目录

**测试目的1**

**测试范围4**

**数据来源1**

**测试工具1**

Dirbuster目录扫描2

Zenmap端口号扫描2

Burspuite 抓包2

SqlmapSQL注入2

人工检测2

**最终发现漏洞1**

人工检测漏洞2

分类信息3

留言板3

登录界面3

功能分类界面3

文件漏洞2

文件包含漏洞3

文件修改漏洞3

文件读取漏洞3

SQL注入漏洞2

xss漏洞2

xss跳转漏洞3

xss反射漏洞3

* 测试目的：

通过实施针对性的渗透测试，发现Bluecms网站系统的安全漏洞，保障业务系统安全运行。

## 测试范围

|  |  |
| --- | --- |
| 系统名称： | Bluecms网站 |
| 测试域名： | http://localhost/bluecms\_1.6/uploads/ |
| 测试实践： | 2021/11/22 |

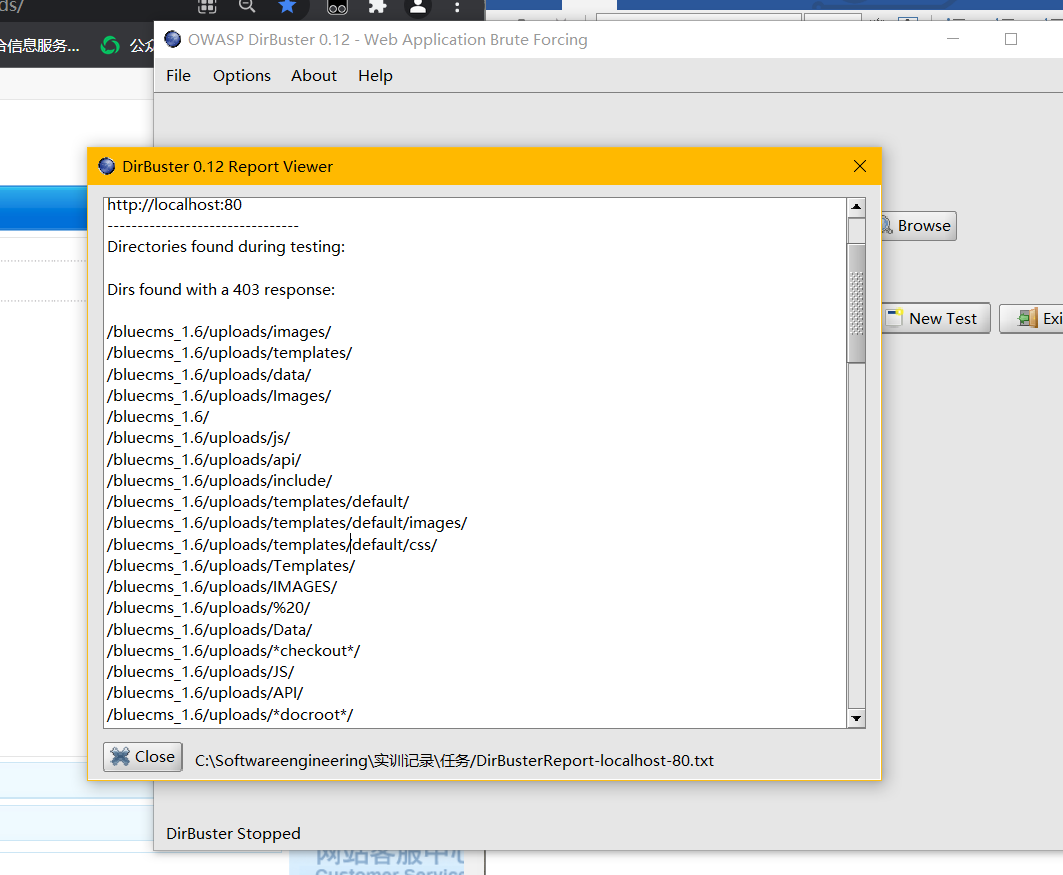
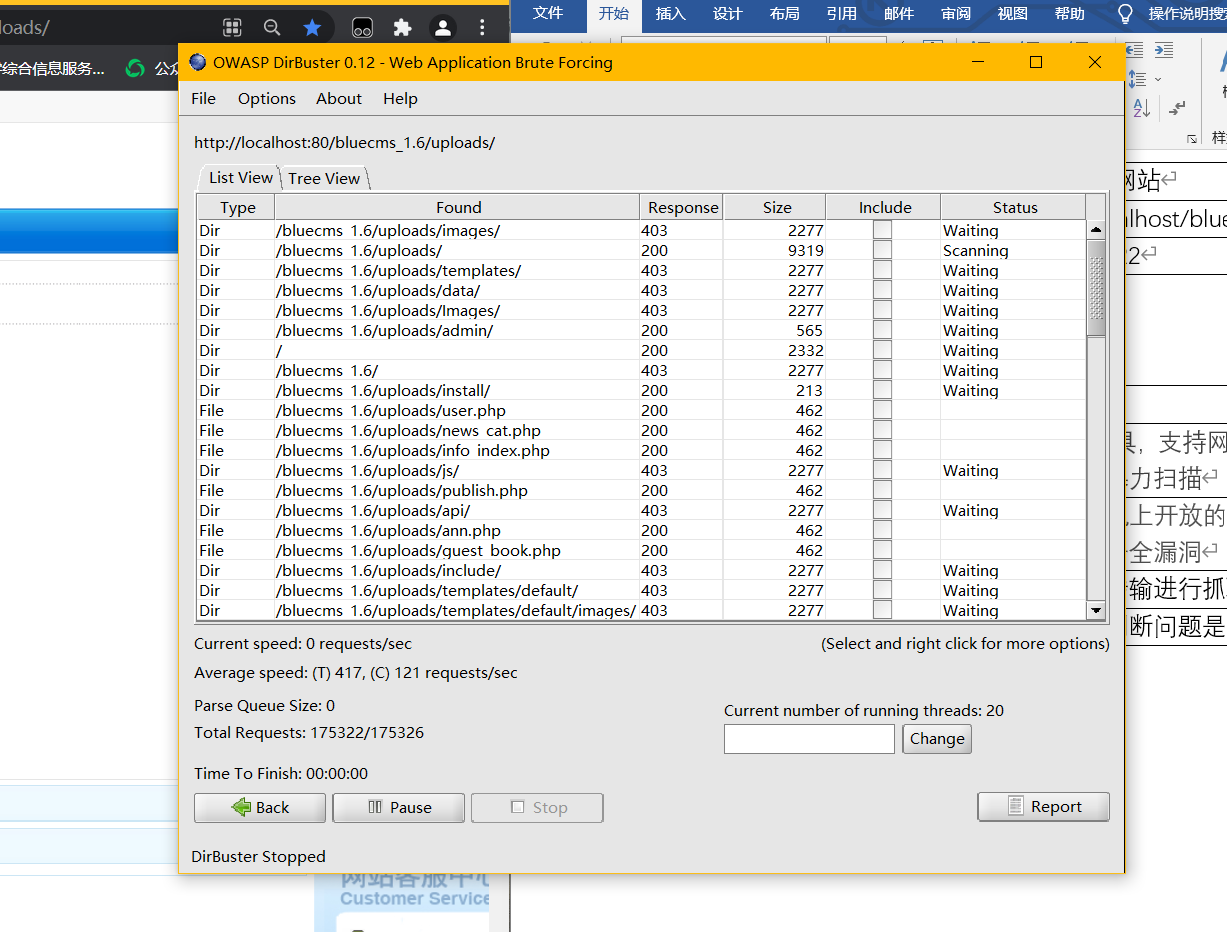
## 数据来源

通过漏洞扫描和手动点击分析获取相关数据

## 测试工具

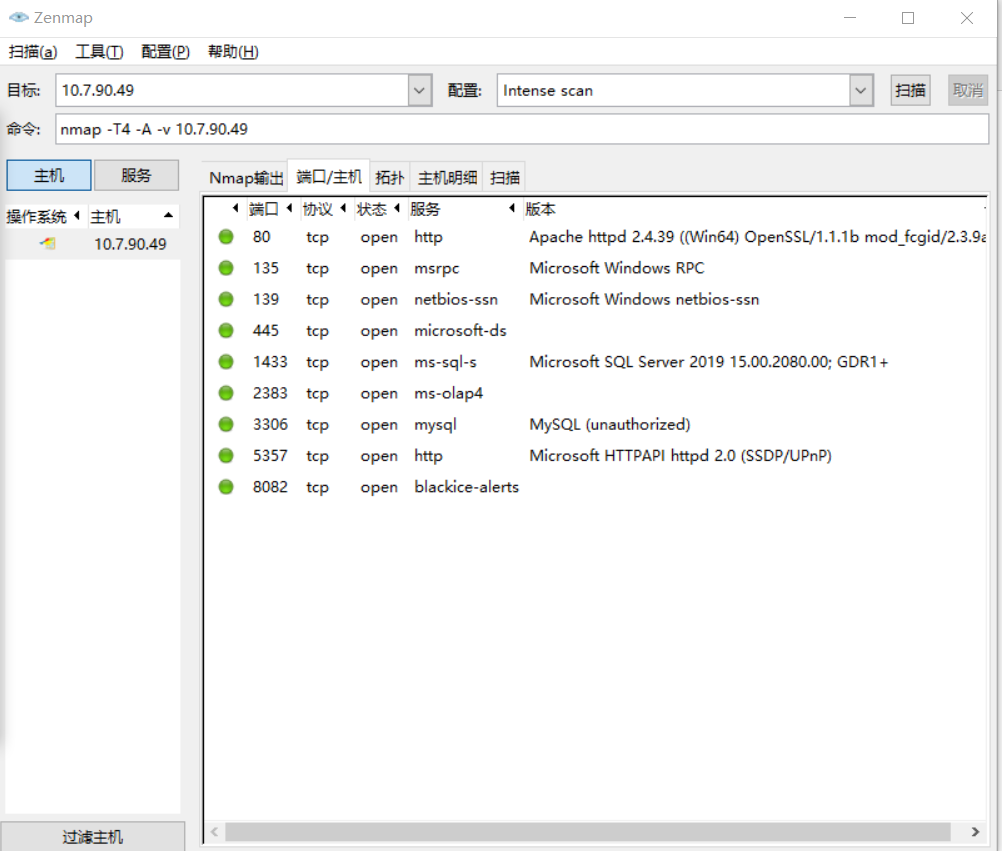
|  |  |
| --- | --- |
| 测试工具 | 用途和说明 |
| Dirbuster | 使用Java语言编写的目录扫描工具，支持网页爬虫方式扫描，也支持基于字典暴力扫描，还支持纯暴力扫描 |
| Zenmap | 检测活在网络上的主机、检测主机上开放的端口、检测到相应的端口的软件和版本以及扫描端口的安全漏洞 |
| Burspuite | 网络抓包工具，对网络的数据包传输进行抓取 |
| Sqlmap | 判断检测页面中get,post参数,cookie,http头，对xss漏洞进行检测 |

### Dirbuster目录扫描

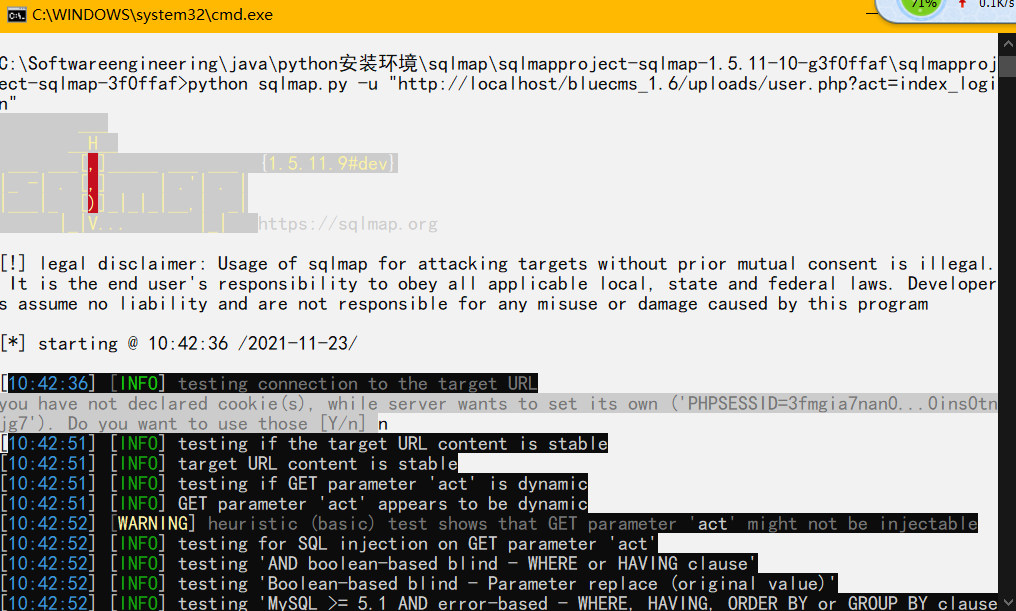


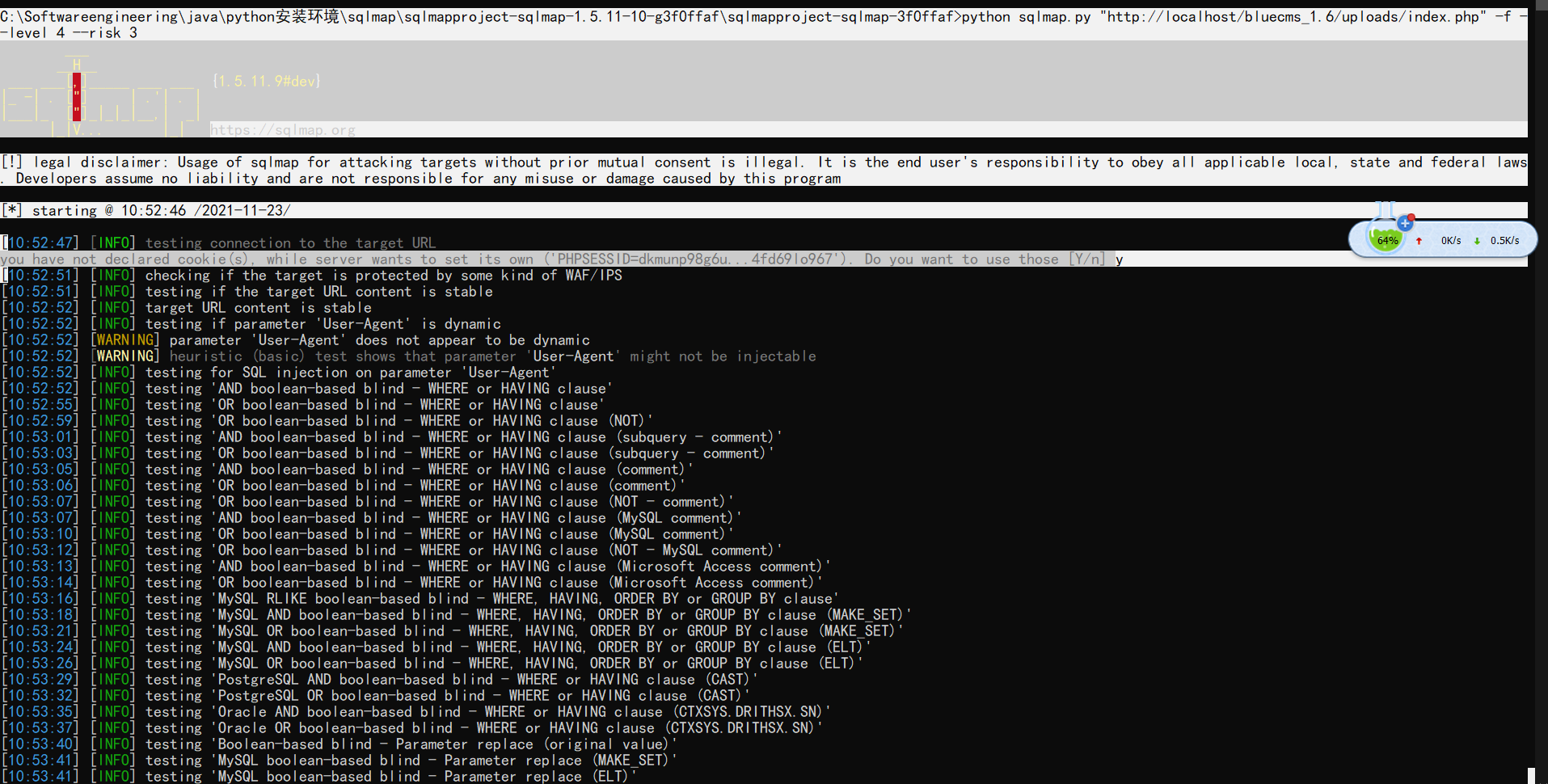
### Zenmap端口扫描

扫描本机的主机号，查看端口

### Sqlmap，对网站进行风险评估等级





## 最终发现的漏洞：

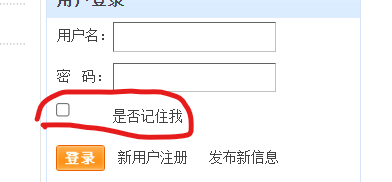
* 人工检测漏洞：
* ①．分类信息页面，搜索地址界面，复选框无法进行选择



* ②．留言板部分，在留言框中输入信息后，点击发表按钮，依然按照未留言的状态弹出提示。



* ③首页用户登录处，单选框与文本未对齐



* ④．副业的功能分类界面的首页上一页下一页均为文字，无法点击实现跳转



# 文件漏洞：

### 1. 文件包含漏洞

user.php文件包含函数存在可控变量，存在文件包含漏洞，act参数为pay值，这包含相应文件，其中pay参数没有过滤

elseif ($act == 'pay'){

include 'data/pay.cache.php';

$price = $\_POST['price'];

$id = $\_POST['id'];

$name = $\_POST['name'];

if (empty($\_POST['pay'])) {

showmsg('对不起，您没有选择支付方式');

}

include 'include/payment/'.$\_POST['pay']."/index.php";

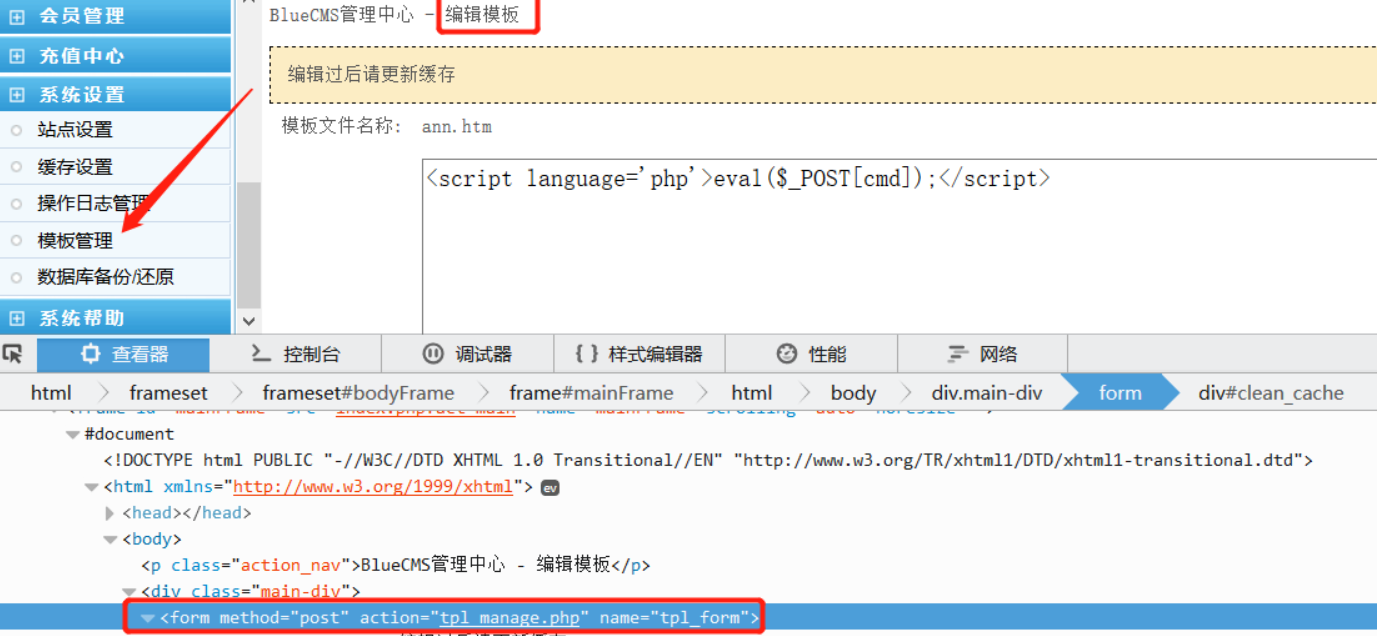
}

漏洞位置：



* 2．文件修改漏洞：使用sqlmap爆破得到用户名和密码：admin/qweasd123，登陆进入后台，这里是不可以写入一句话的，需要找到后台的php文件，写入一句话提交，在源码中进

行行查找，发现存在后台模板文件修改处的验证不严格，导致任意文件修改漏洞



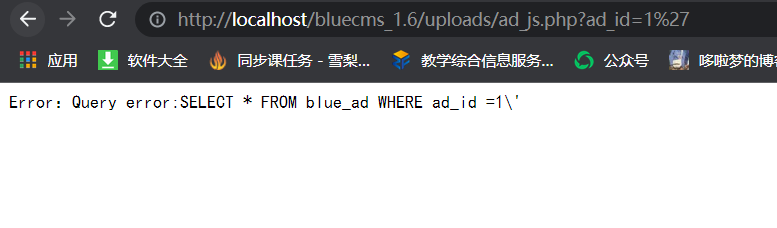
### 3．文件读取漏洞

用户登录的代码里面的函数的变量可以任意的更改，burp suite抓包测试，发现可以抓取网站根目录下的任意文件

## SQL注入漏洞：

ad\_js.php发现数值型SQL注入漏洞

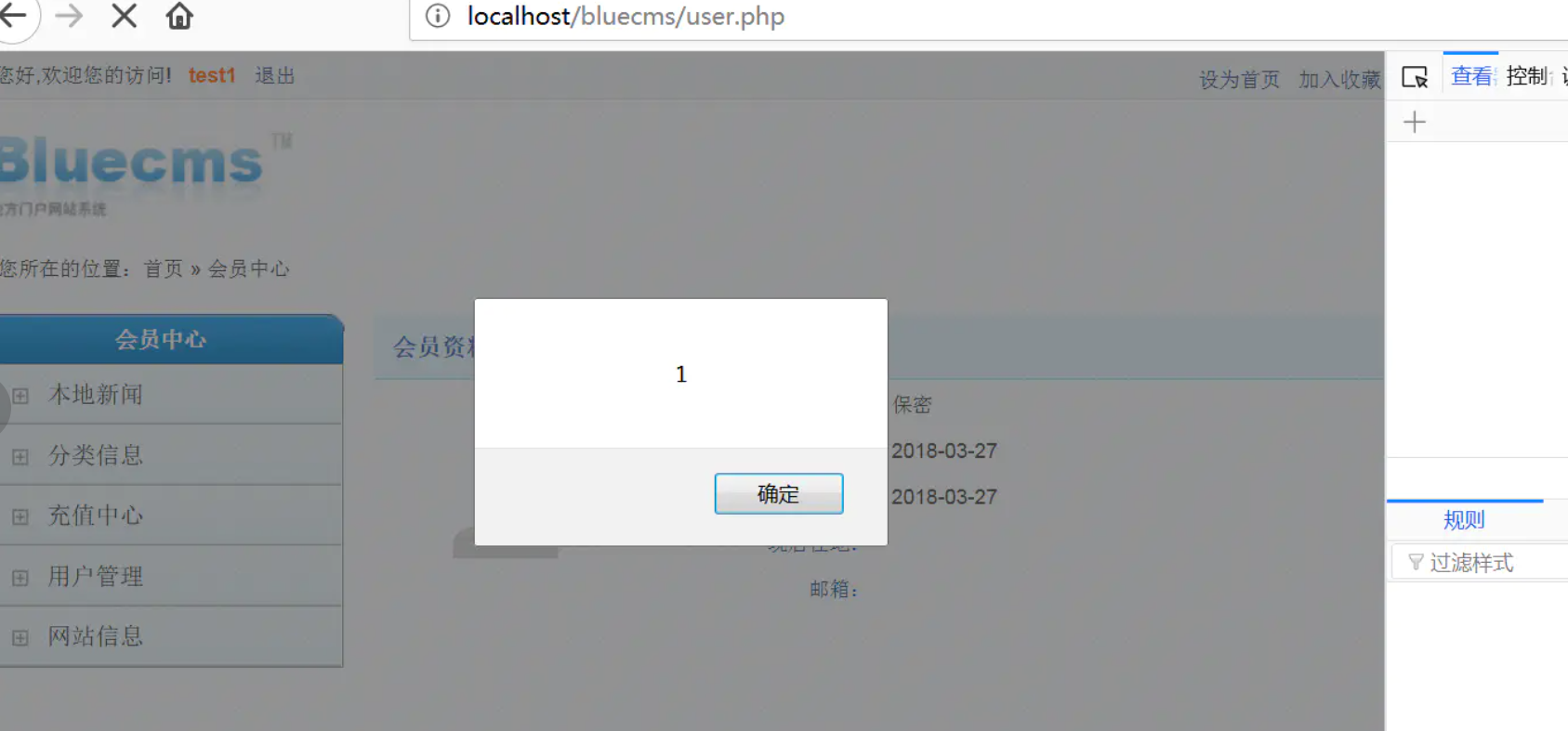
参数ad\_id可控，且没有进行过滤就进行拼接sql，尝试进行注入，测试ad\_id=1'报错



## **xss漏洞**：

### Xss存储漏洞

·在用户编辑个人资料的时候，在电子邮件的地址栏输入代码<script>alert(王岩渗透测试)</script>,就会直接提交到数据库里，后台管理进入后台后会直接弹窗，以至于用户伪造管理员进入后台，随意窜覆盖数据。



### xss反射漏洞

进入user.php中的时候，几乎是同时获取$act和$from的值，然后判断$act的值，来进行相应的操作。但是当$act的值为’reg‘，也就是注册的时候，他会将$from的值渲染到浏览器上，导致了反射型XSS

