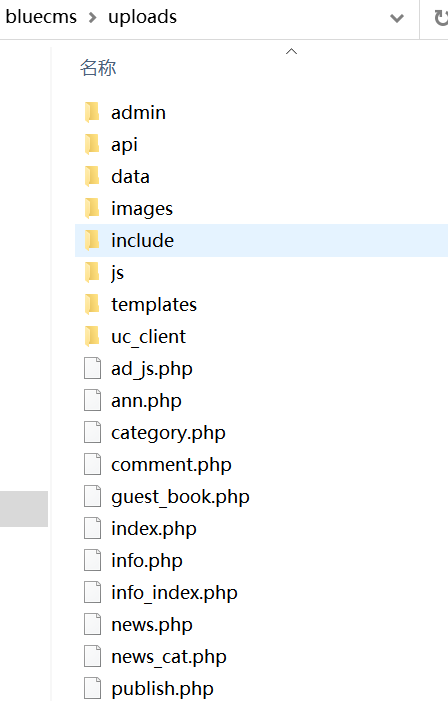
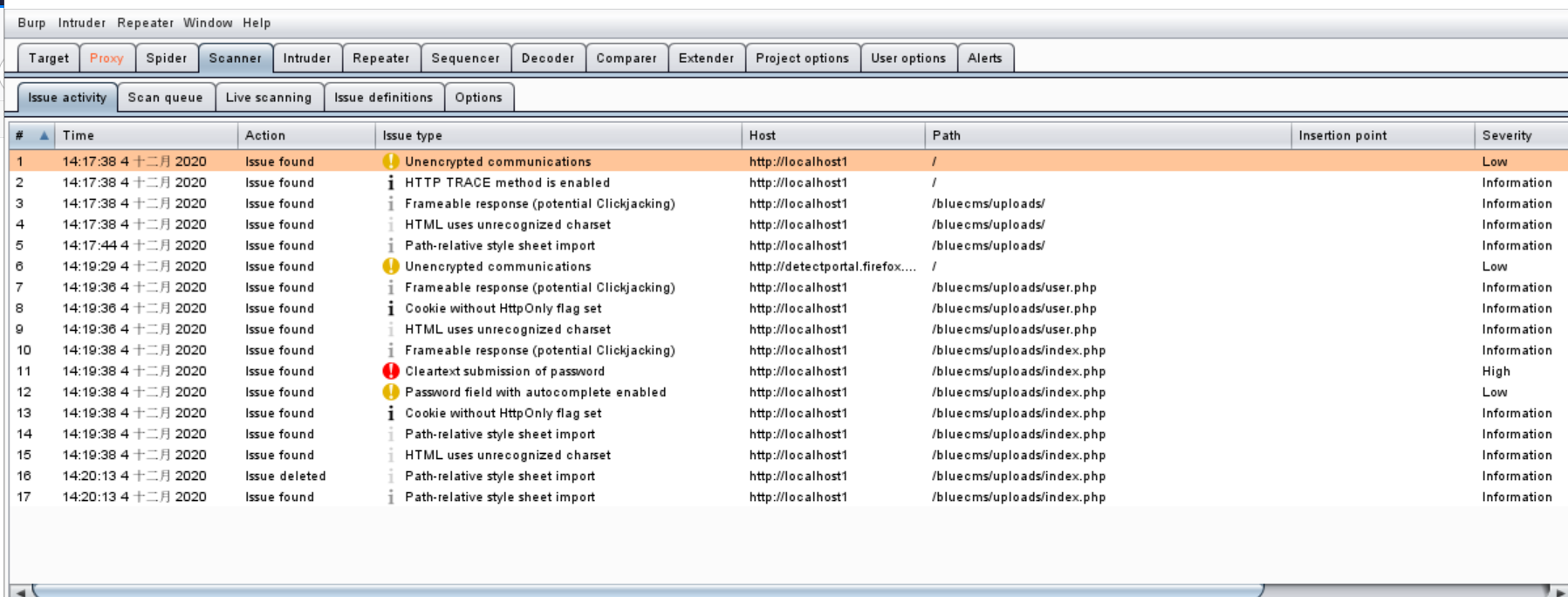
1. **信息收集**
2. IP地址： 127.0.0.1
3. 敏感目录：



**2、利用burpsuit进行漏洞扫描**

（1）利用burpsuit对网站bluecms\_1.6前台网站进行漏洞扫描：

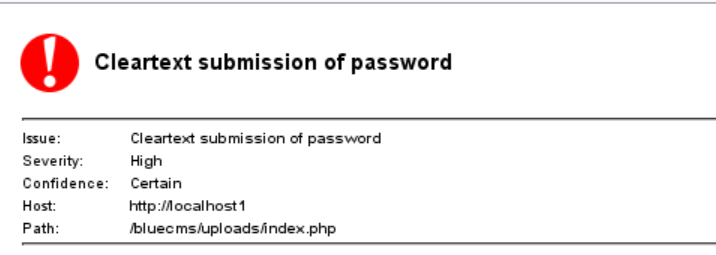


主要漏洞分别是：

①未加密通信



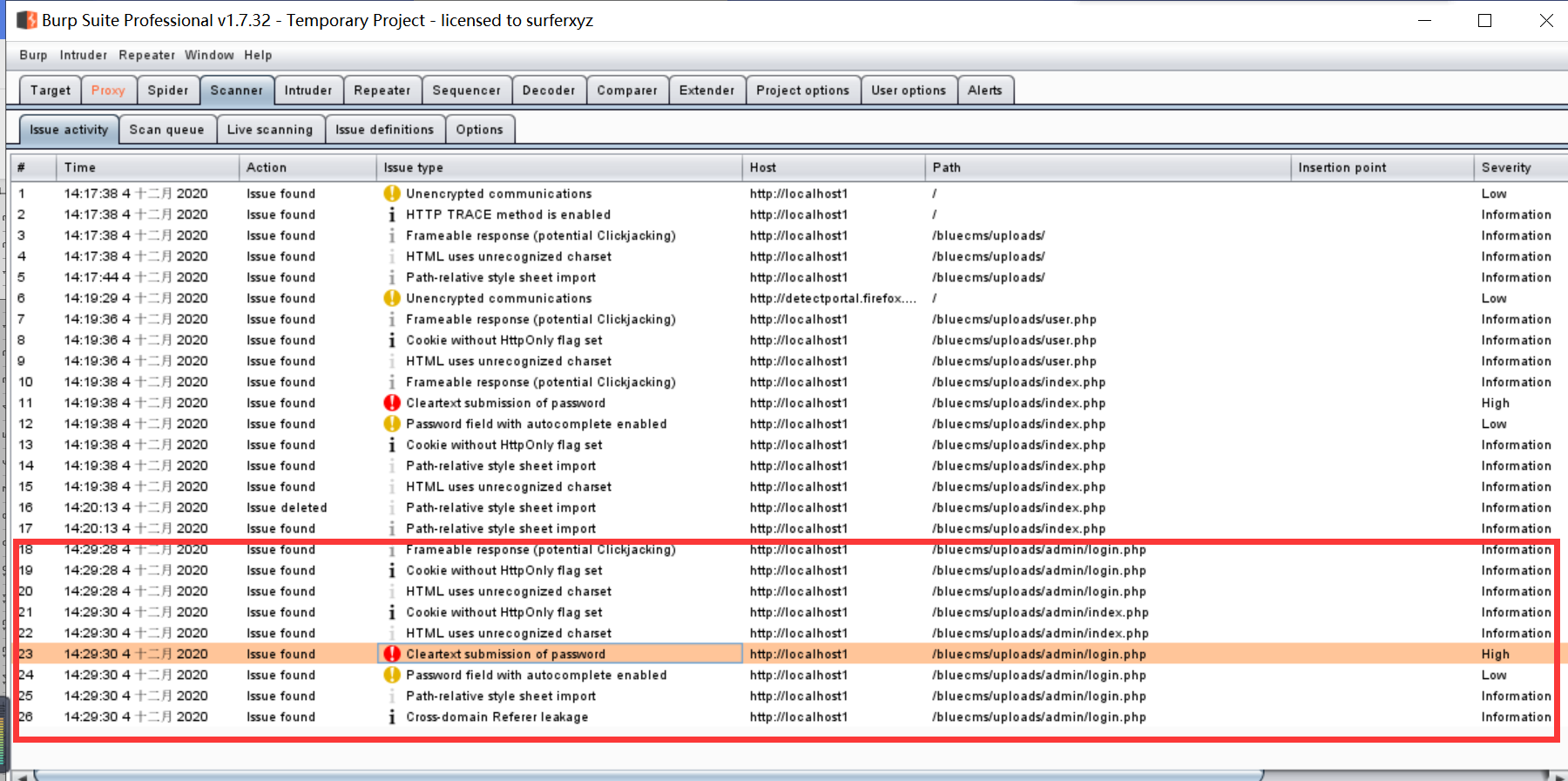
②明文提交密码



③启用自动完成功能的密码字段

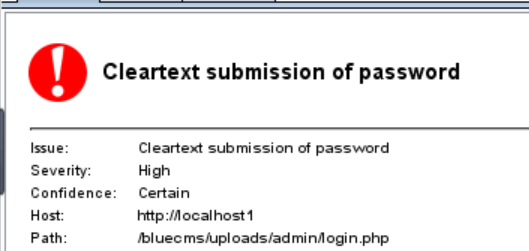


（2）利用burpsuit对网站bluecms\_1.6后台网站进行漏洞扫描：



主要漏洞有：

①明文提交密码

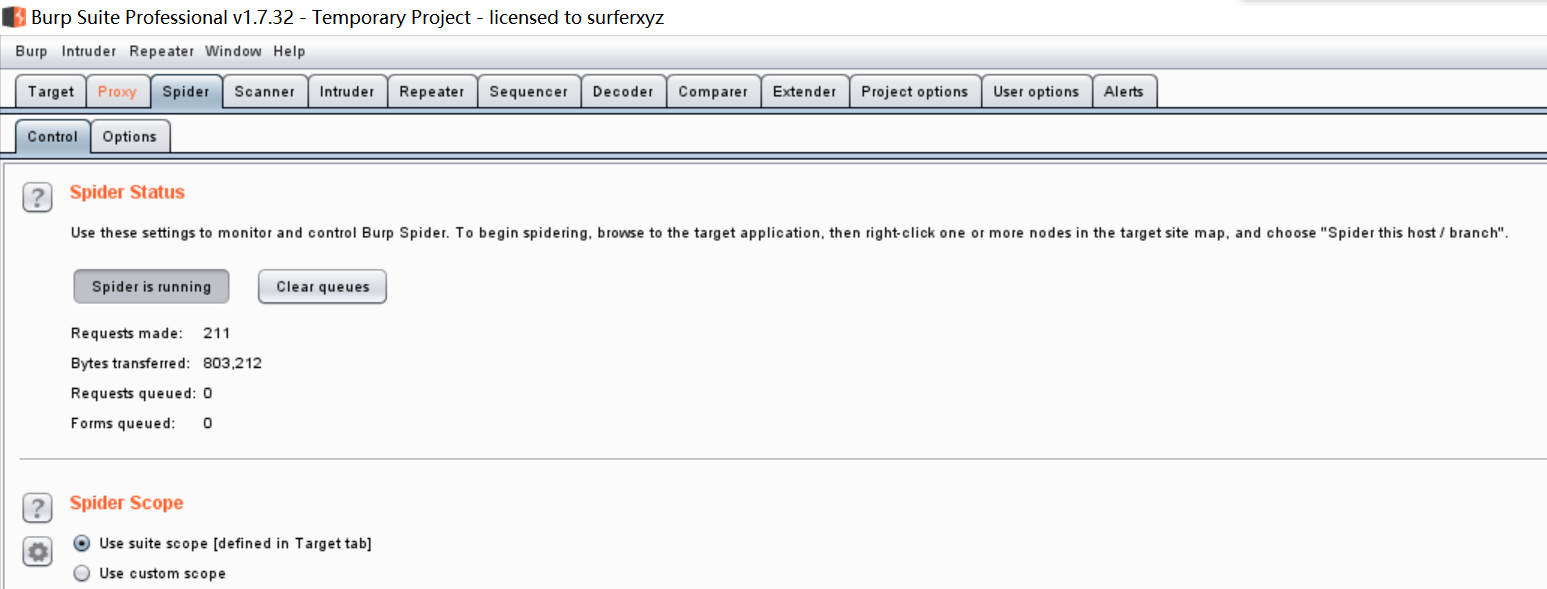


②启用自动完成功能的密码字段

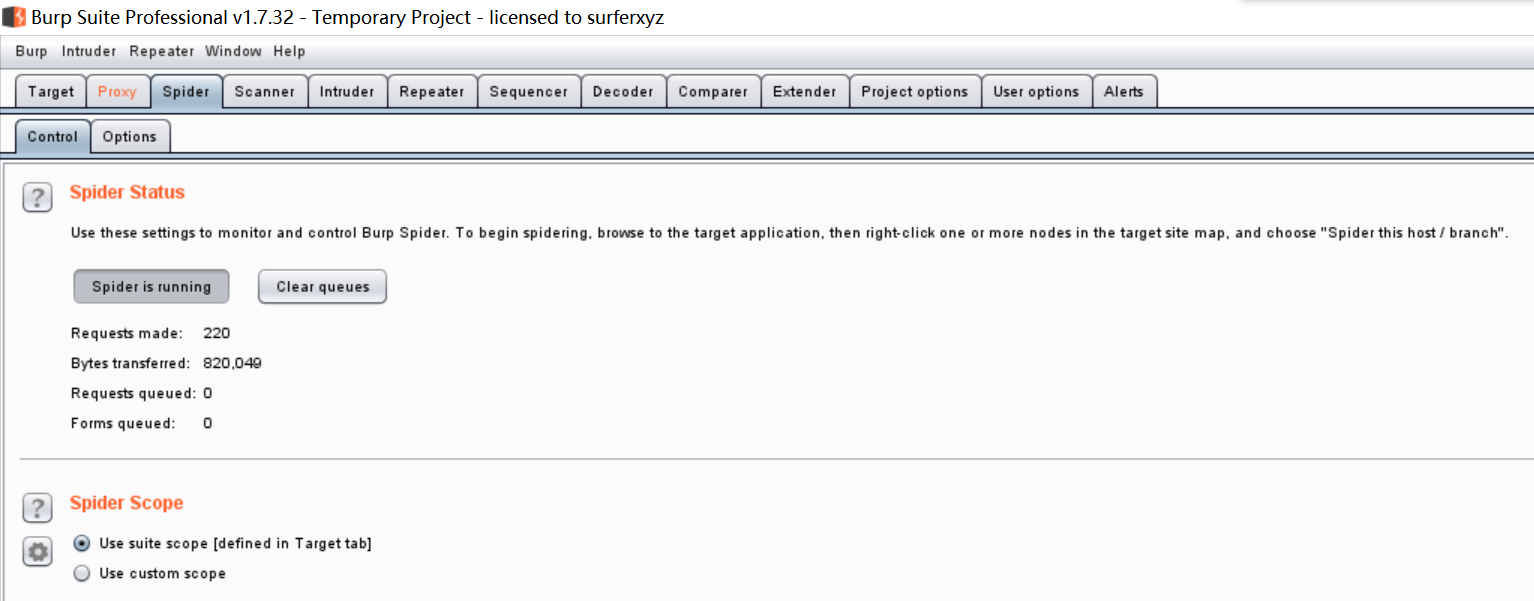


1. **网站爬取**

（1）利用burpsuit进行爬取网站：后台网站



（2）利用burpsuit进行爬取网站：前台网站



**4、手工测试漏洞**

（1）前台首页添加新闻，新闻分为为必填，但是无新闻分类。



1. 前台留言部分，填写留言内容，点击【发表留言】，弹出“留言内容不能为空！”的弹框。

