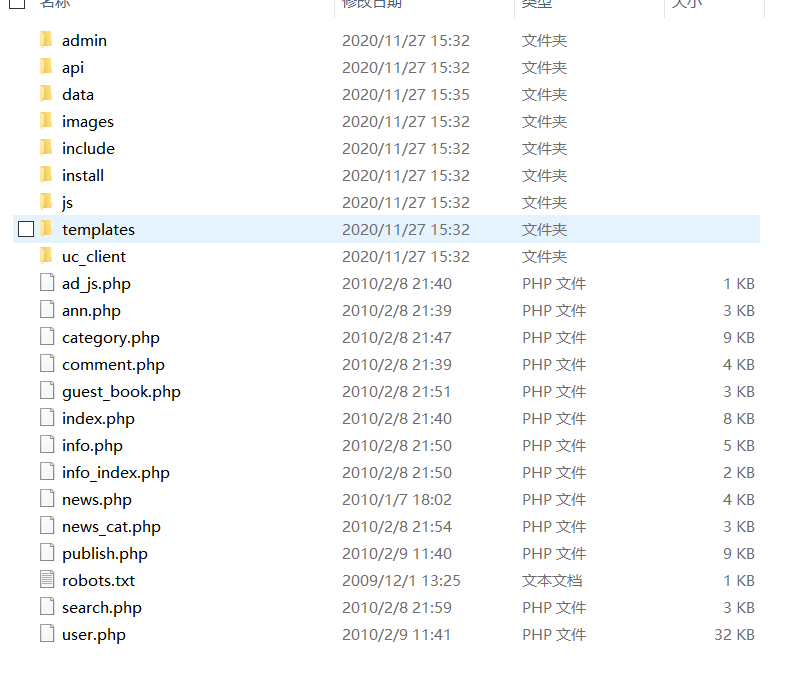
1. 信息收集

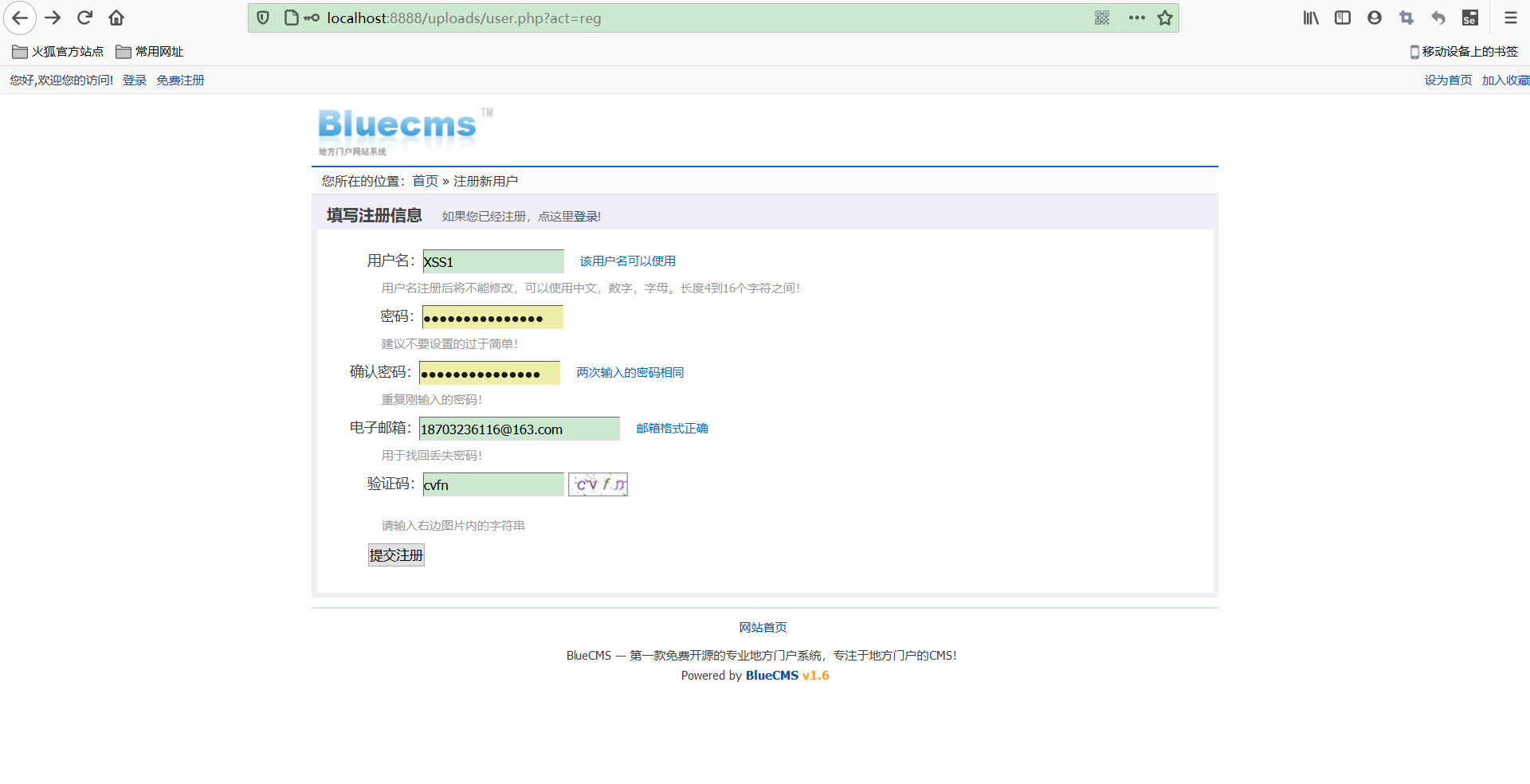
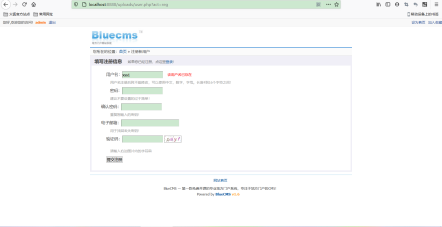
搭建的演示网站BlueCMS基于PHPstudy\_pro的本地网站

观察基本的网站结构



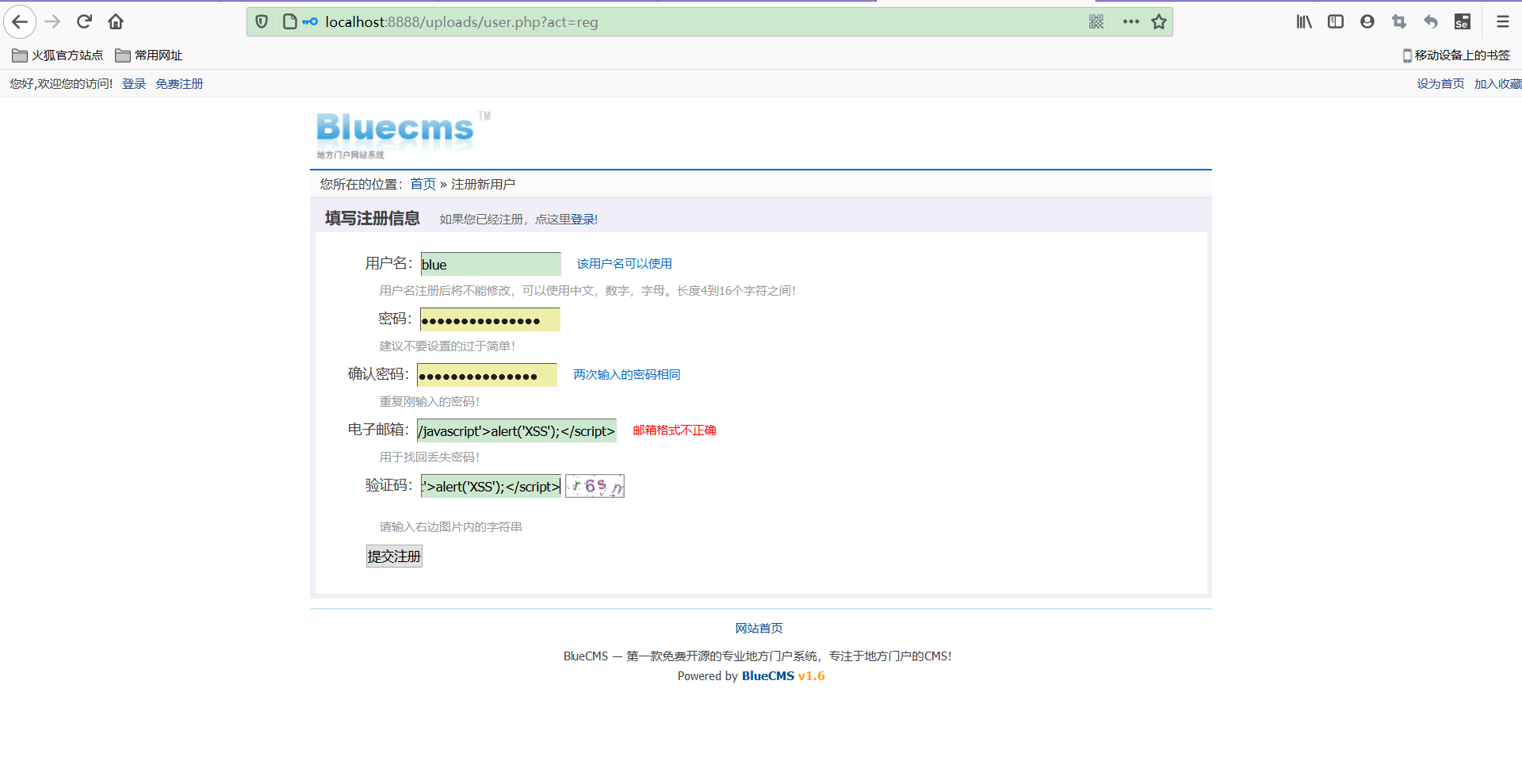
IP：（本地ip）10.7.86.246

1. 漏洞检测
2. 注册时名字不区分大小写

（2）XSS漏洞测试

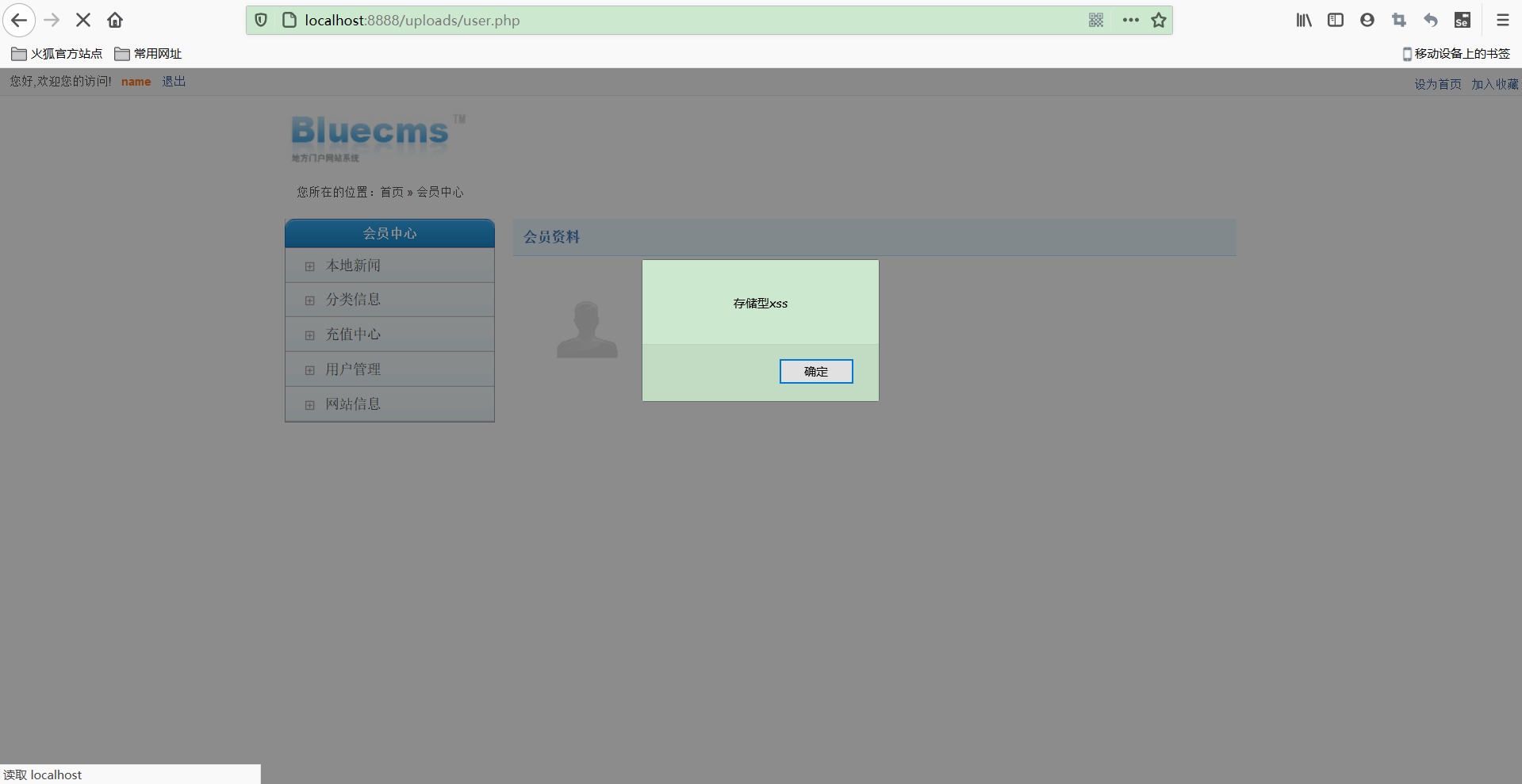
反射型XSS（注册新用户）：



当在输入框中输入<script>alert('xss')</script>时，点击提交注册并不会出现弹框，但在user.php中，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。这也就导致了反射型XSS。

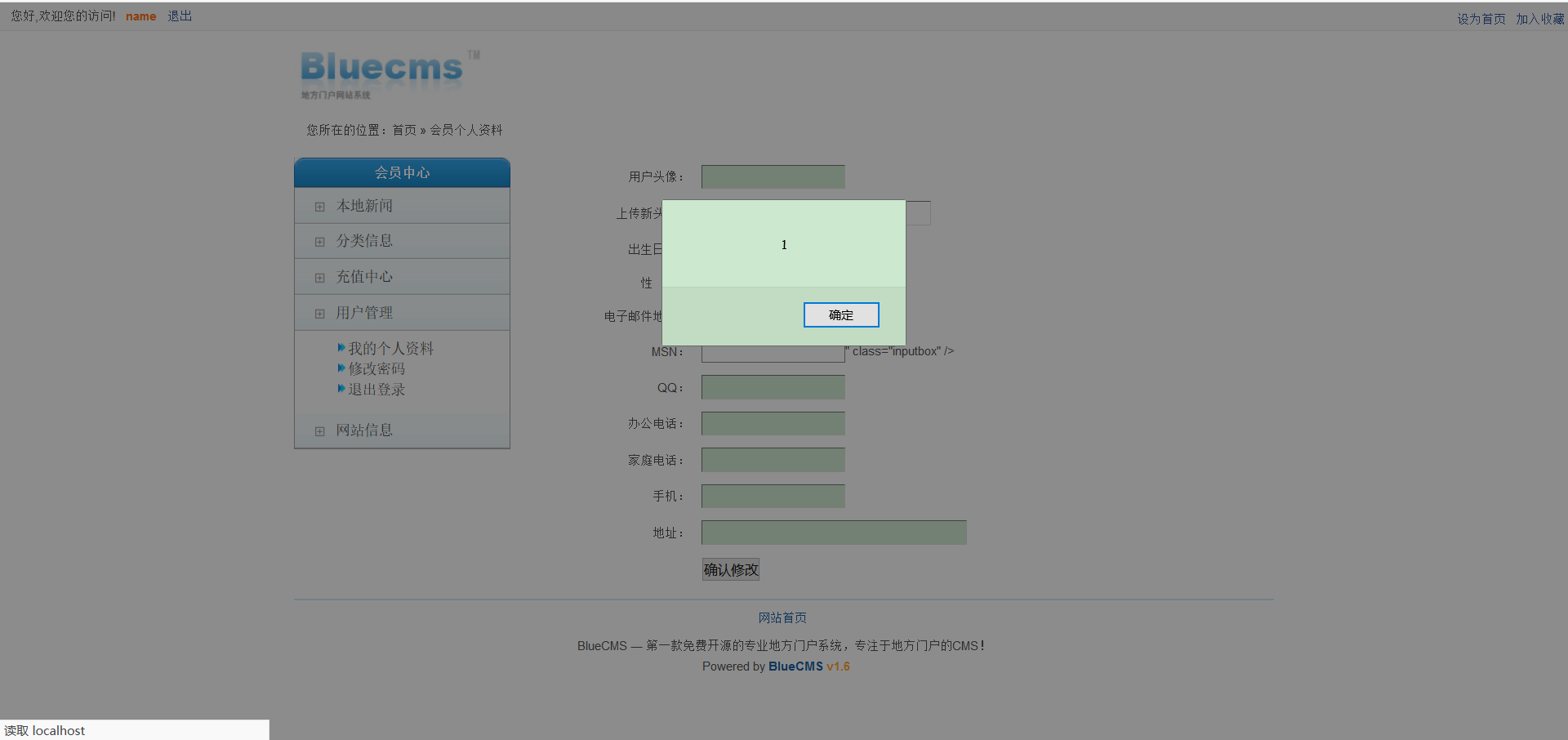
（3）存储型XSS（编辑资料）：

在电子邮件地址中填入<script>alert(‘存储型xss’)</script>，更改成功之后会出现弹框

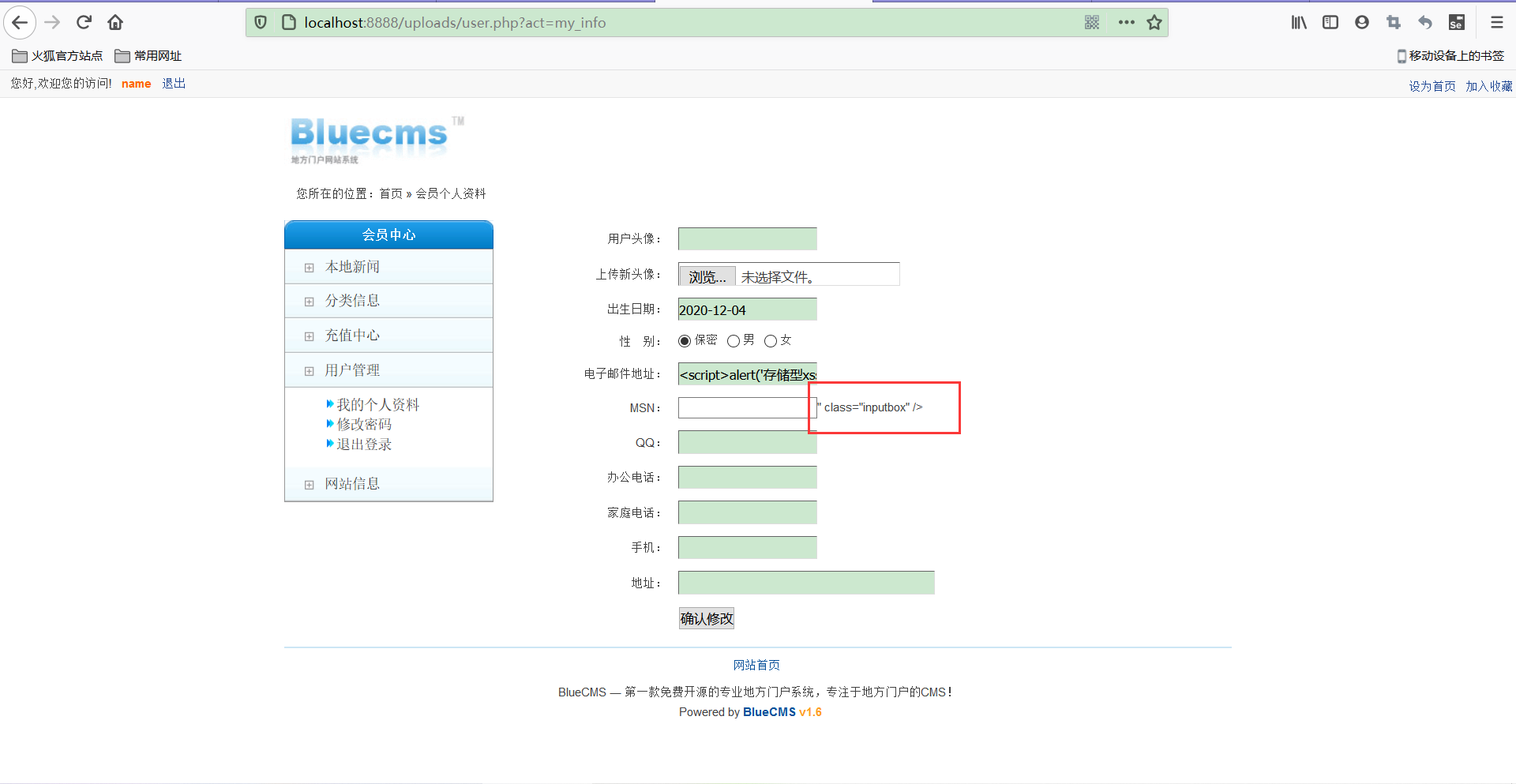
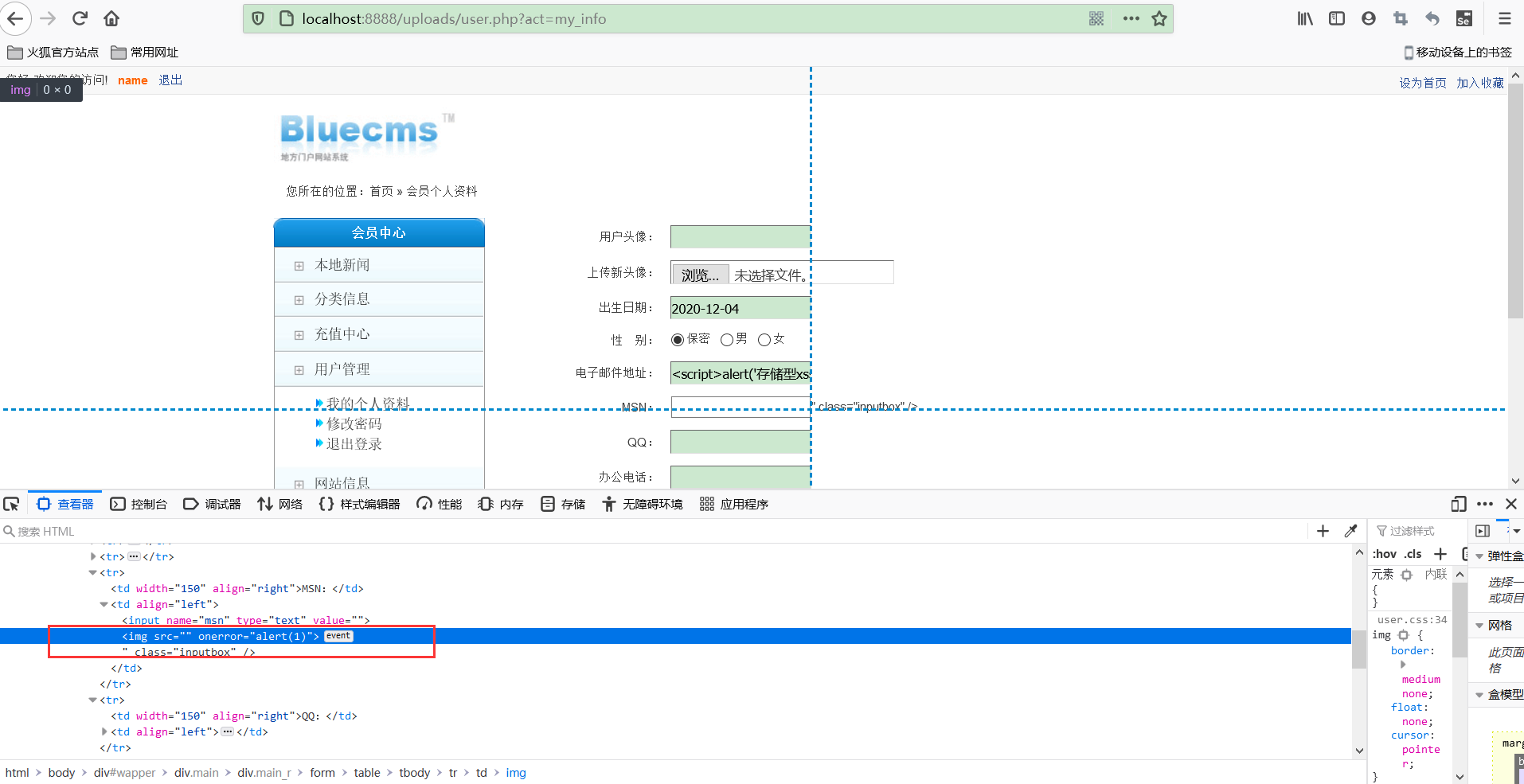
 

（4）存储型XSS（编辑资料）：

在MSN中插入"><img src='' onerror=alert(1)>，更改成功后再次点击个人信息资料会出现弹框：

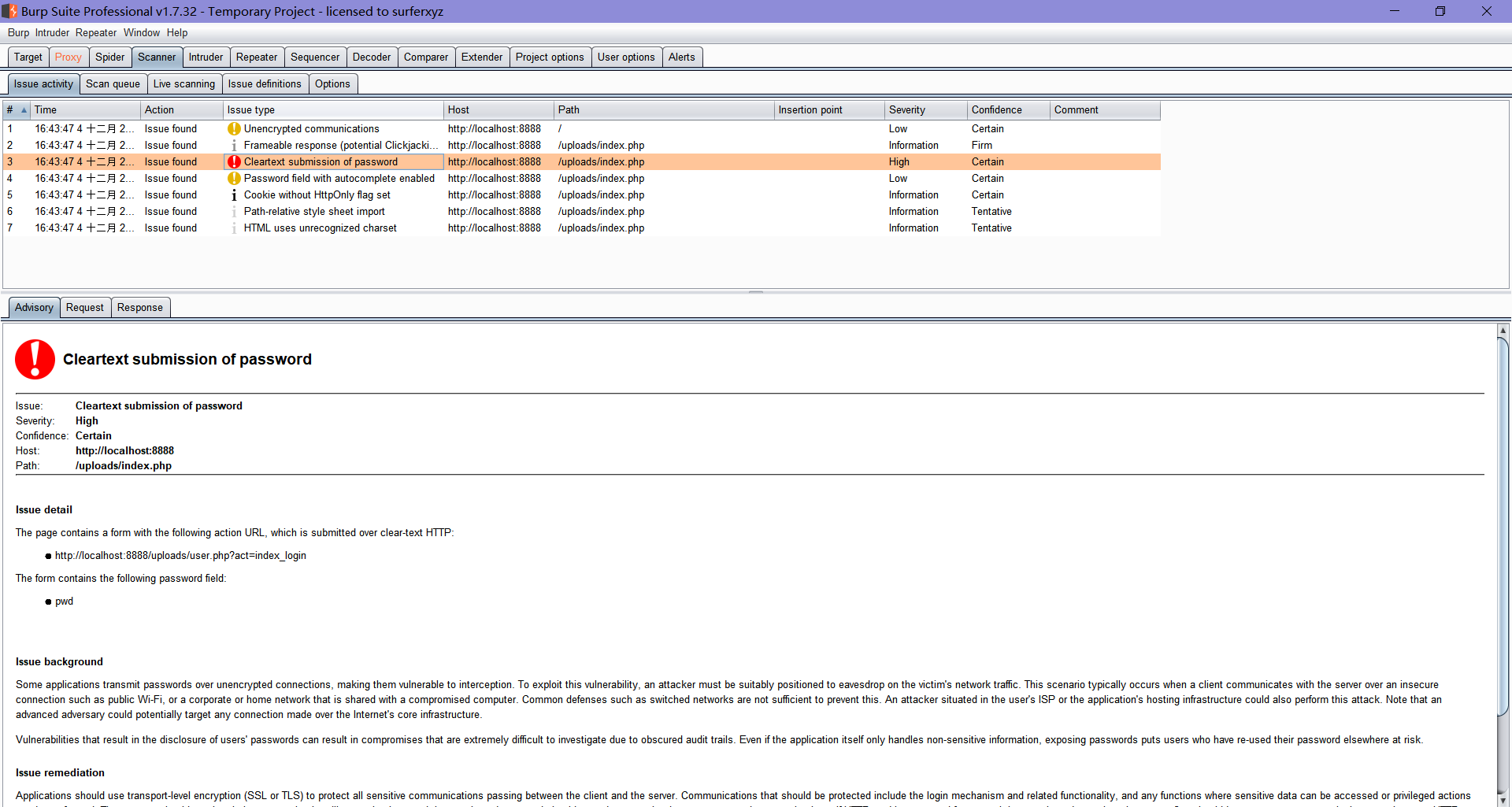
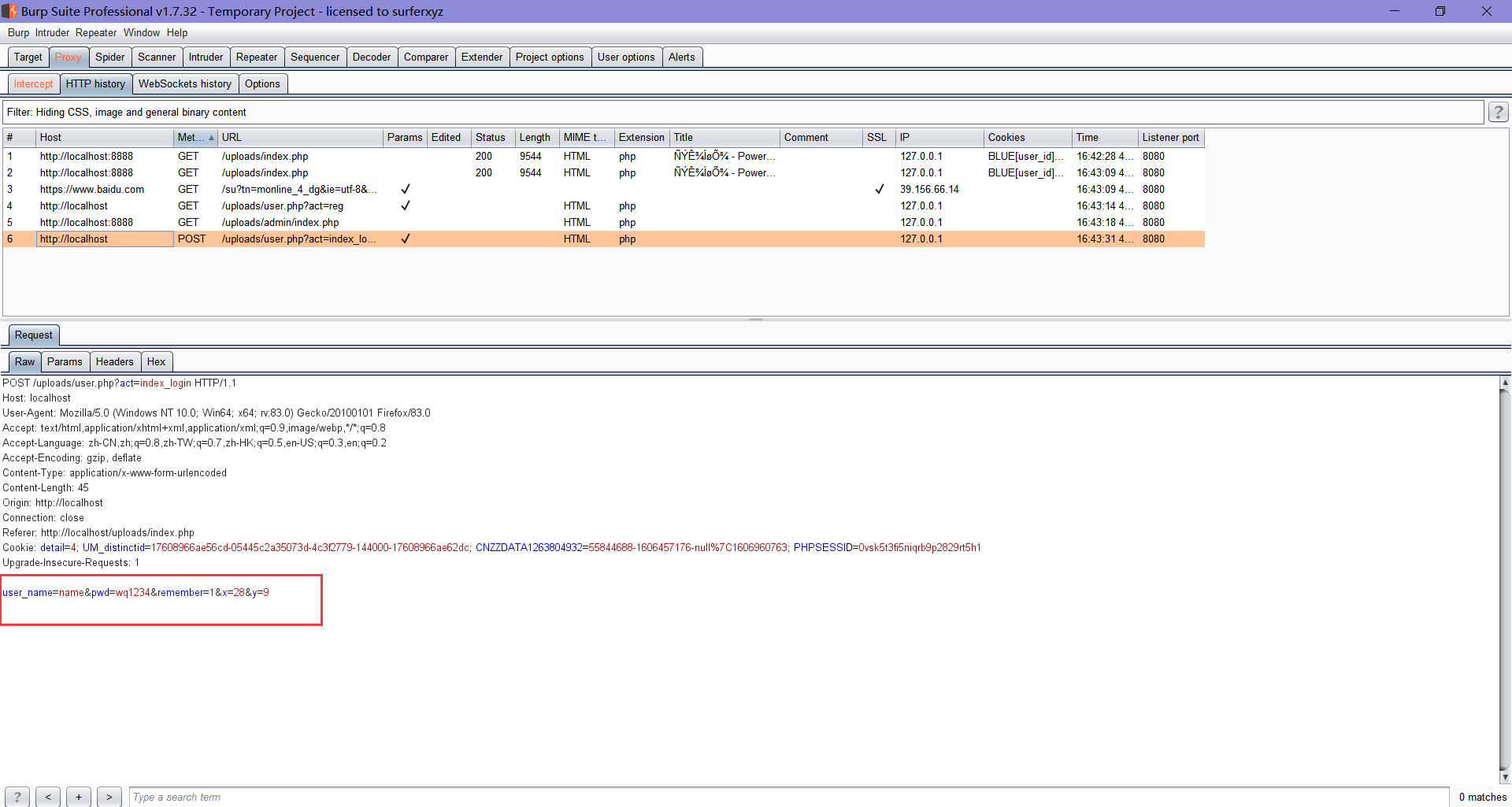
 

点击确定后MSN后会出现字符，点击检查元素时，网页代码中出现不该出现的代码

1. 明文提交密码

前台 使用Burp Suite工具在登录时进行扫描，抓包：

1. 明文提交密码

后台 使用Burp Suite工具在登录时进行扫描，抓包：

