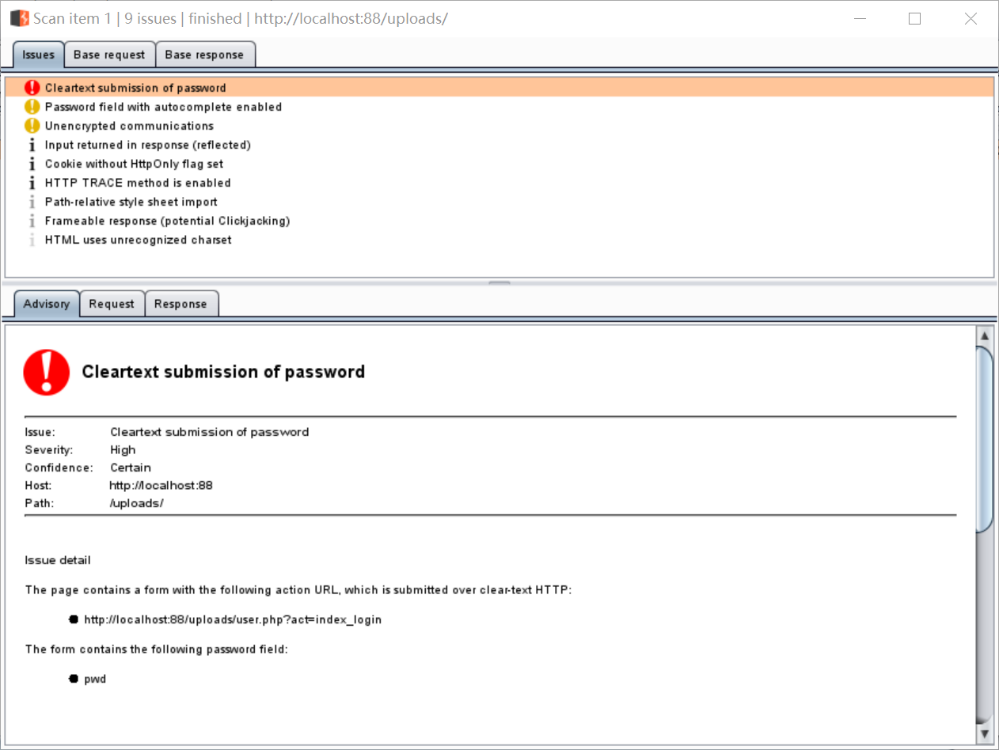
1. **利用burpsuit进行漏洞扫描：**

打开网站，配置代理服务器，开始扫描漏洞

、

前台：





共9个漏洞：

High：Cleartext submission of password(明文提交密码)

Low：Password field with autocomplete enabled(密码字段自动完成启用)

Unencrypted communications(未加密的通讯)

Information：Input returned in response (reflected) (响应返回的输入)

Cookie without Http Only flag set (不设置Http Only标志的Cookie)

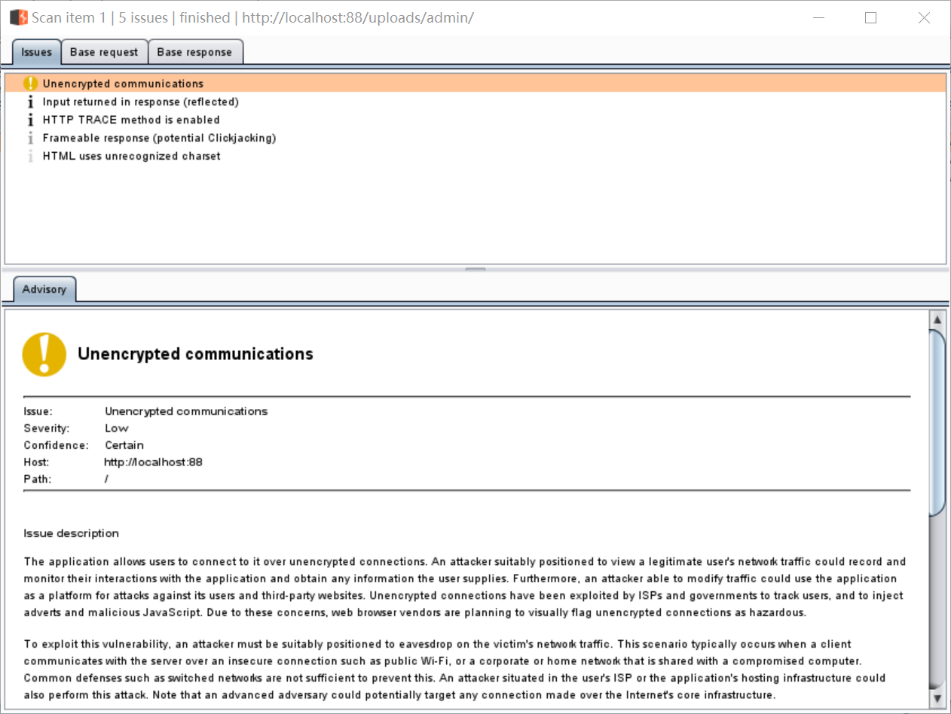
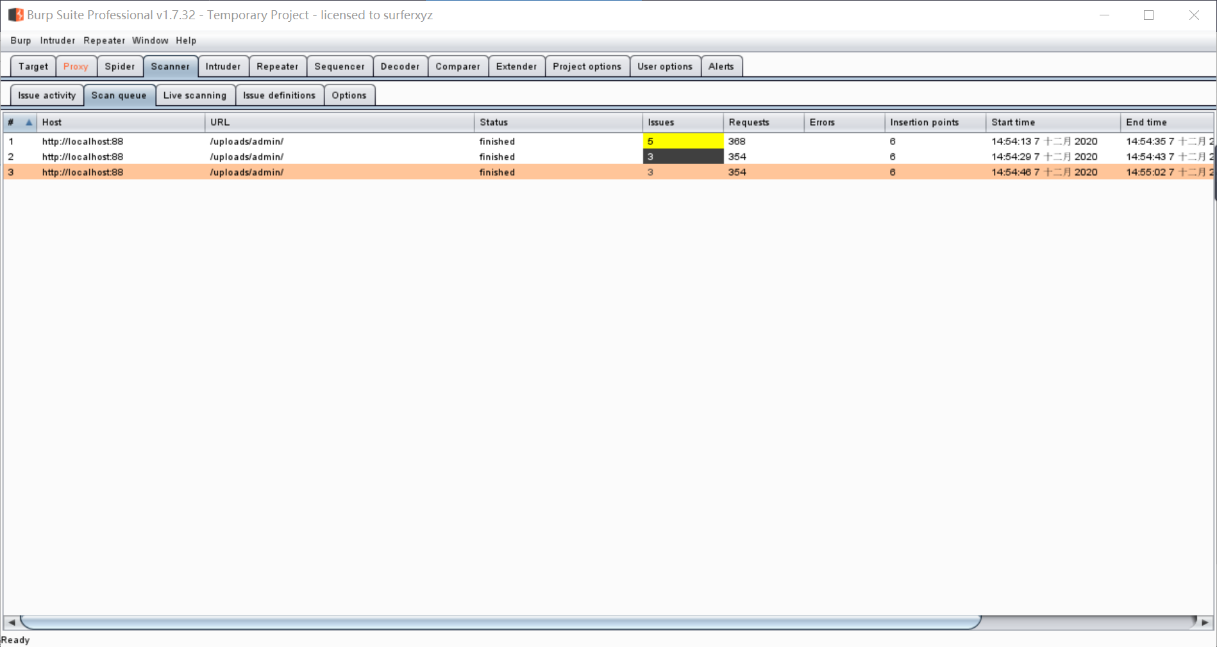
HTTP TRACE method is enabled (启用了HTTP TRACE方法)

Path-relative style sheet import (相对路径样式表导入)

Frameable response(potential Clickjacking) (框架响应（潜在的点击劫持）)

HTML uses unrecognized charset (HTML使用无法识别的字符集)

后台：



共5个漏洞：

Low：Unencrypted communications(未加密的通讯)

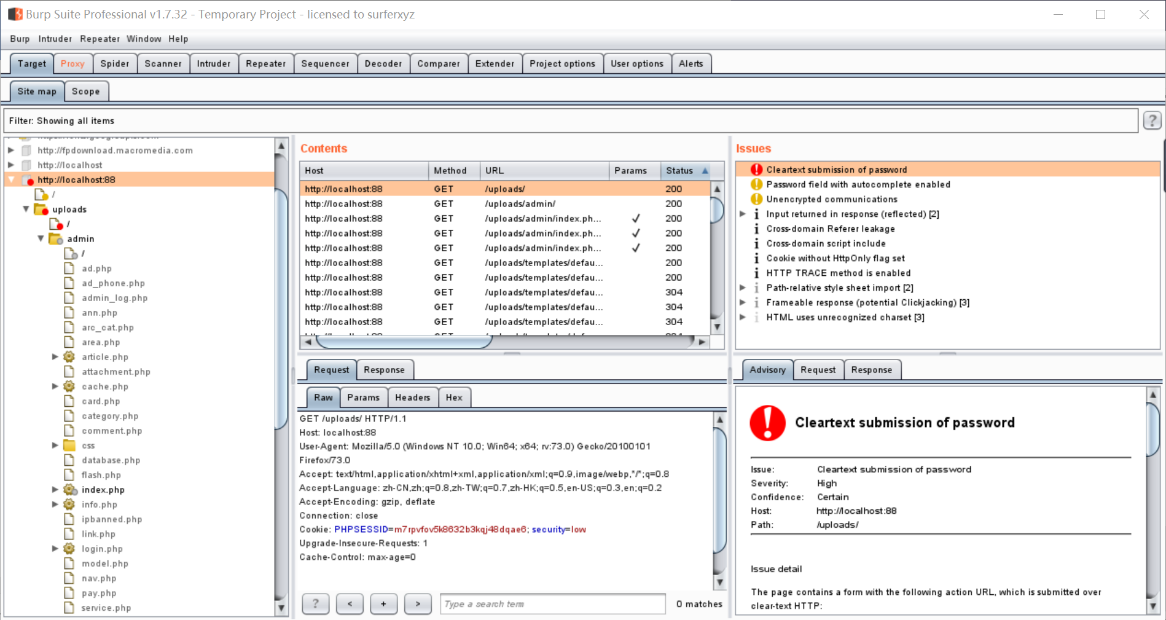
Information：Input returned in response (reflected) (响应返回的输入)

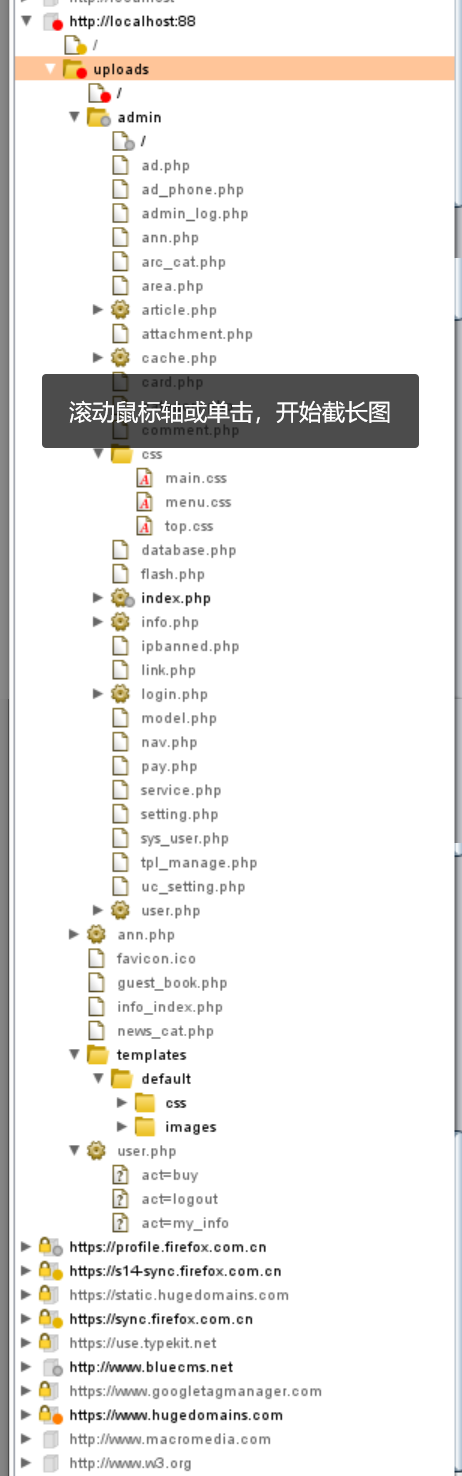
HTTP TRACE method is enabled (启用了HTTP TRACE方法)

Frameable response(potential Clickjacking) (框架响应（潜在的点击劫持）)

HTML uses unrecognized charset (HTML使用无法识别的字符集)

1. **爬取网站：**

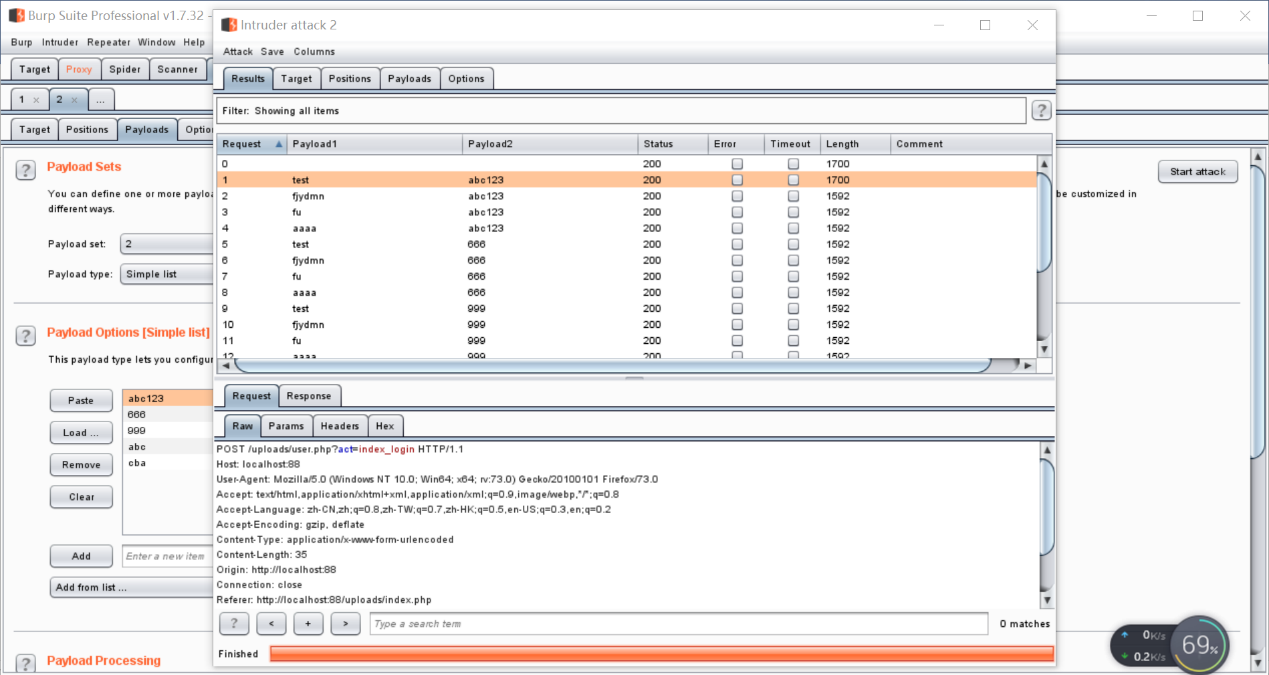




1. **自动化攻击：**

**intruder密码爆破**

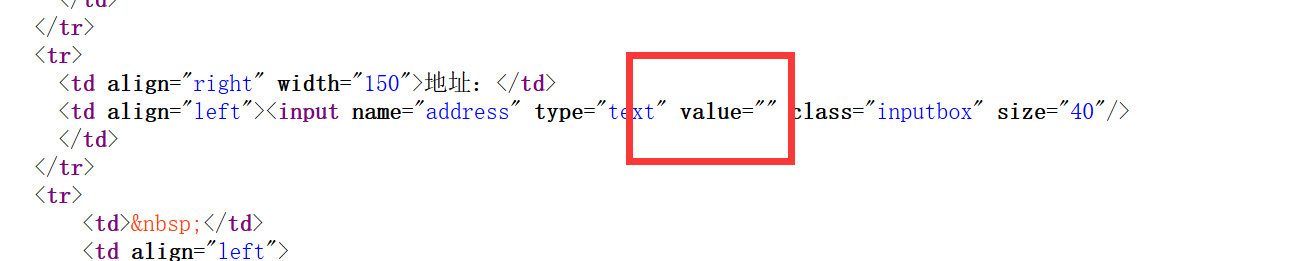
前提是注册用户：test abc123



1. **对网站进行手工测试：**

xss漏洞测试

**前台**：登录，点击会员中心-我的个人资料



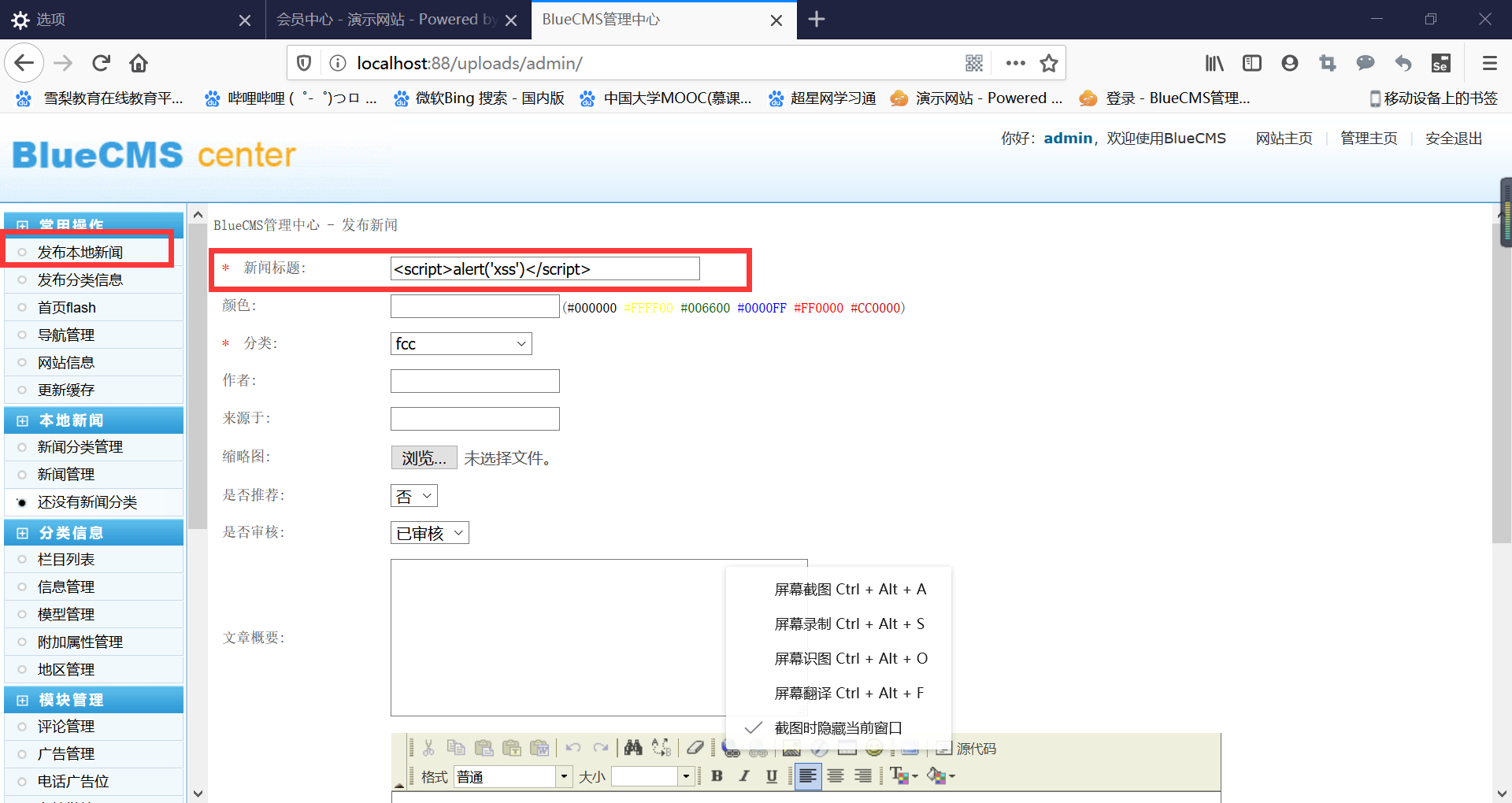




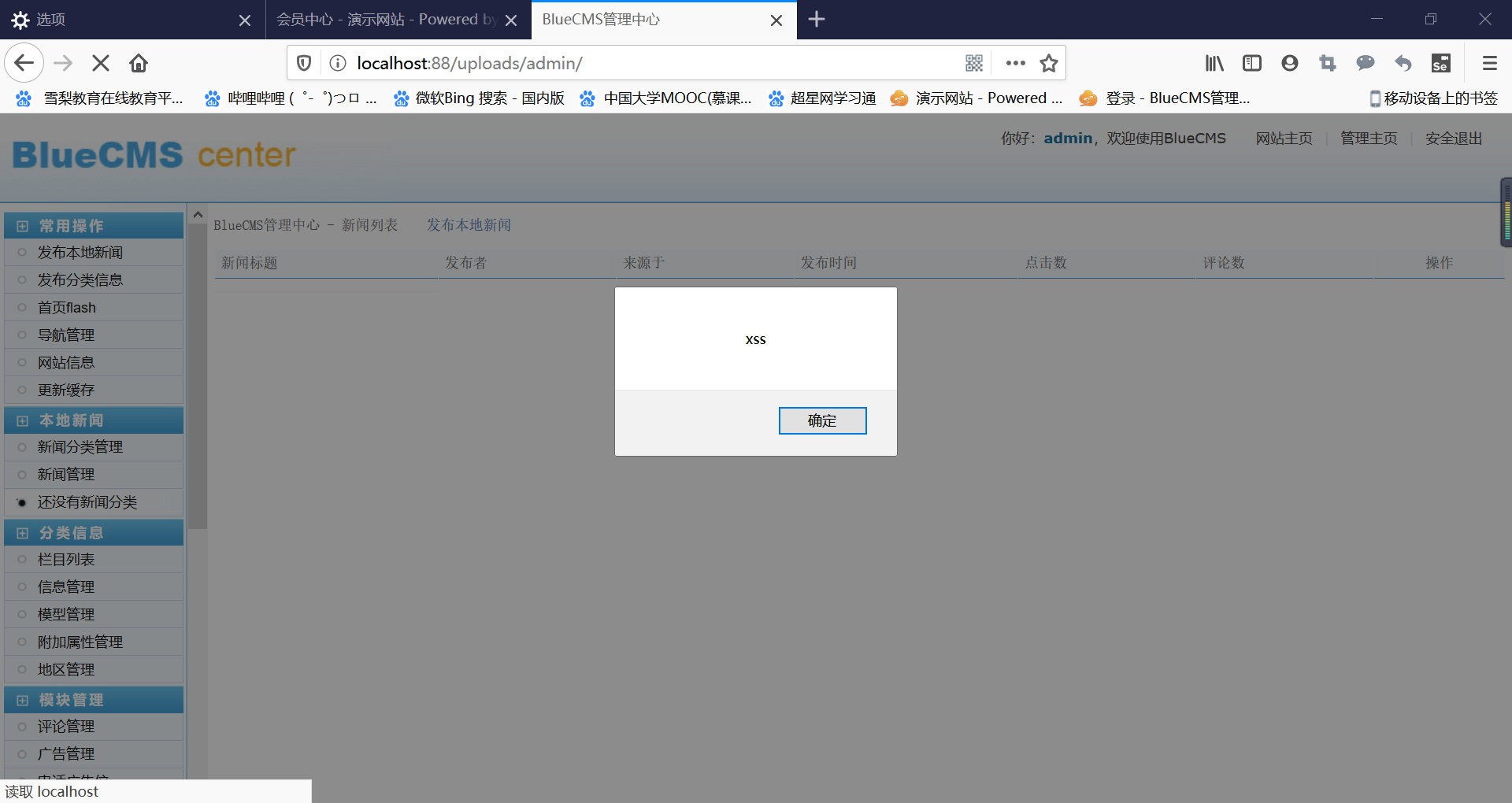
点击确认修改并无弹窗，查看网页源代码发现进行了转码，

所以前台不存在xss漏洞。

**后台**：登录，常用操作-发布本地新闻



点击提交



出现弹窗

前台浏览新闻时也会出现弹窗

所以后台存在xss漏洞