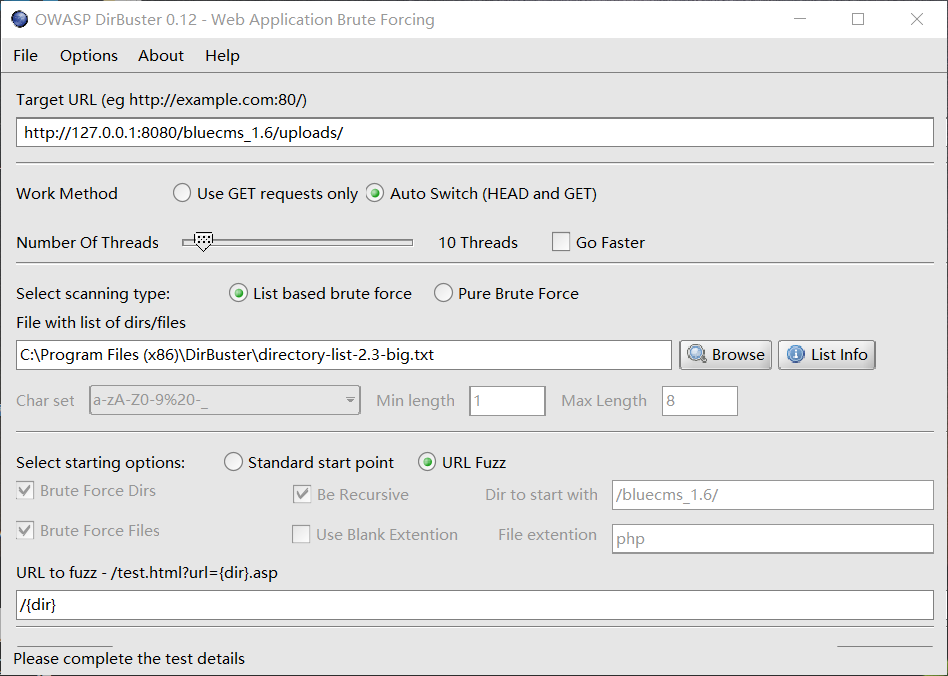
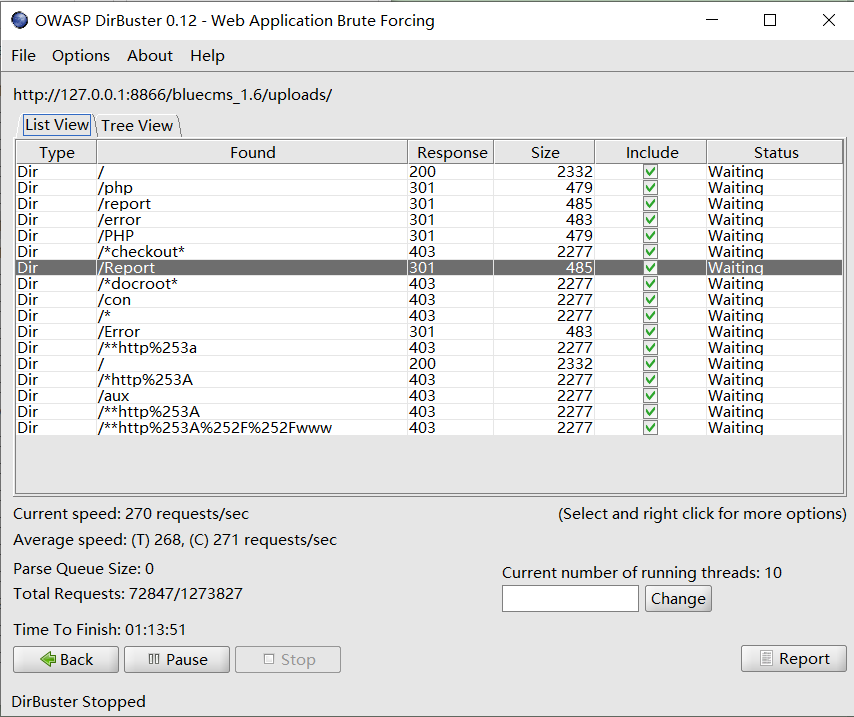
# 信息收集

### 域名信息

网站搭建在本机，无域名信息

### 敏感目录





### 端口扫描：

软件扫描报告崩溃

### 整站分析：

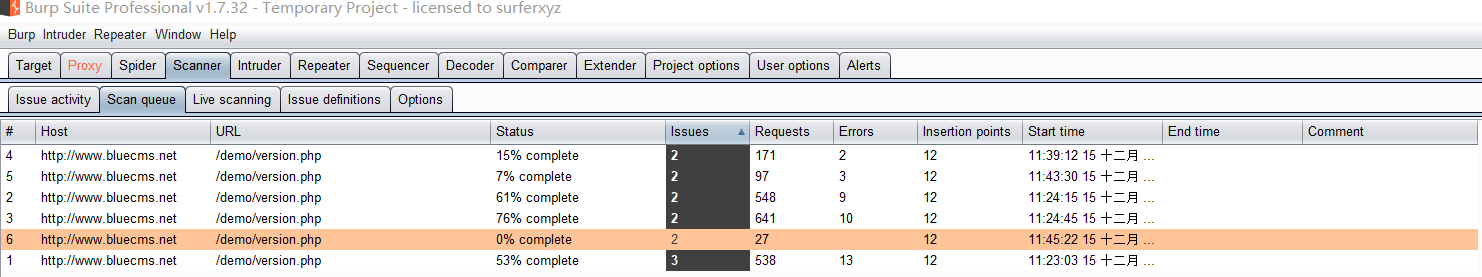
服务器的操作系统为windows系统

网站容器为Apache

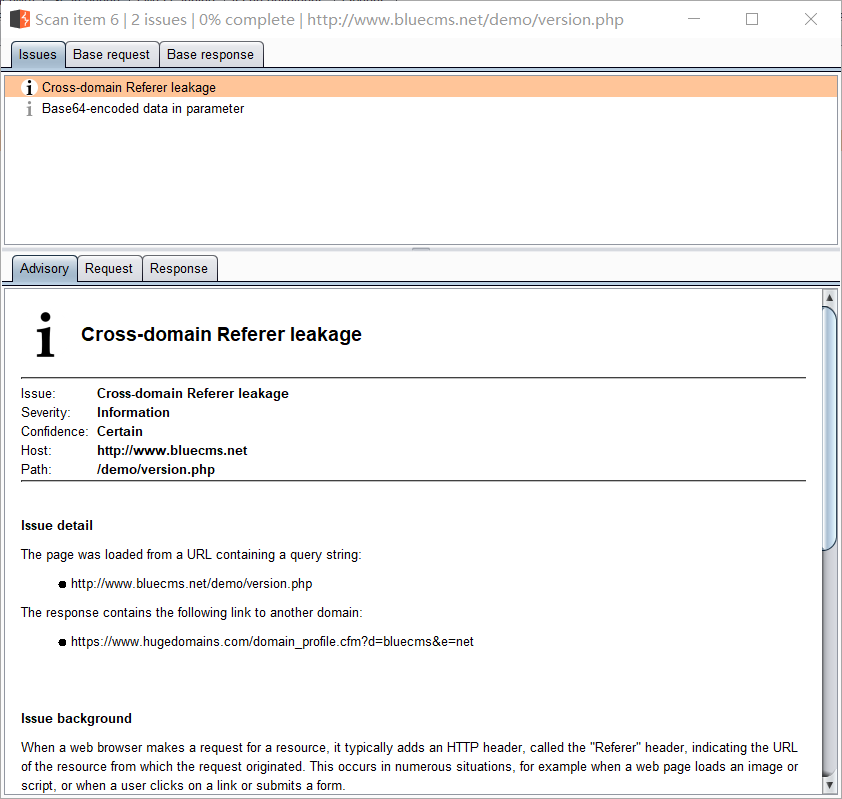
脚本类型为php

数据库为mysql

# 漏洞扫描：IMG_256



对http://127.0.0.1:8080/bluecms\_1.6/uploads/admin/后台进行扫描。

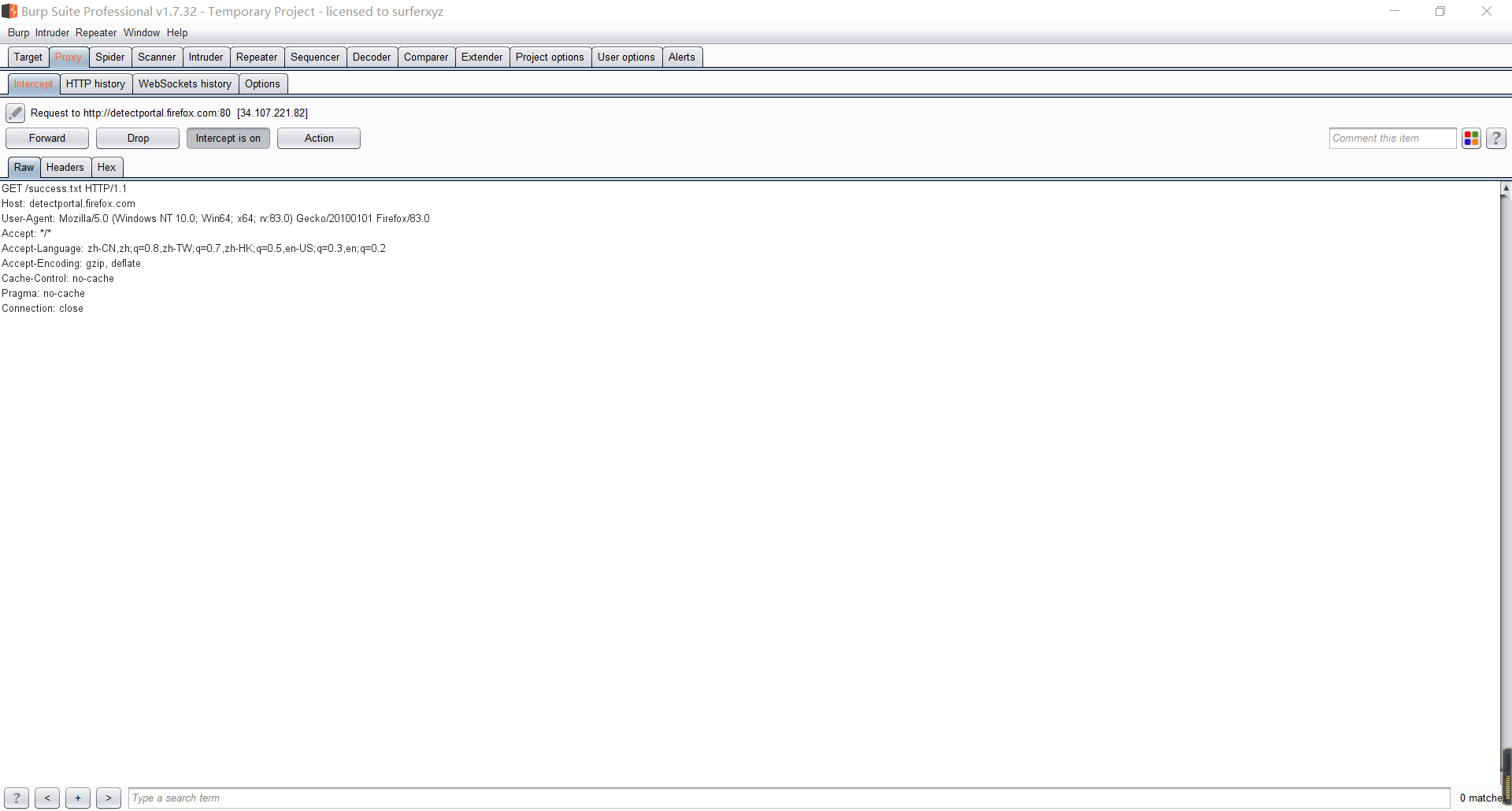


一共有2个漏洞，

1. Cross-domain Referer leakage
2. Base64-encoded data in parameter

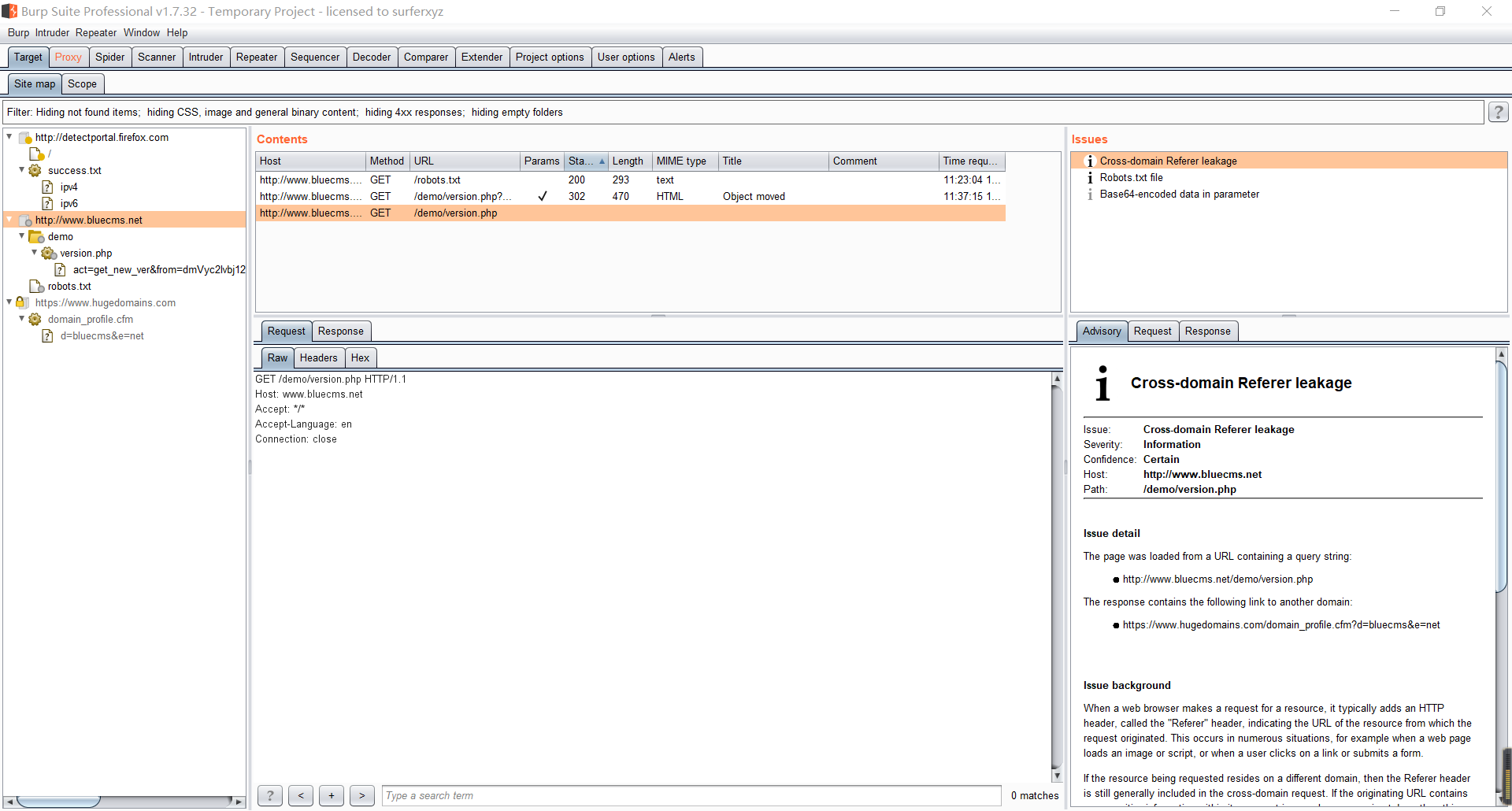
对http://127.0.0.1:8080/bluecms\_1.6/uploads/前台进行扫描

无法扫描出来，如下图：



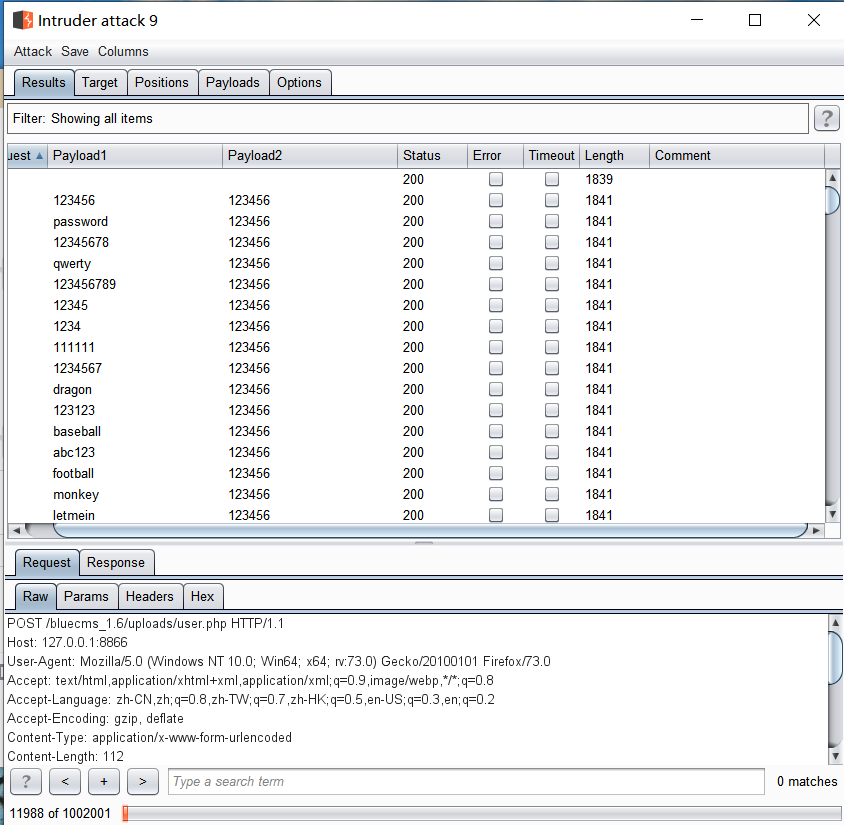
# 爬取网站：

爬取出的目录结构如下：



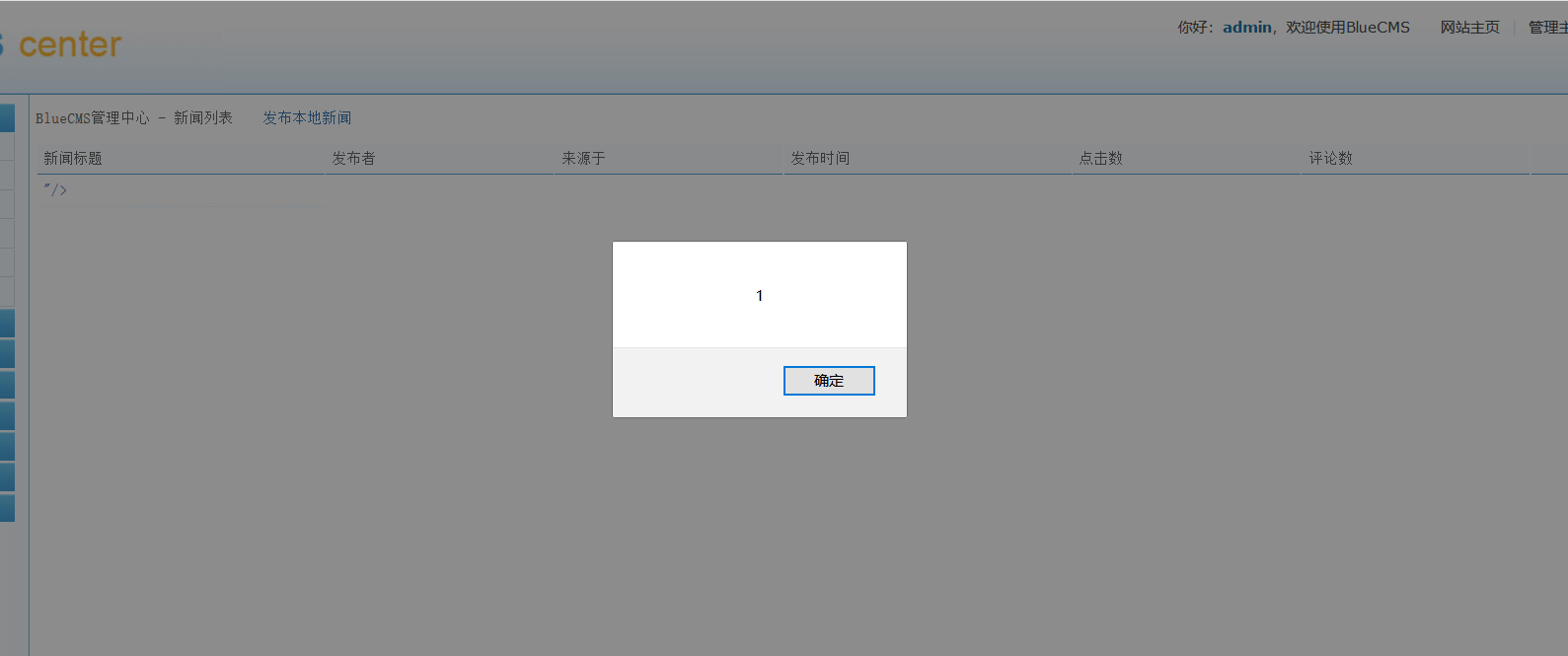
# 自动化攻击：

在前台登录界面，进行密码爆破，找了一个密码字典，采用cluster bomb

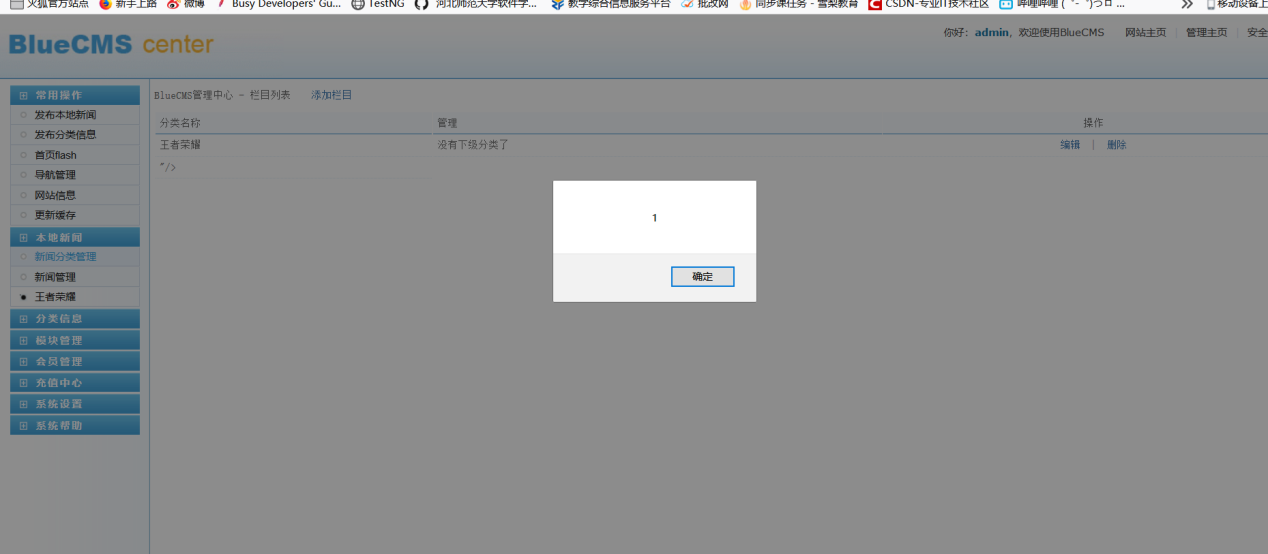


# 手工测试

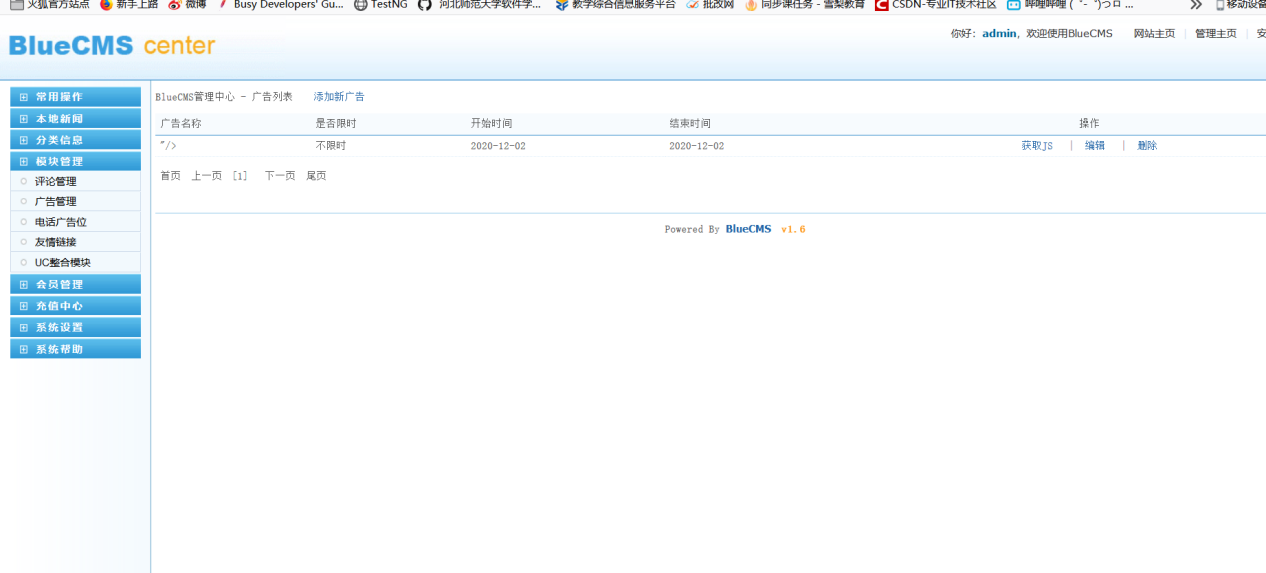
1.后台发布新闻，存在反射性xss漏洞。



2.后台本地新闻里的新闻分类管理，添加栏目里输入js脚本，存在存储型xss漏洞，每次打开这个界面，都会弹出弹窗。



3.后台，广告管理，添加新广告，存在存储型xss漏洞，每次打开这个界面，都会弹出弹窗。



4.会员管理，会员列表，添加新会员，存在存储型xss漏洞，每次打开这个界面，都会弹出弹窗。

