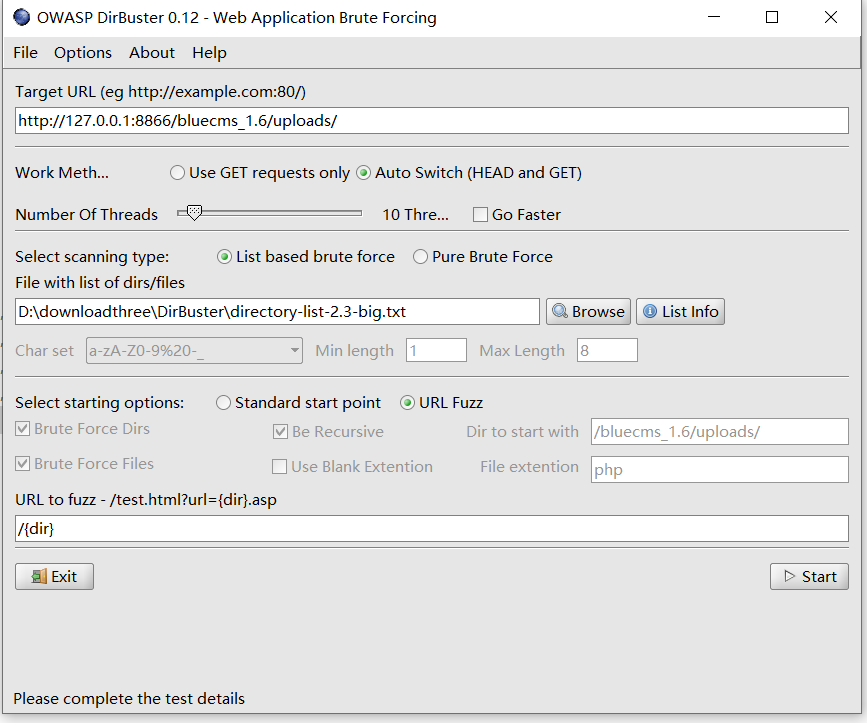
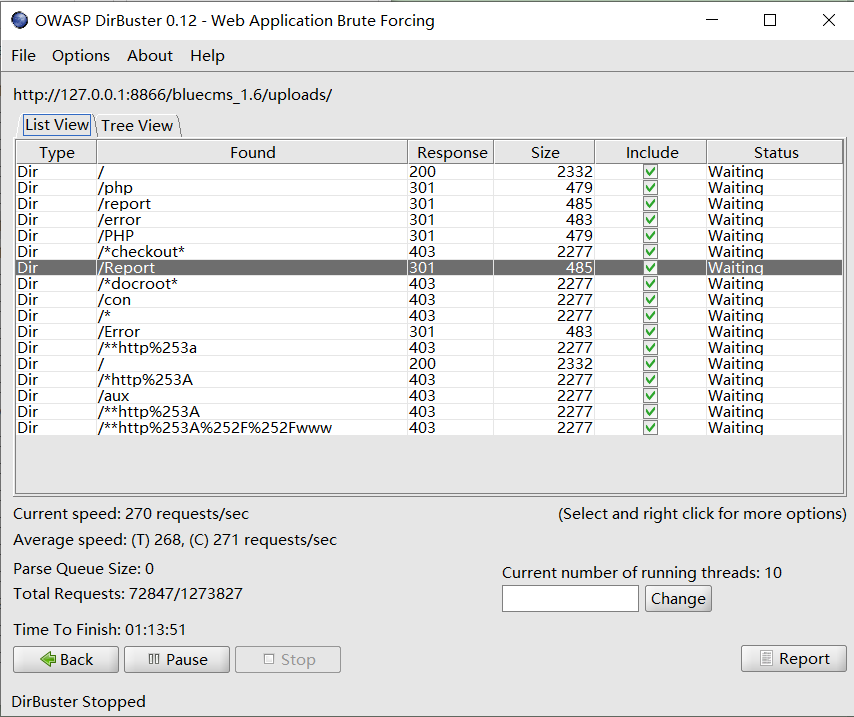
# 信息收集。

### 域名信息

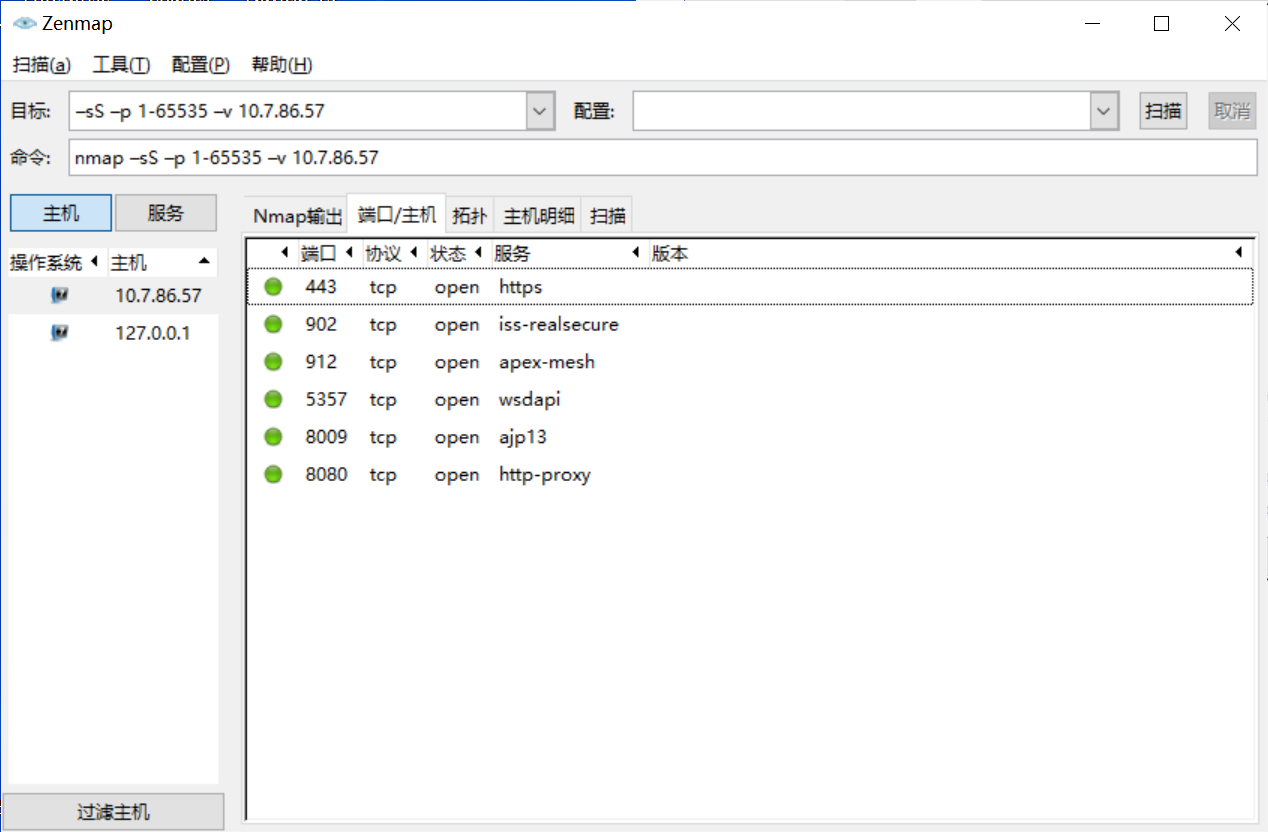
网站搭建在本机，无域名信息

### 敏感目录





### 端口扫描：



### 整站分析：

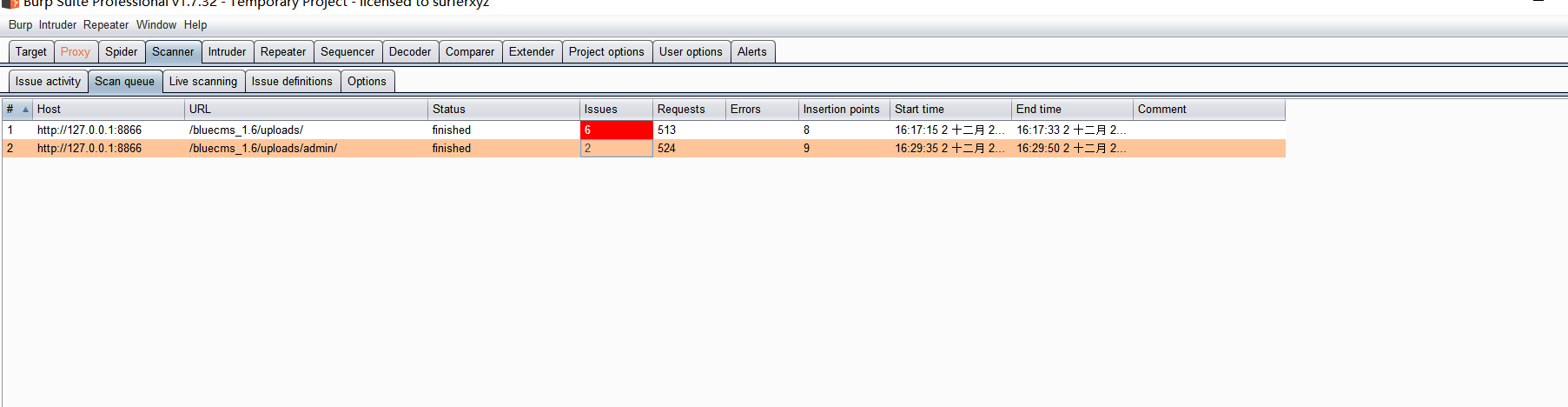
服务器的操作系统为windows系统

网站容器为Apache

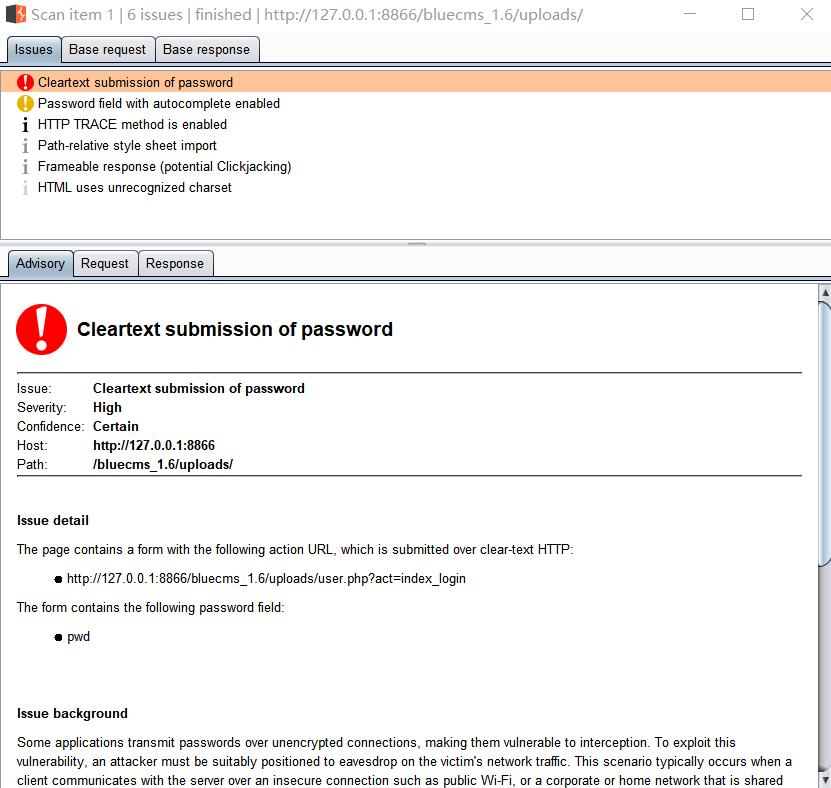
脚本类型为php

数据库为mysql

# 漏洞扫描：



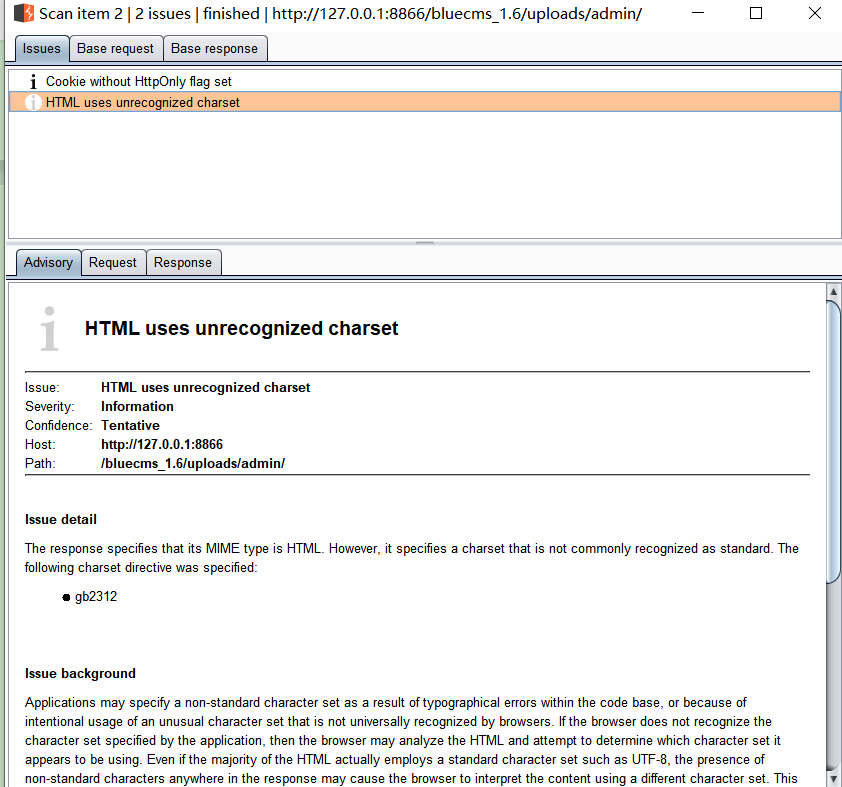
对http://127.0.0.1:8866/bluecms\_1.6/uploads/前台进行扫描。



一共有6个漏洞，

1. cleartext submission of password（明文提交密码）
2. password field with autocomplete enabled（密码字段与自动完成启用）
3. http trace method is enadbled(添加了http跟踪方法)
4. path-relative style sheet import(路径相关样式表导入)
5. potential clickjacking(潜在的点击劫持)
6. HTML uses unrecognized charset（HTML使用无法识别的字符集）

对http://127.0.0.1:8866/bluecms\_1.6/uploads/admin/后台进行扫描

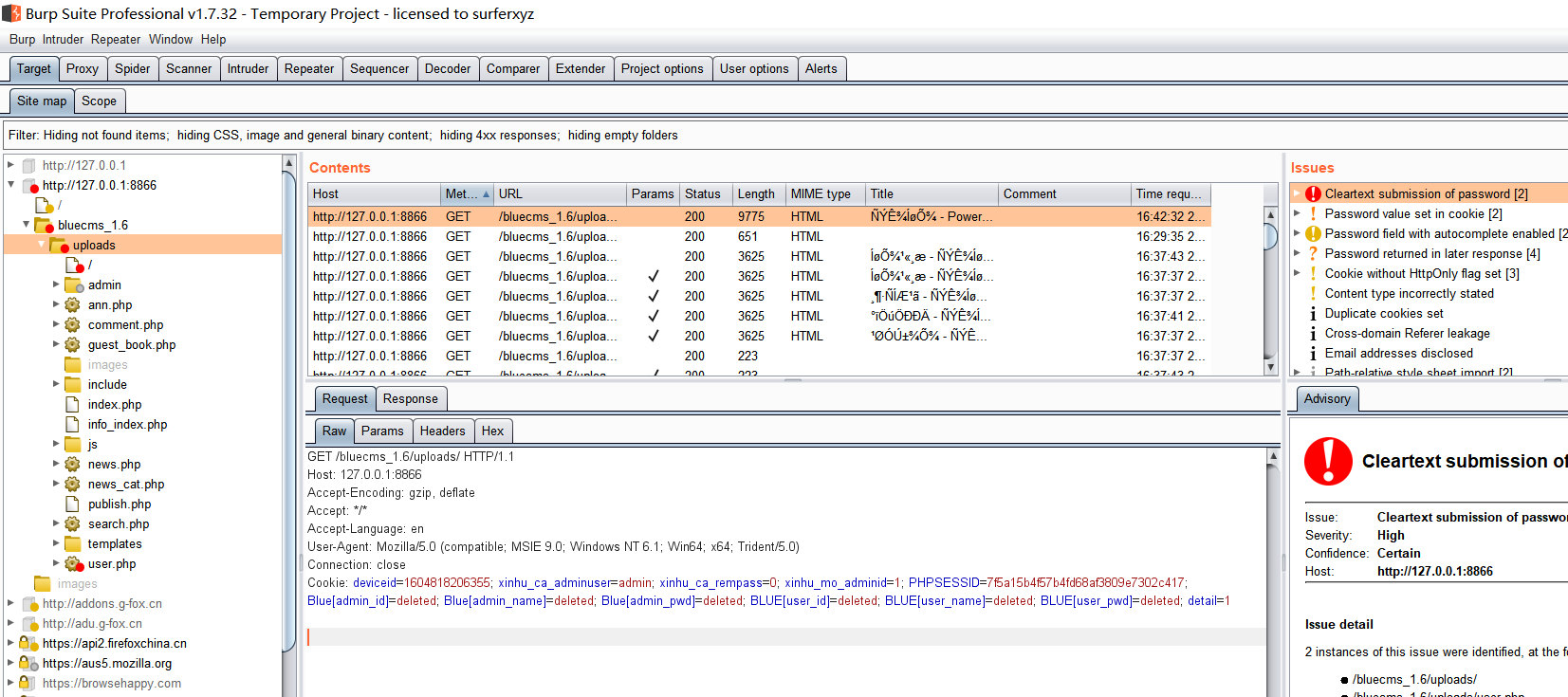


一共有两个漏洞

* 1.Cookie without HttpOnly flag set（没有设置HttpOnly标志的Cookie）
* 2.HTML uses unrecognized charset（HTML使用无法识别的字符集）

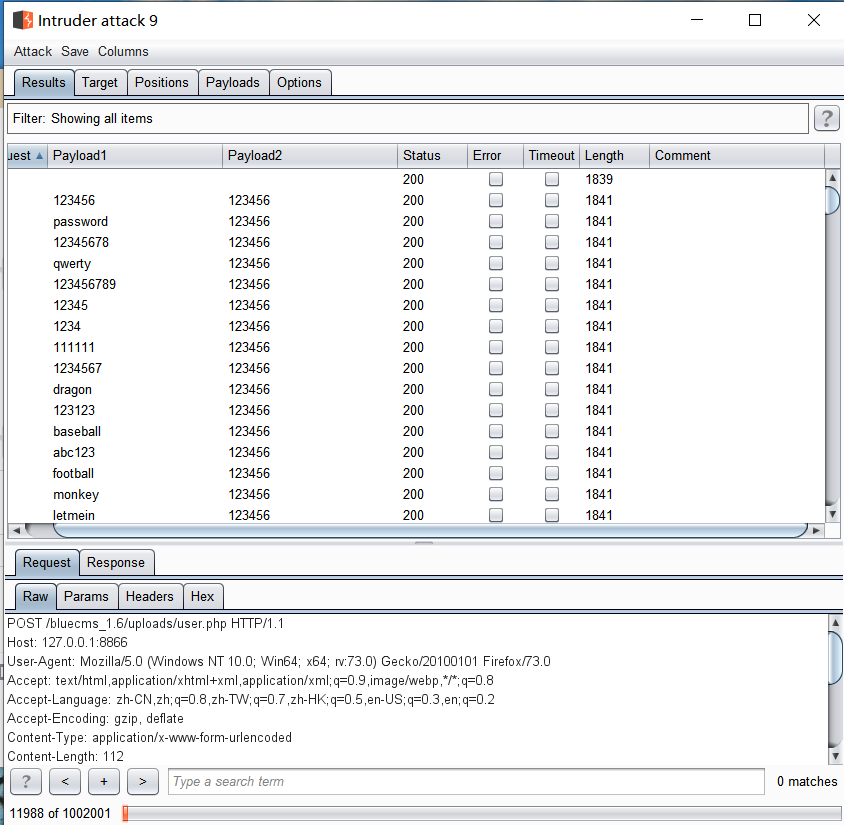
# 爬取网站：

爬取出的目录结构如下：



# 自动化攻击：

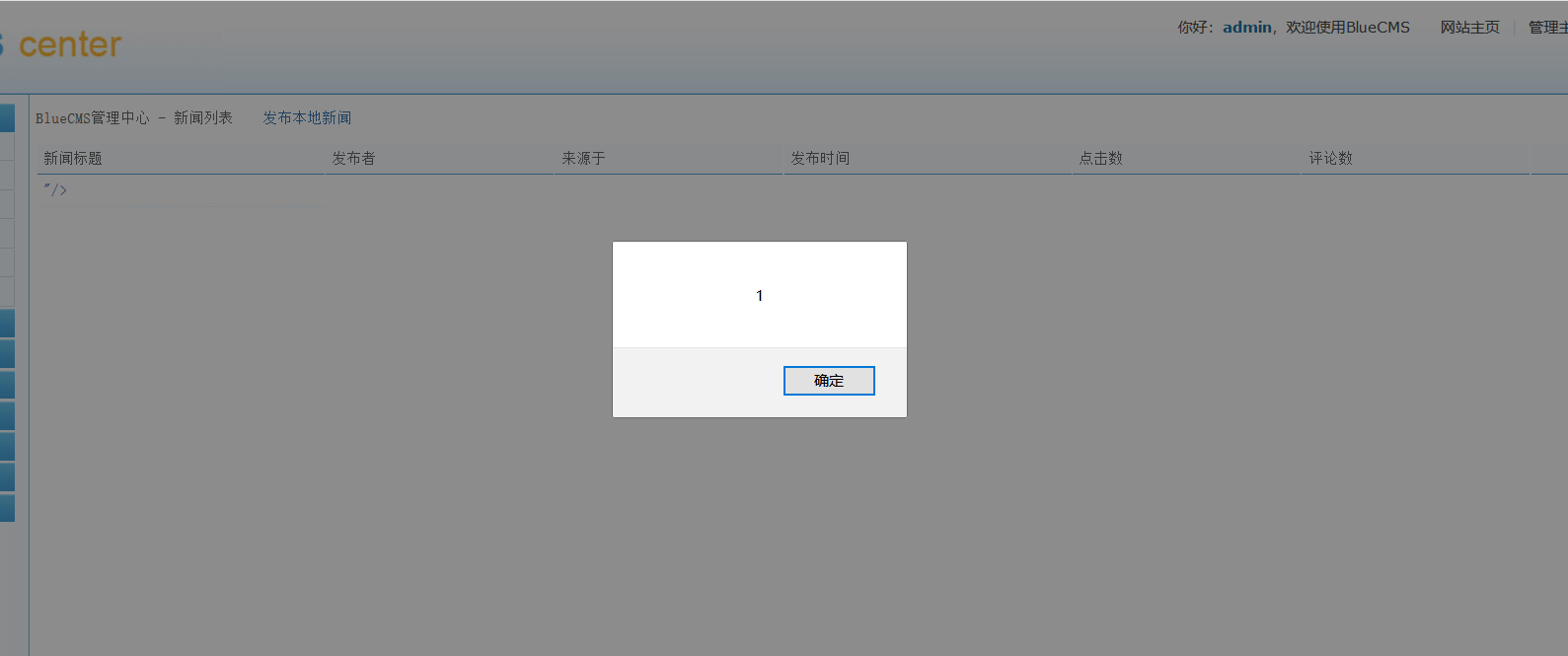
在前台登录界面，进行密码爆破，找了一个密码字典，采用cluster bomb

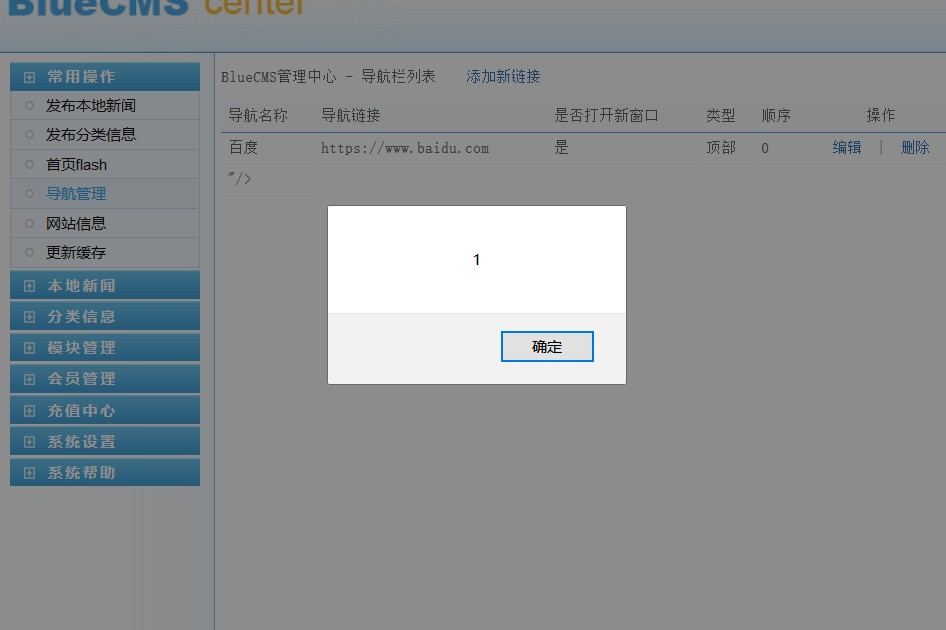


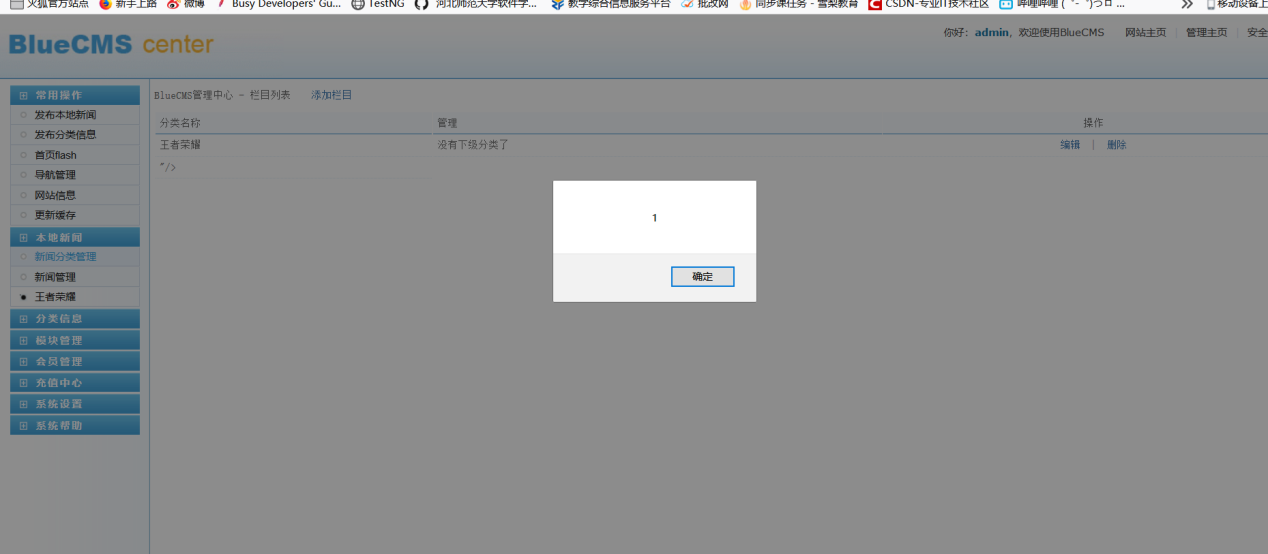
# 手工测试

1.拿前台和后台登陆⻚⾯测试，⼿动输⼊了⼀些常⻅数据库的sql注⼊语句，都没有成功登陆，所以不存在sql注入。

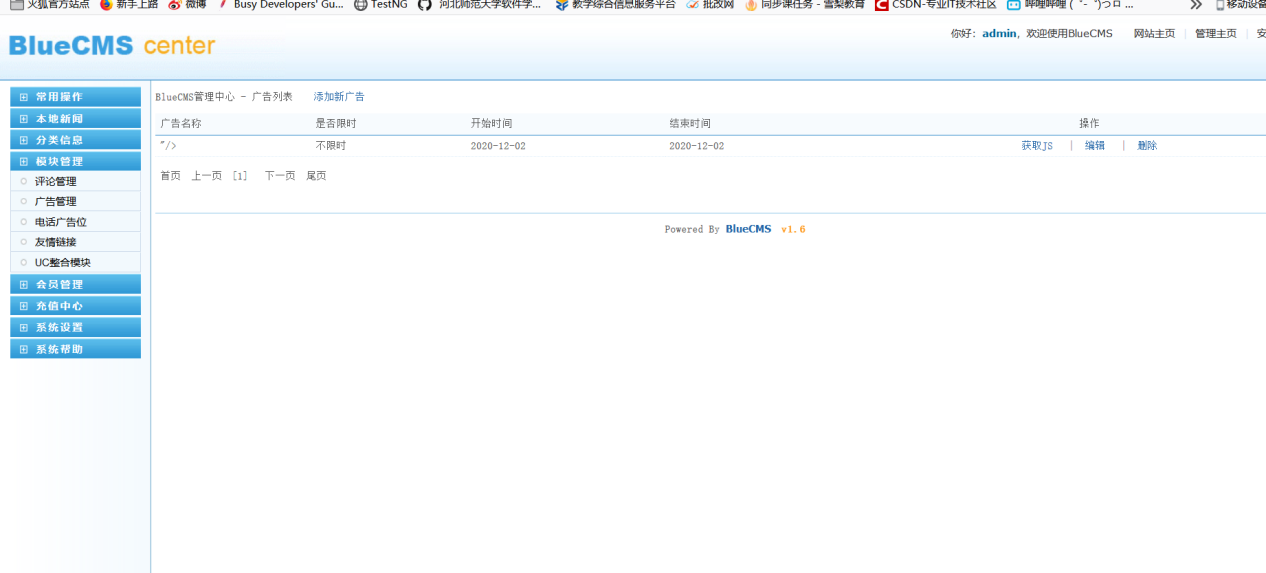
2.后台发布新闻，存在反射性xss漏洞。



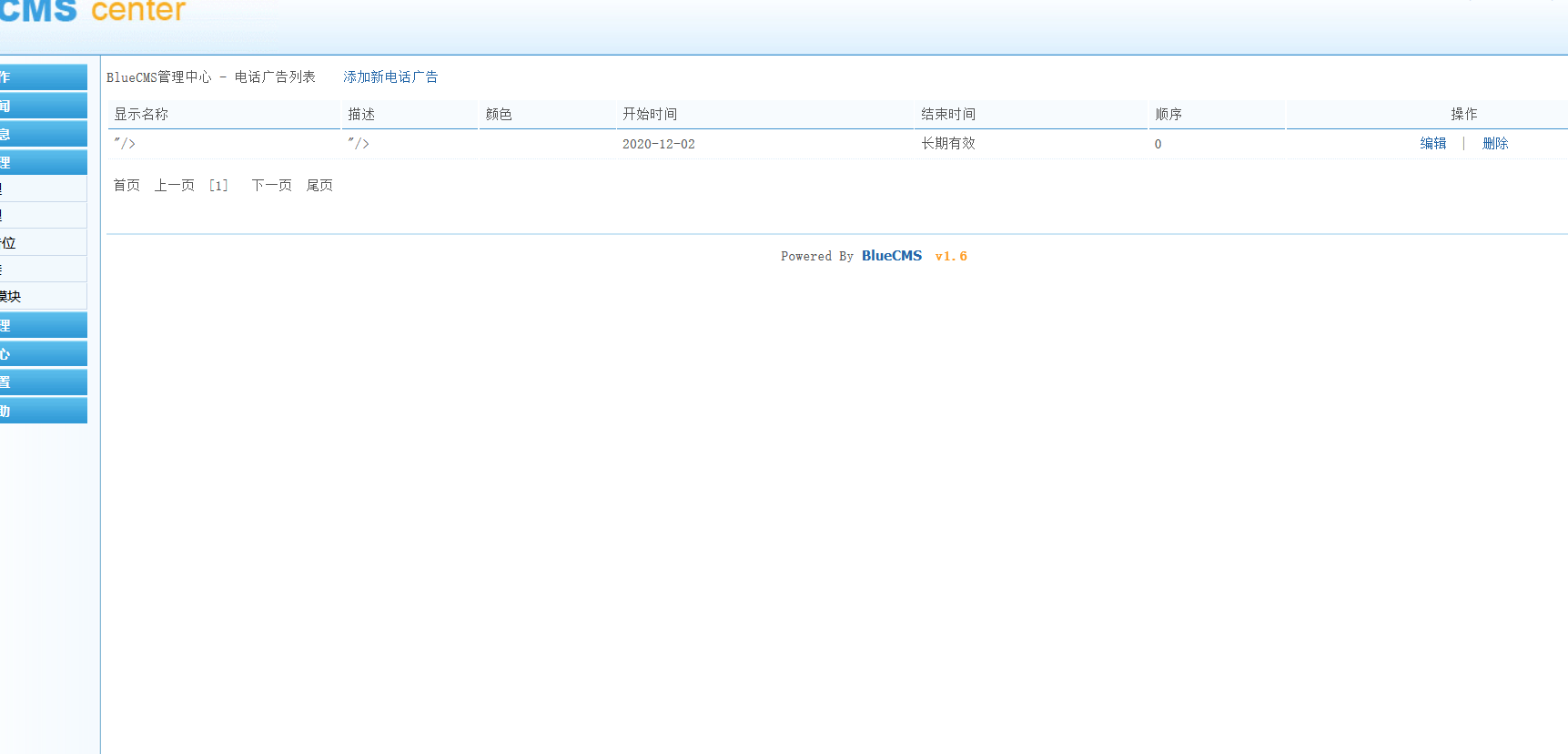
1. 后台导航管理的添加新链接，存在存储型xss漏洞，每当打开这个界面，都会弹出弹窗。
2. 后台本地新闻里的新闻分类管理，添加栏目里输入js脚本，存在存储型xss漏洞，每次打开这个界面，都会弹出弹窗。



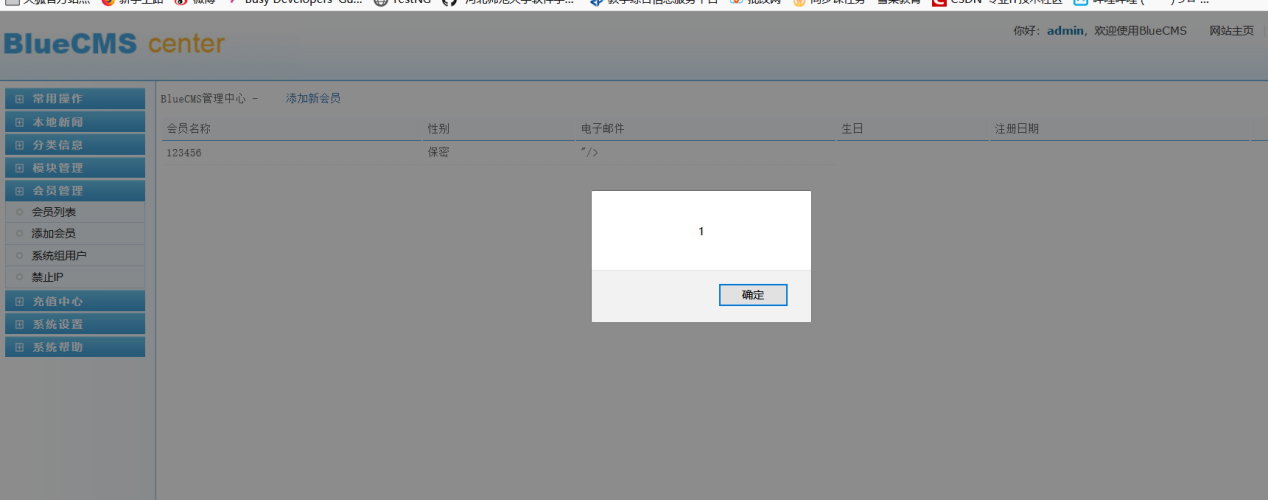
1. 5.后台，广告管理，添加新广告，存在存储型xss漏洞，每次打开这个界面，都会弹出弹窗。



6.后台，电话广告位理，添加新电话广告，存在存储型xss漏洞，每次打开这个界面，都会弹出弹窗。



7.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。



8.系统里的站点设置，存在存在存储型xss漏洞，每次打开这个界面，都会弹出弹窗。

