**渗透测试测试报告**

目录

[测试目的 1](#_Toc88834135)

[测试范围 1](#_Toc88834136)

[信息收集 2](#_Toc88834137)

[Dirbuster目录扫描 2](#_Toc88834138)

[Nmap端口扫描 3](#_Toc88834139)

[漏洞扫描 3](#_Toc88834140)

[Web爬取 4](#_Toc88834141)

[手工测试发现的漏洞 4](#_Toc88834142)

[界面测试漏洞 4](#_Toc88834143)

[功能测试漏洞 5](#_Toc88834144)

[文件漏洞 5](#_Toc88834145)

[文件包含漏洞 5](#_Toc88834146)

[文件读取漏洞 6](#_Toc88834147)

[XSS漏洞 6](#_Toc88834148)

[XSS存储漏洞 6](#_Toc88834149)

[XSS反射漏洞 7](#_Toc88834150)

[SQL注入 7](#_Toc88834151)

# 测试目的

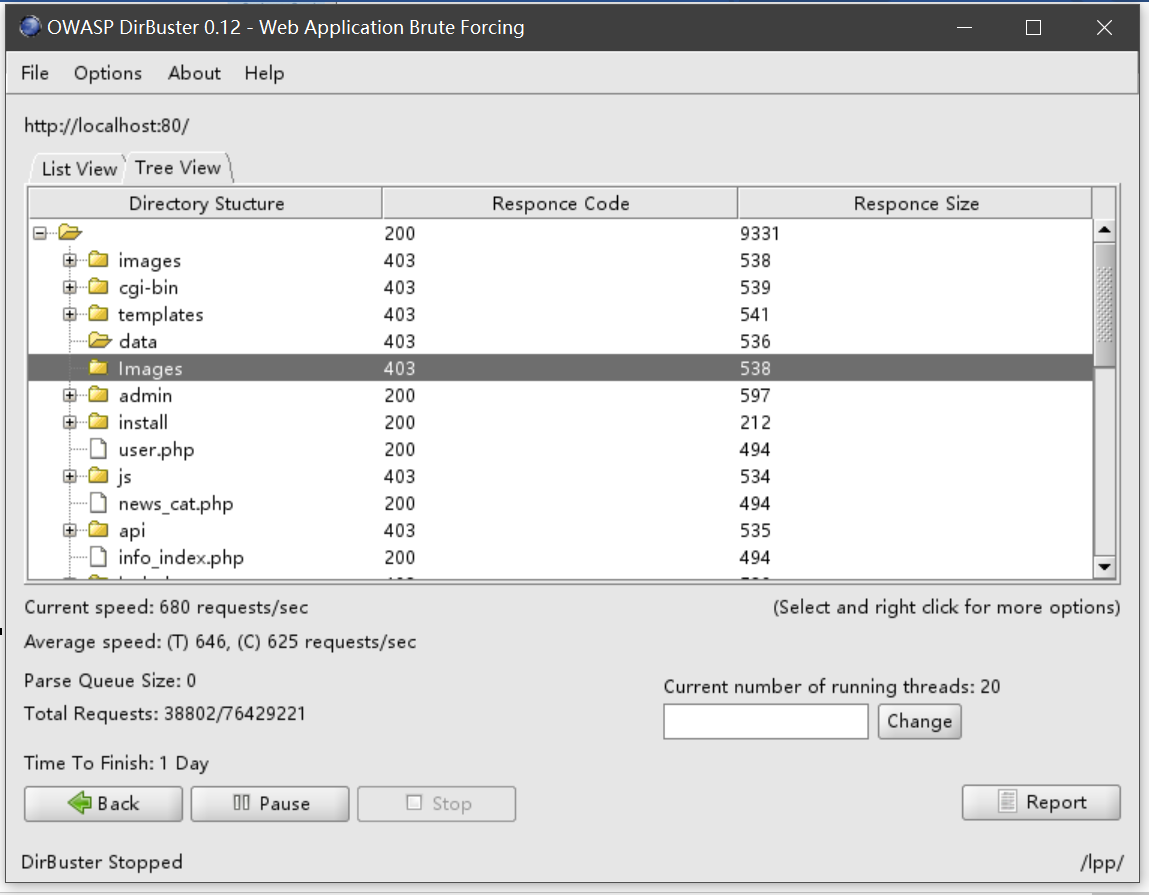
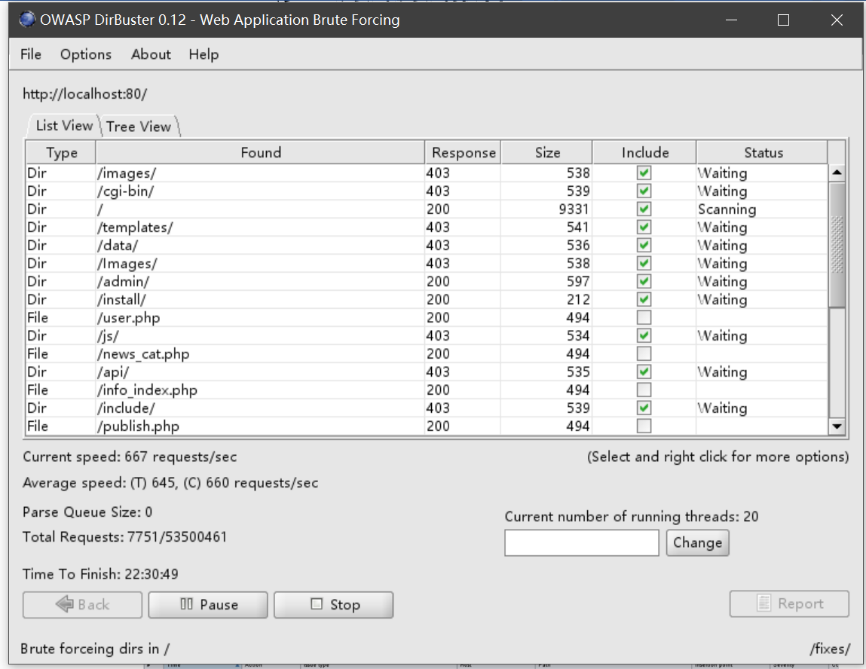
通过渗透测试，发现Bluecms网站系统的安全漏洞，确保用户的操作在安全的环境下进行。

# 测试范围

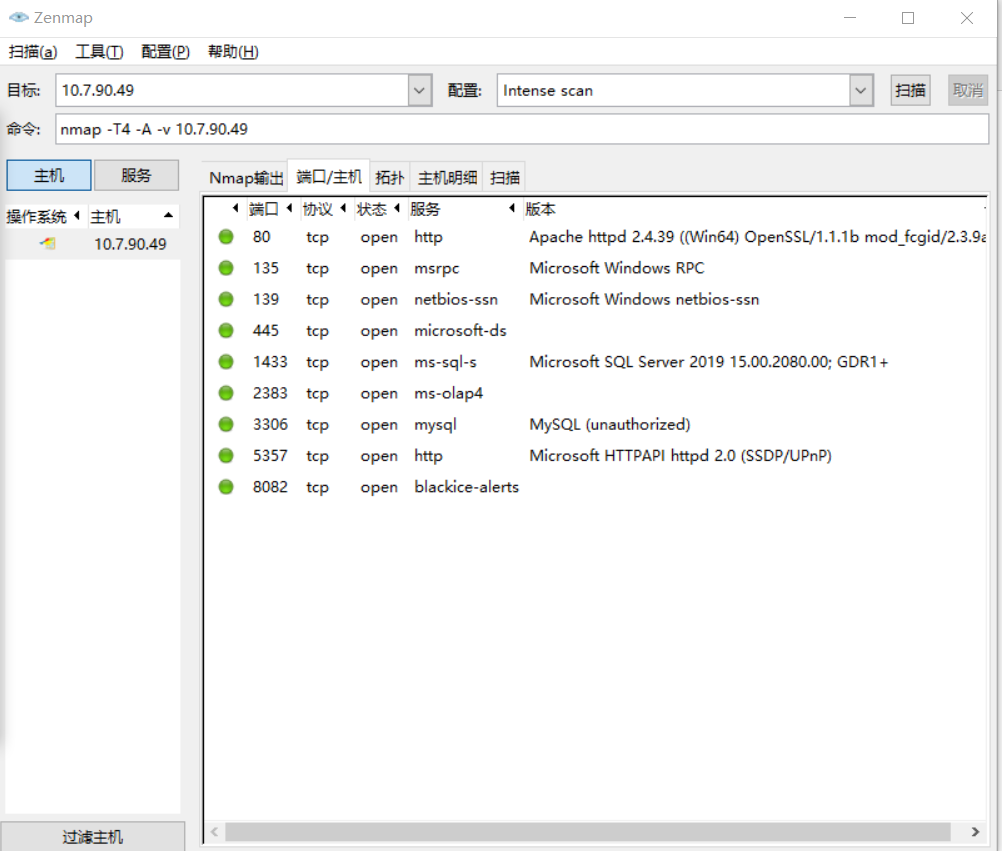
|  |  |
| --- | --- |
| 网站名称 | Bluecms网站 |
| 网址 | http://localhost/bluecms\_1.6/uploads/ |
| 测试时间 | 2021/11/24 |

# 信息收集

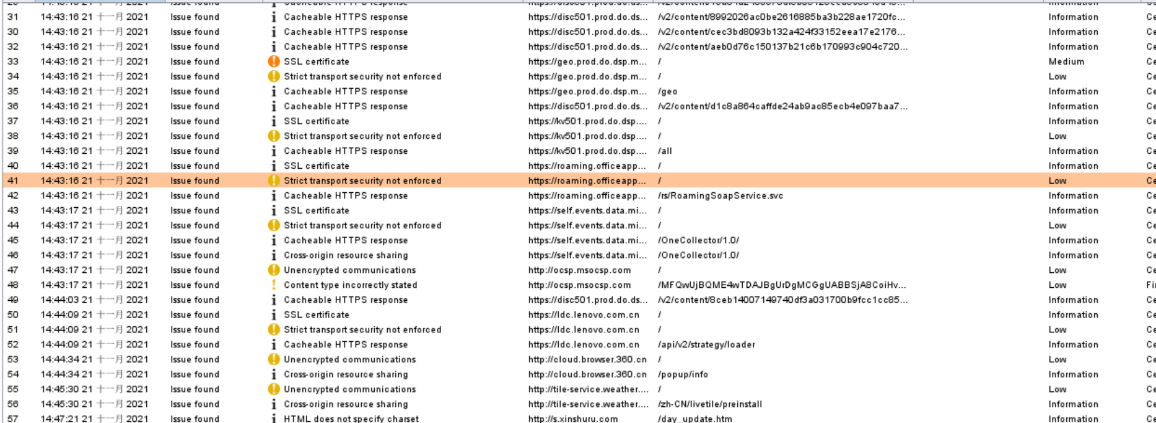
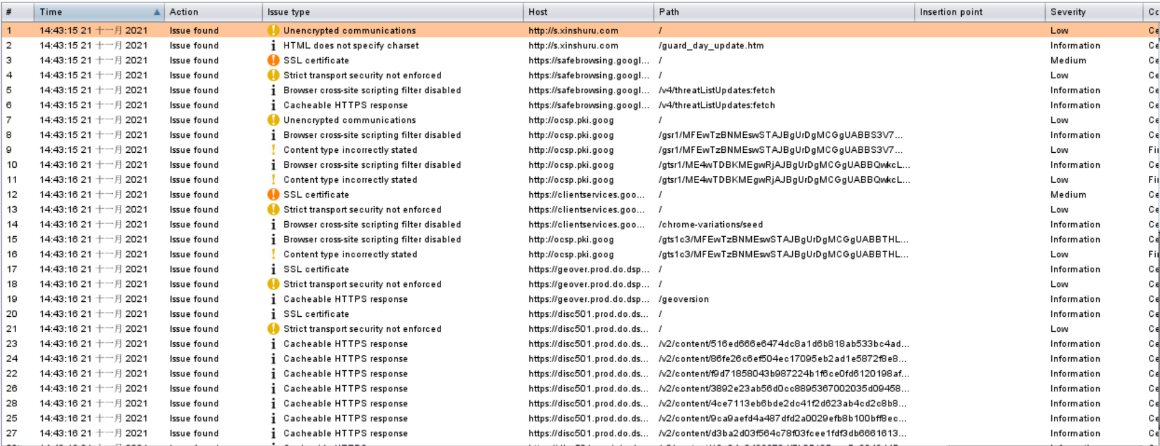
Dirbuster目录扫描

****

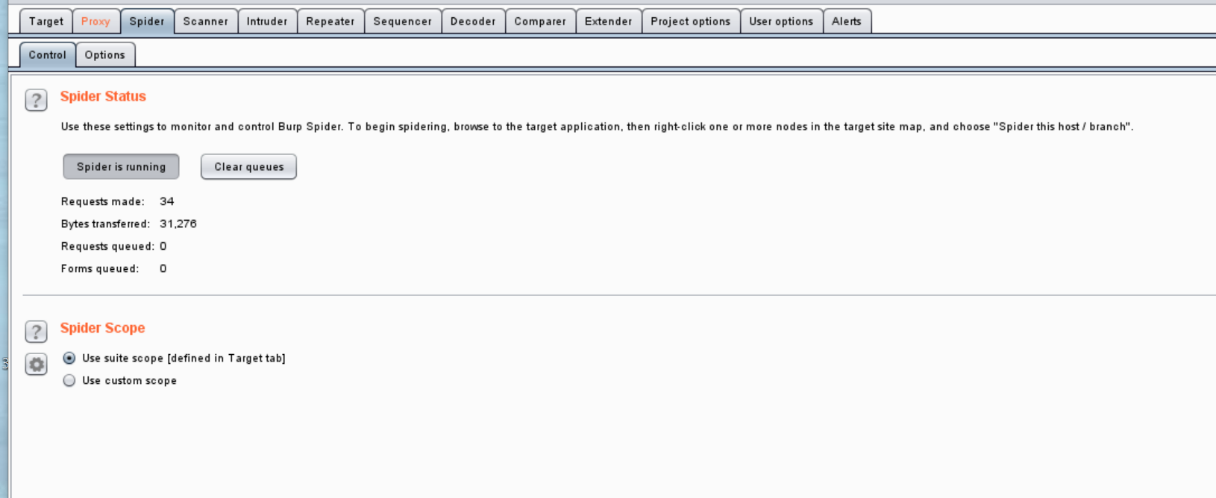
Nmap端口扫描



漏洞扫描

****

Web爬取

****

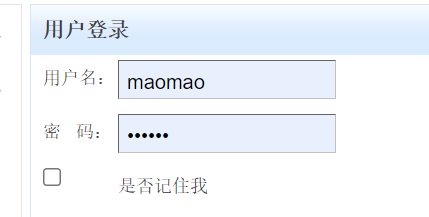
# 手工测试发现的漏洞

界面测试漏洞

没有支付方式可选择

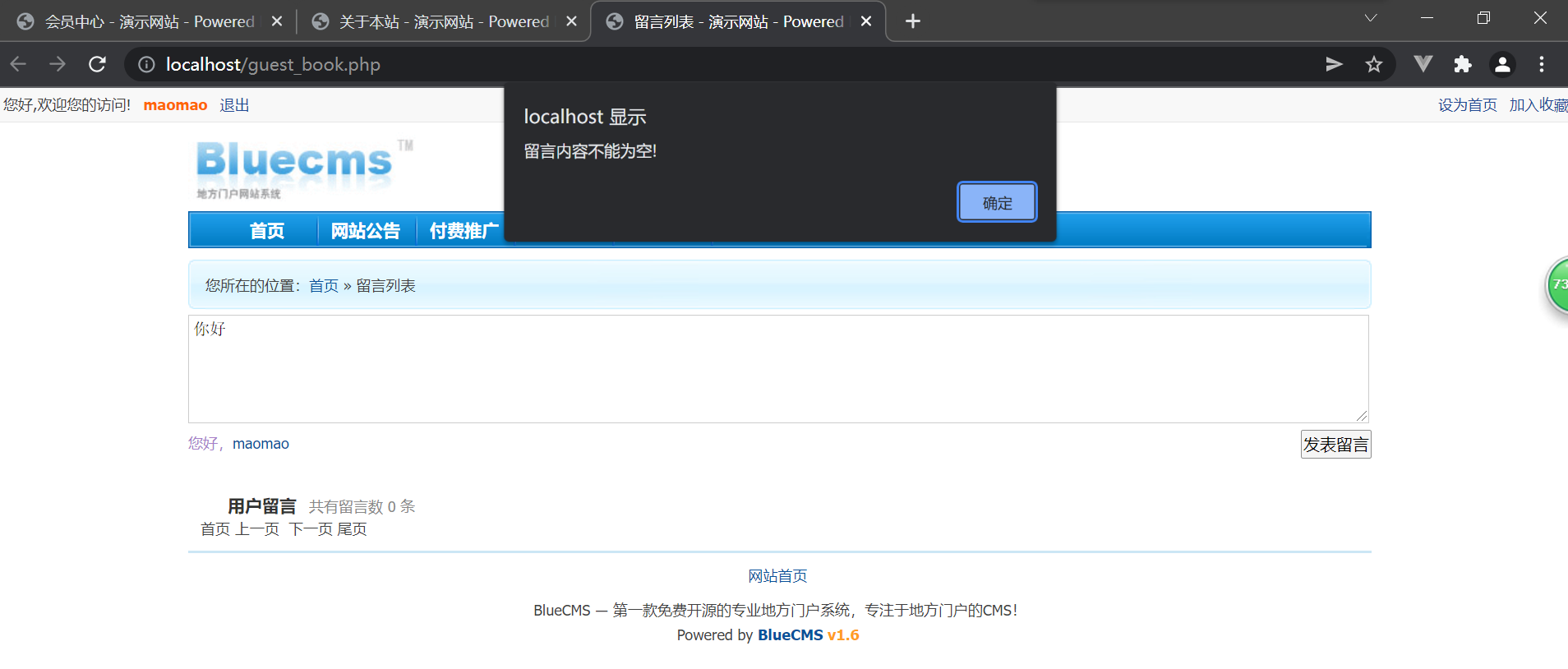


页面不整齐

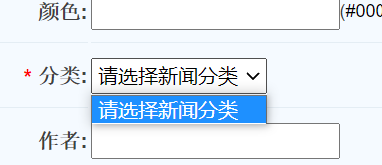


功能测试漏洞

输入内容无法识别



下拉框无法选择



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

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');

}

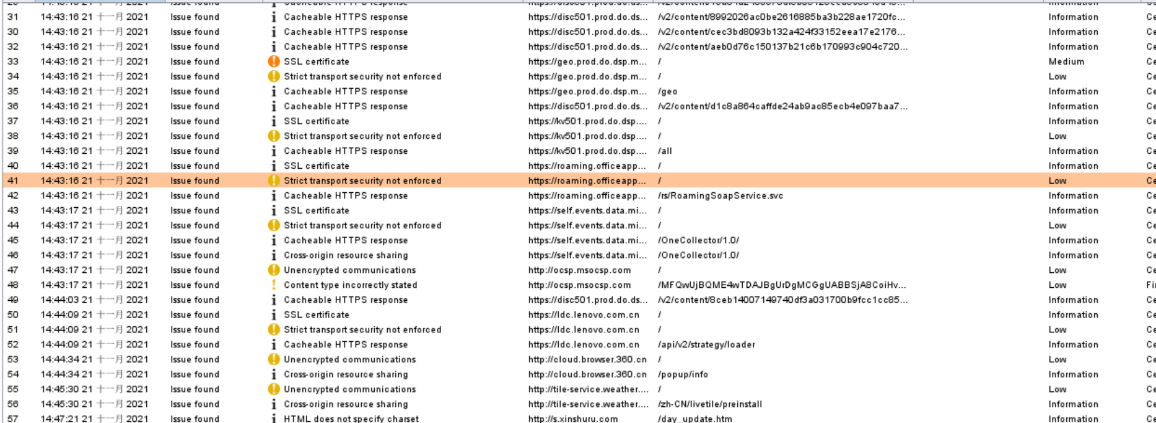
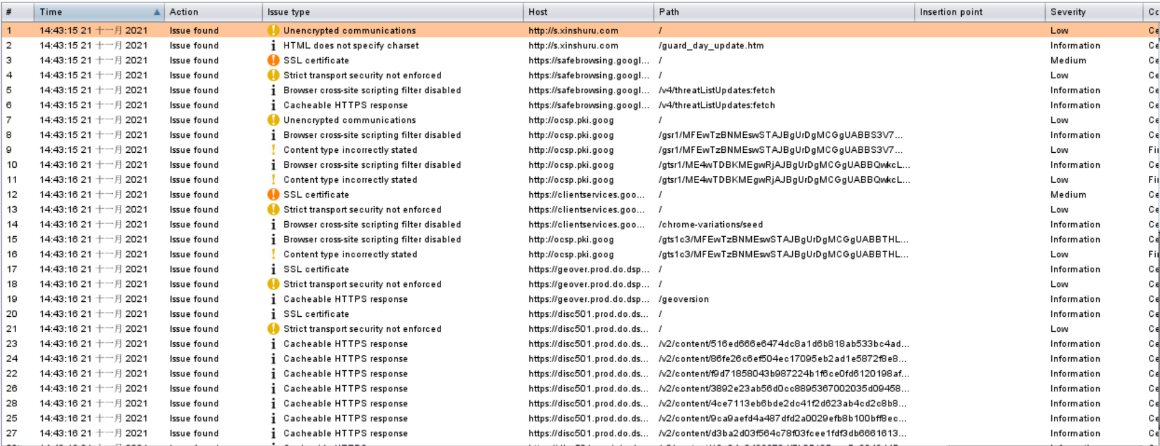
include 'include/payment/'.$\_POST['pay']."/index.php";

}

**此处漏洞对应上述界面漏洞无支付方式可选择漏洞**

文件读取漏洞

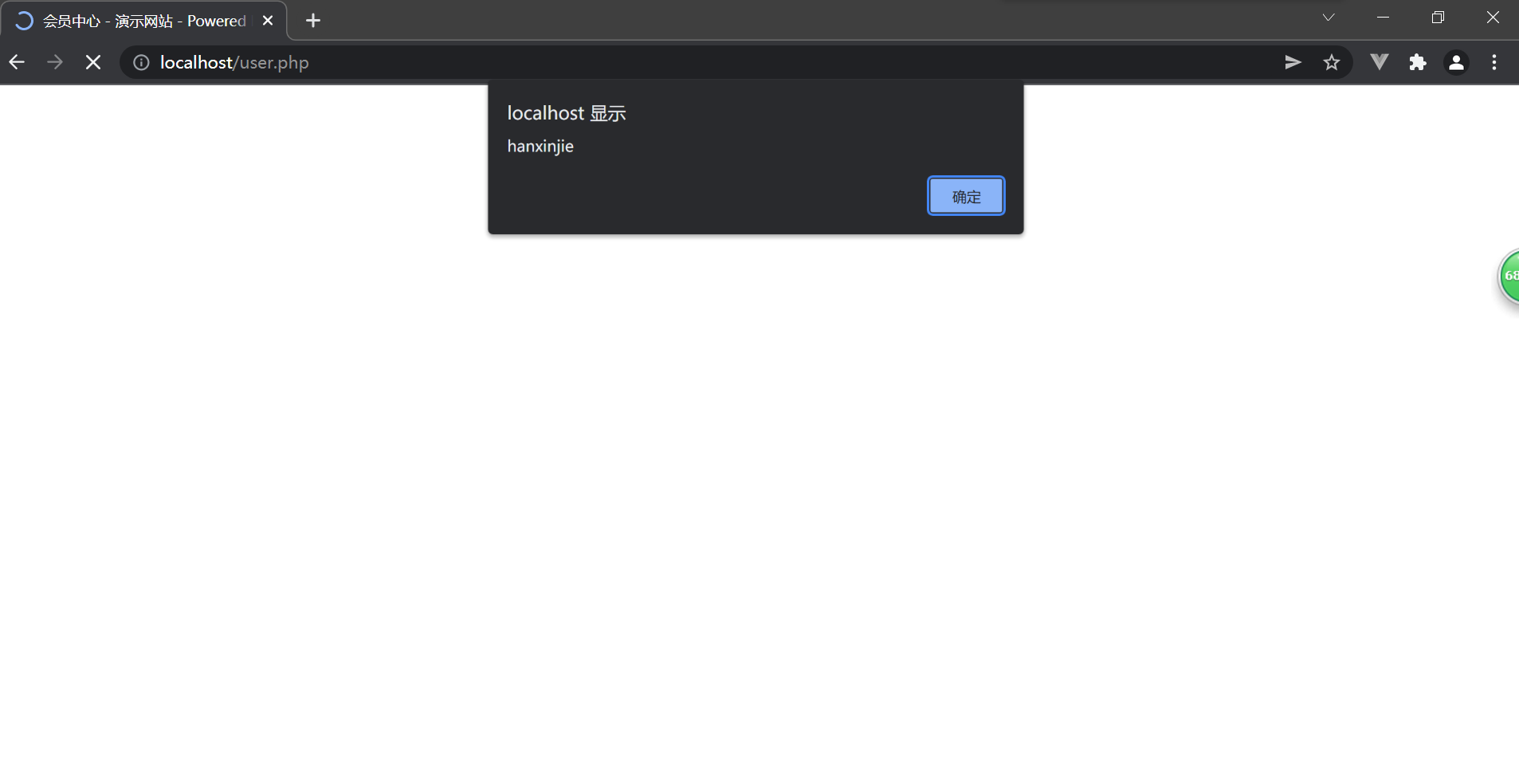
用户登录的代码里面的函数的变量可以任意的更改，burp suite抓包测试，发现可以抓取网站根目录下的任意文件

****

# XSS漏洞

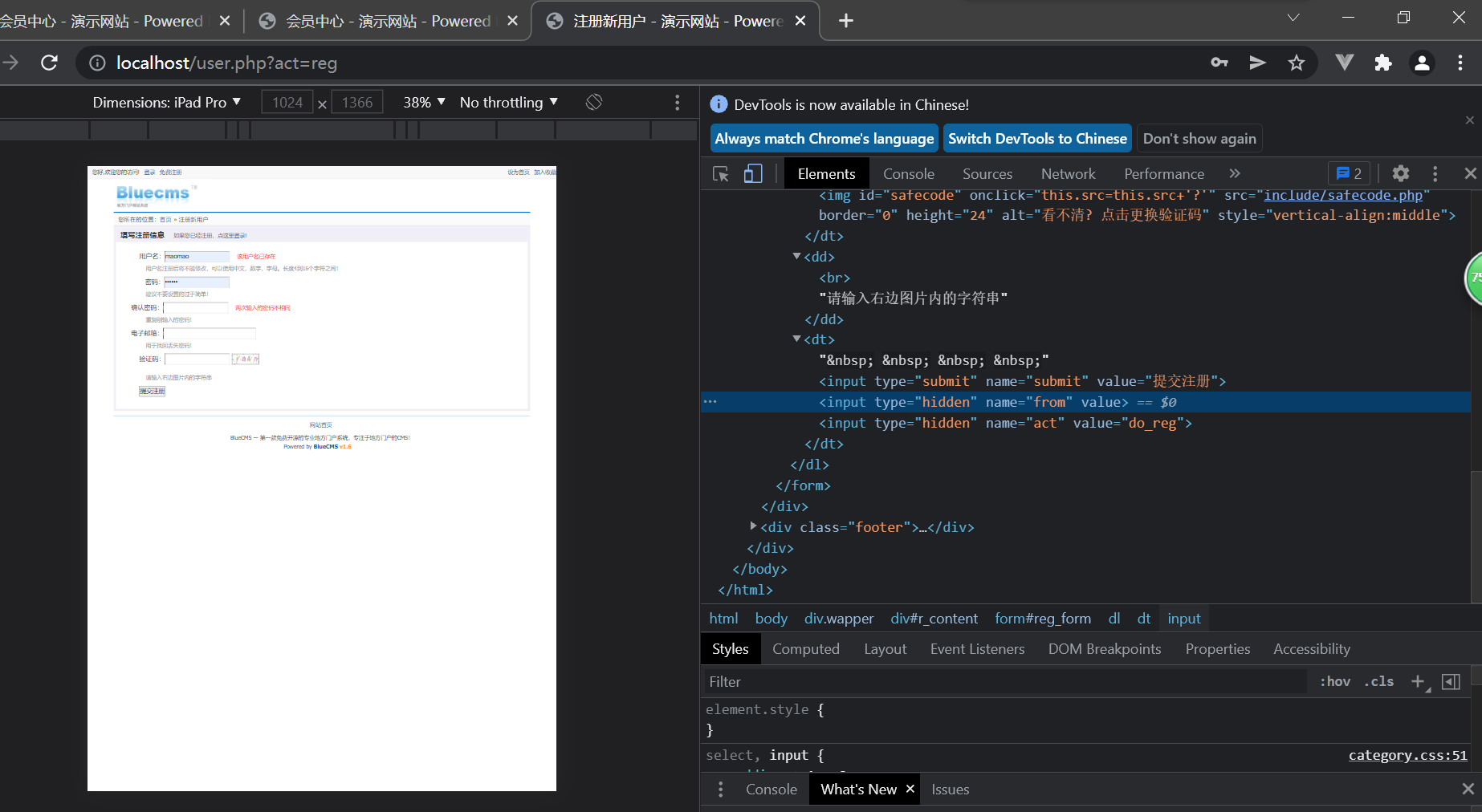
XSS存储漏洞

在修改个人信息时在邮箱处输入<script>alert("hanxinjie")</script>,系统自动存入数据库，当下次再访问时调出该信息，执行恶意脚本代码，弹出弹框hanxinjie



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

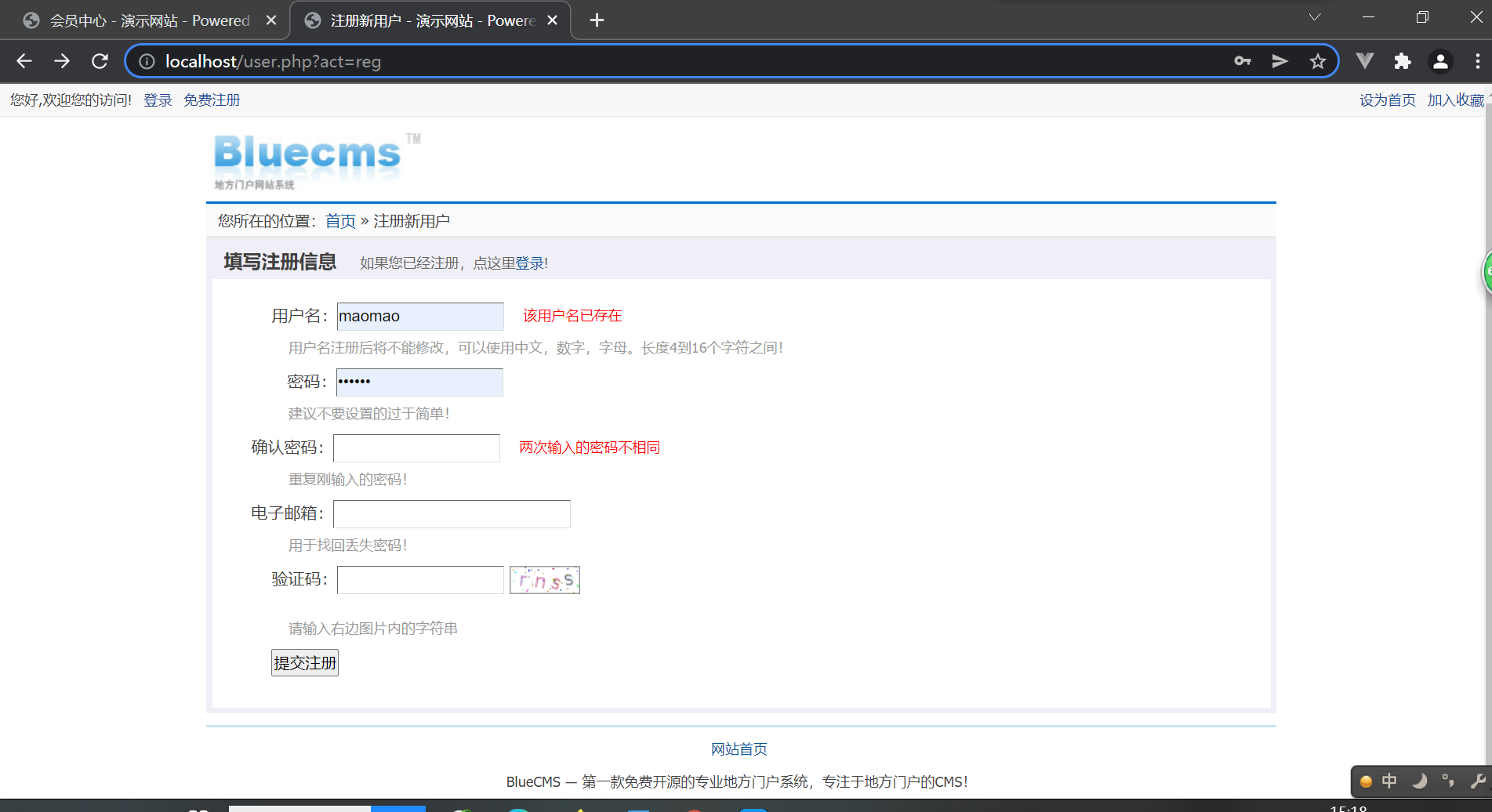


# SQL注入

user.php发现数值型SQL注入漏洞

参数act可控，且没有进行过滤就进行拼接sql

**Act=reg**



**Act=r**

