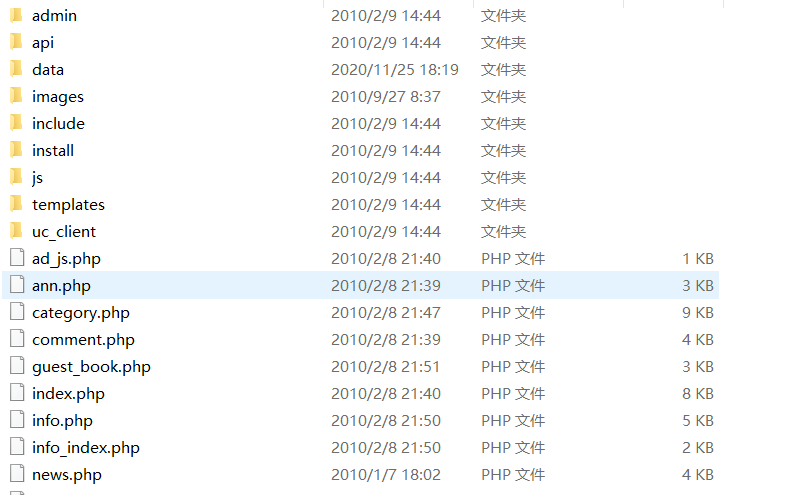
### 信息收集

搭建的演示网站BlueCMS基于PHPstudy\_pro的本地网站

1. 观察基本的网站结构



②．IP：即本地的IP：10.7.86.30

### 2.网站漏洞检测

①.XSS漏洞测试

反射型XSS（注册新用户）：

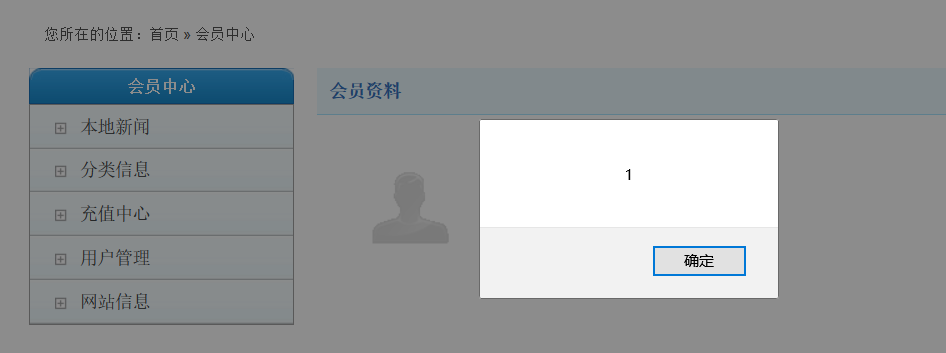


当在输入框中输入<script>alert('xss')</script>时，点击提交注册并不会出现弹框，但在user.php中，几乎是同时获取$act和$from的值，然后判断$act的值，来进行相应的操作。但是当$act的值为’reg‘，也就是注册的时候，他会将$from的值渲染到浏览器上。这也就导致了反射型XSS。

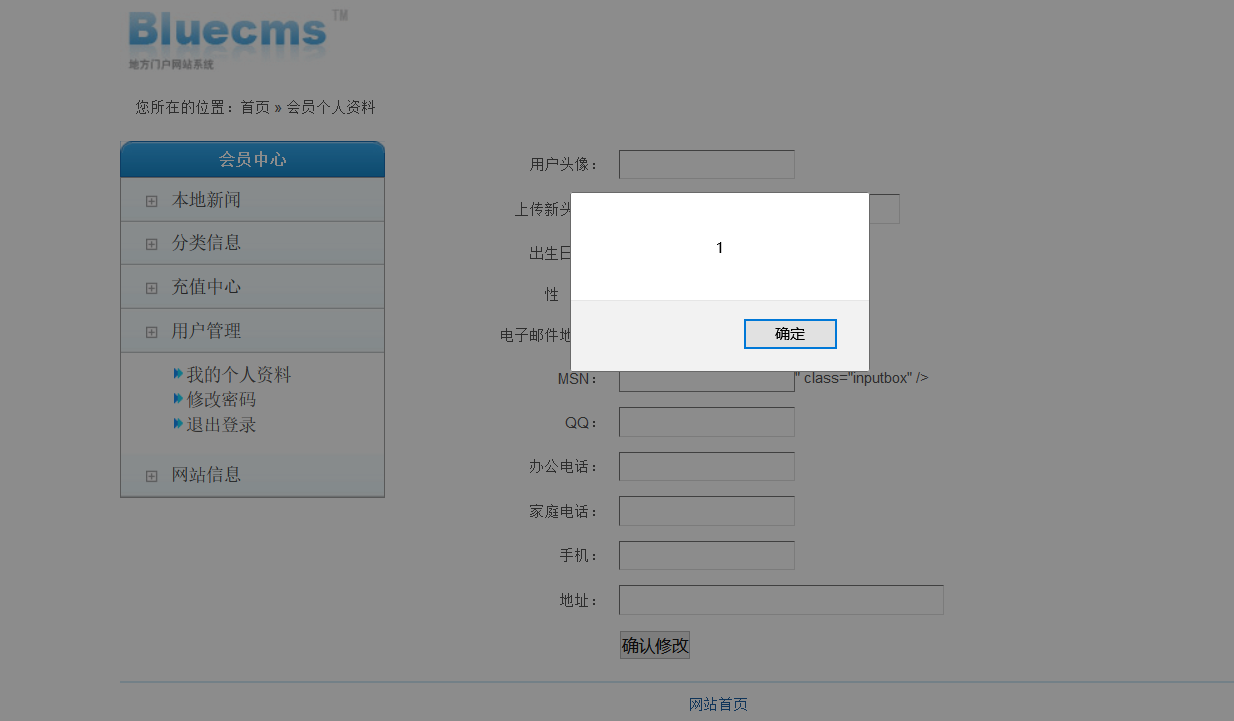
存储型XSS（编辑资料）：

在电子邮件地址中填入<script>alert(1)</script>，更改成功之后会出现弹框





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：



点击确定之后，会出现：

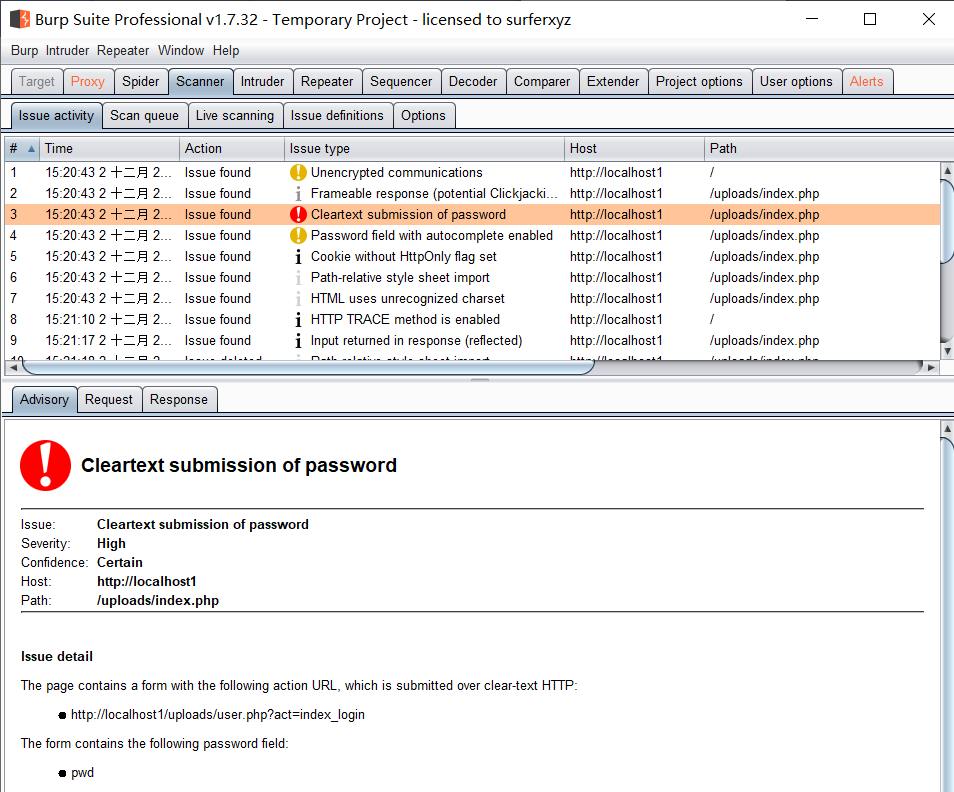


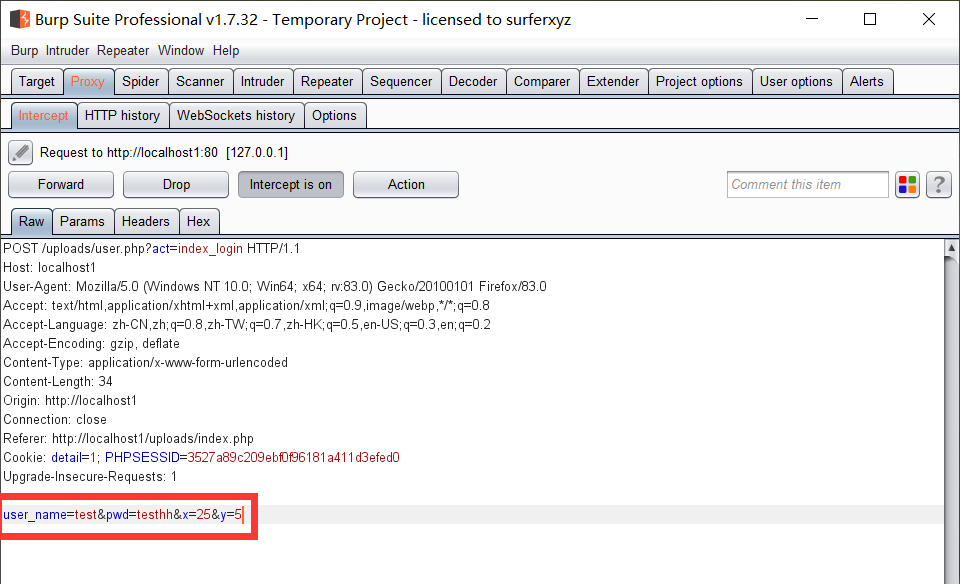
检查页面元素后，在代码中出现：

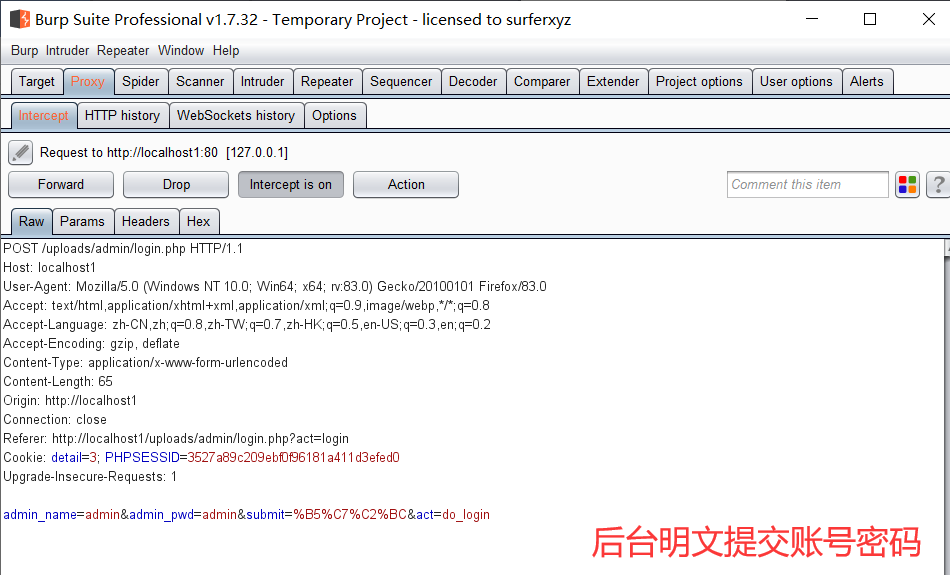


②．明文提交密码

前台 使用Burp Suite工具在登录时进行扫描，抓包：

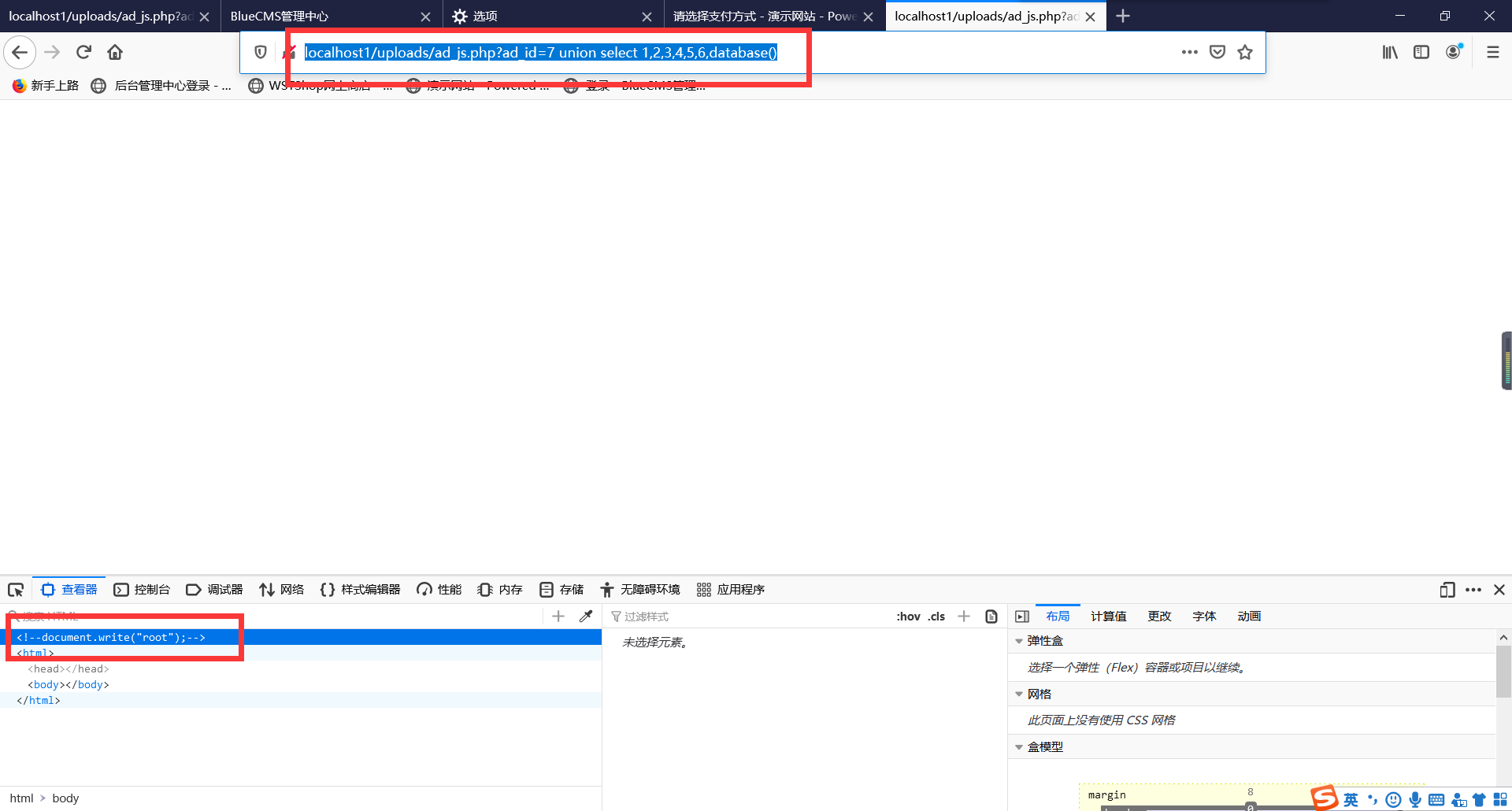






③.

输入网址http://localhost1/uploads/ad\_js.php?ad\_id=7 union select 1,2,3,4,5,6,database()



会出现数据库的名称

