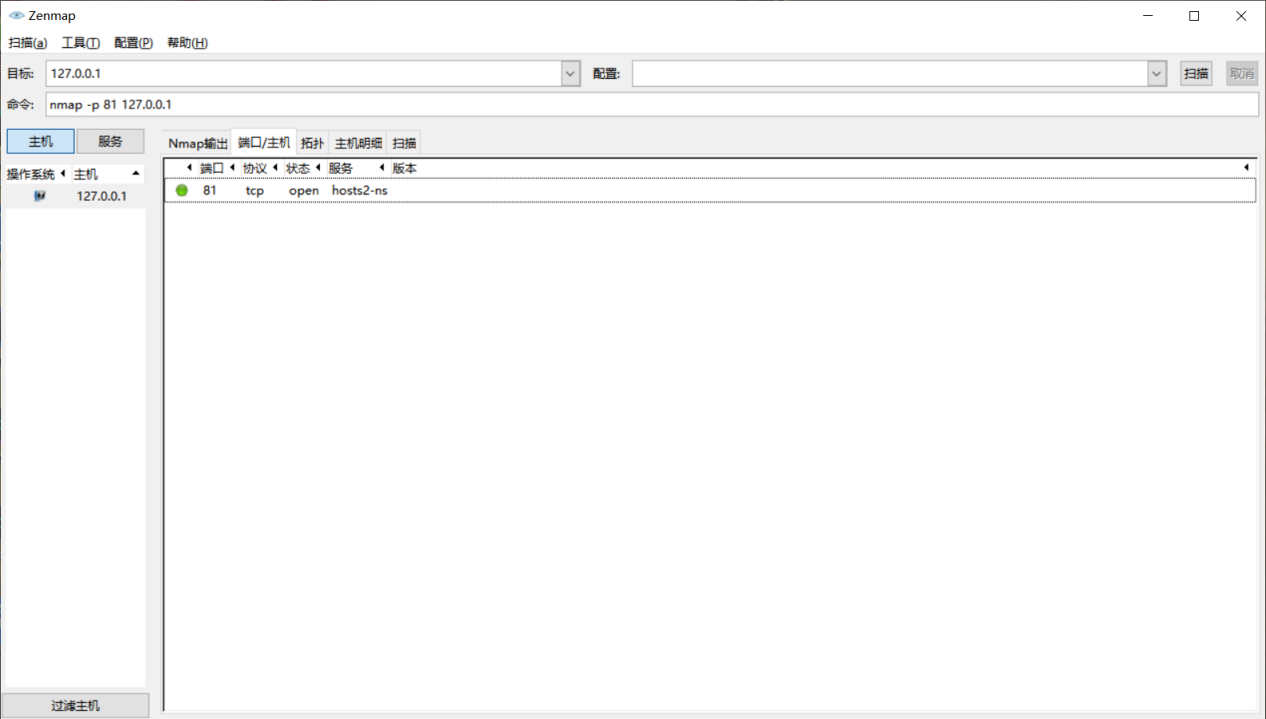
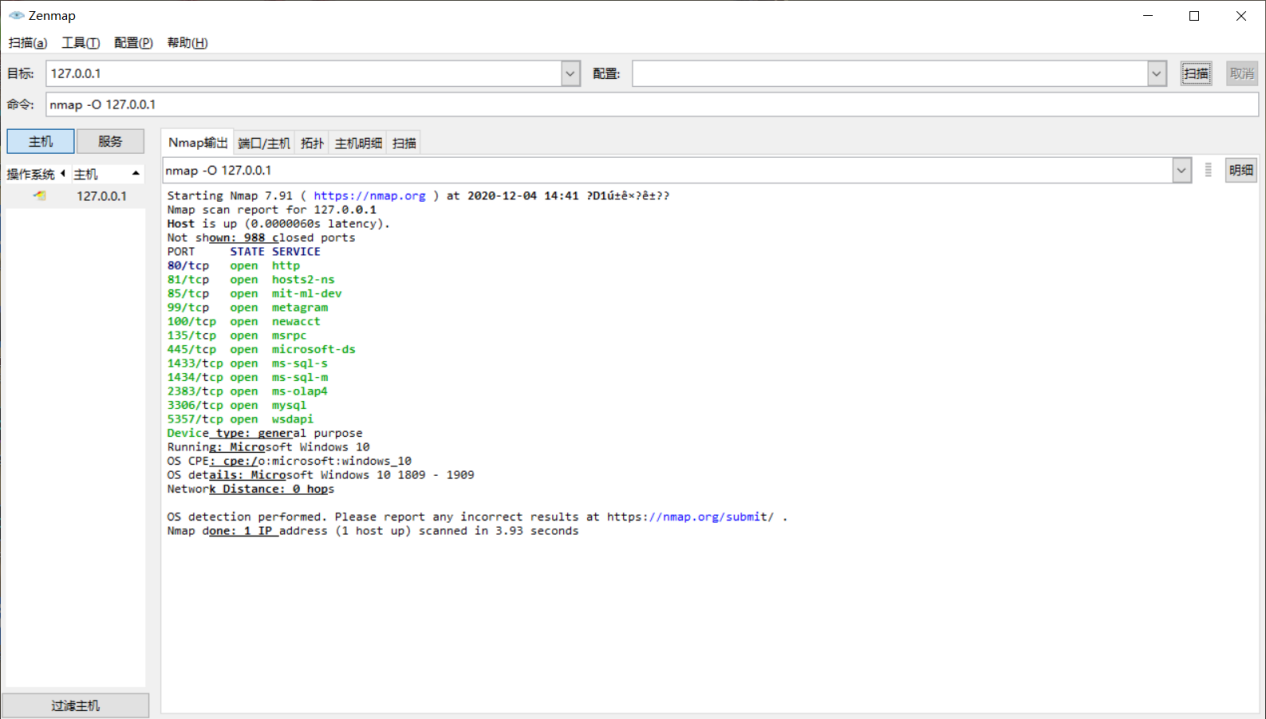
**王帅渗透测试**

**1.信息收集**

### 端口扫描：

****

****

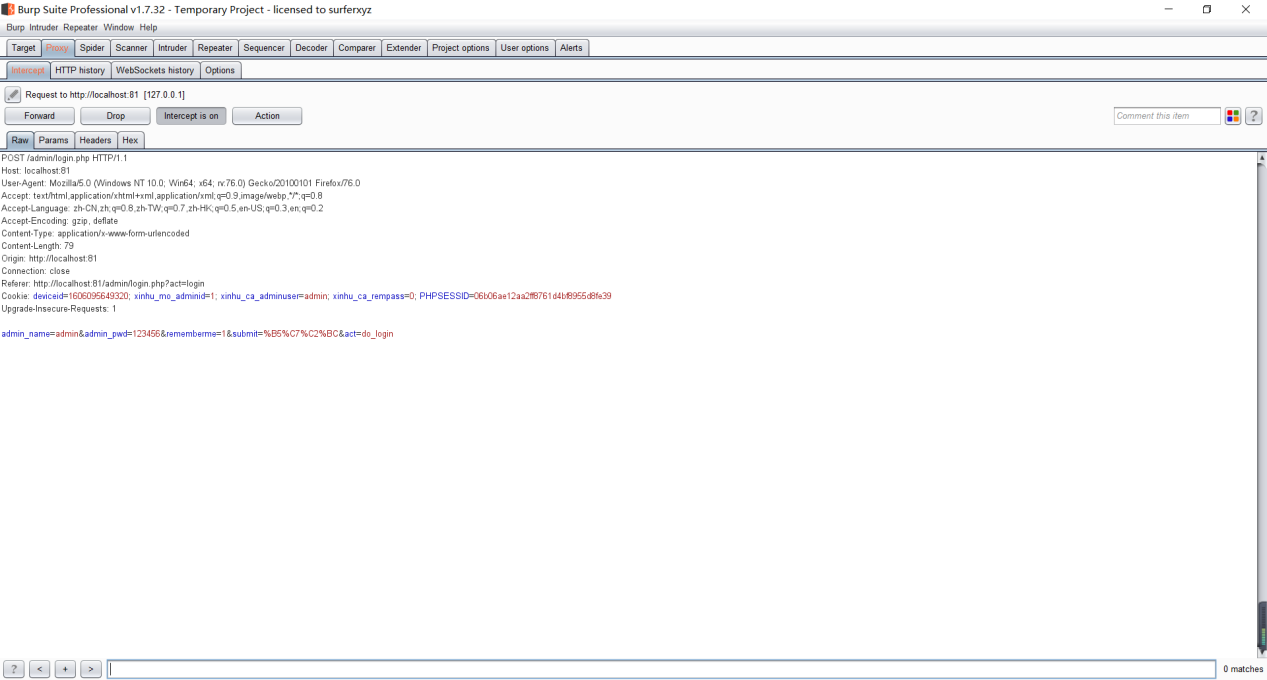
**版本信息：**

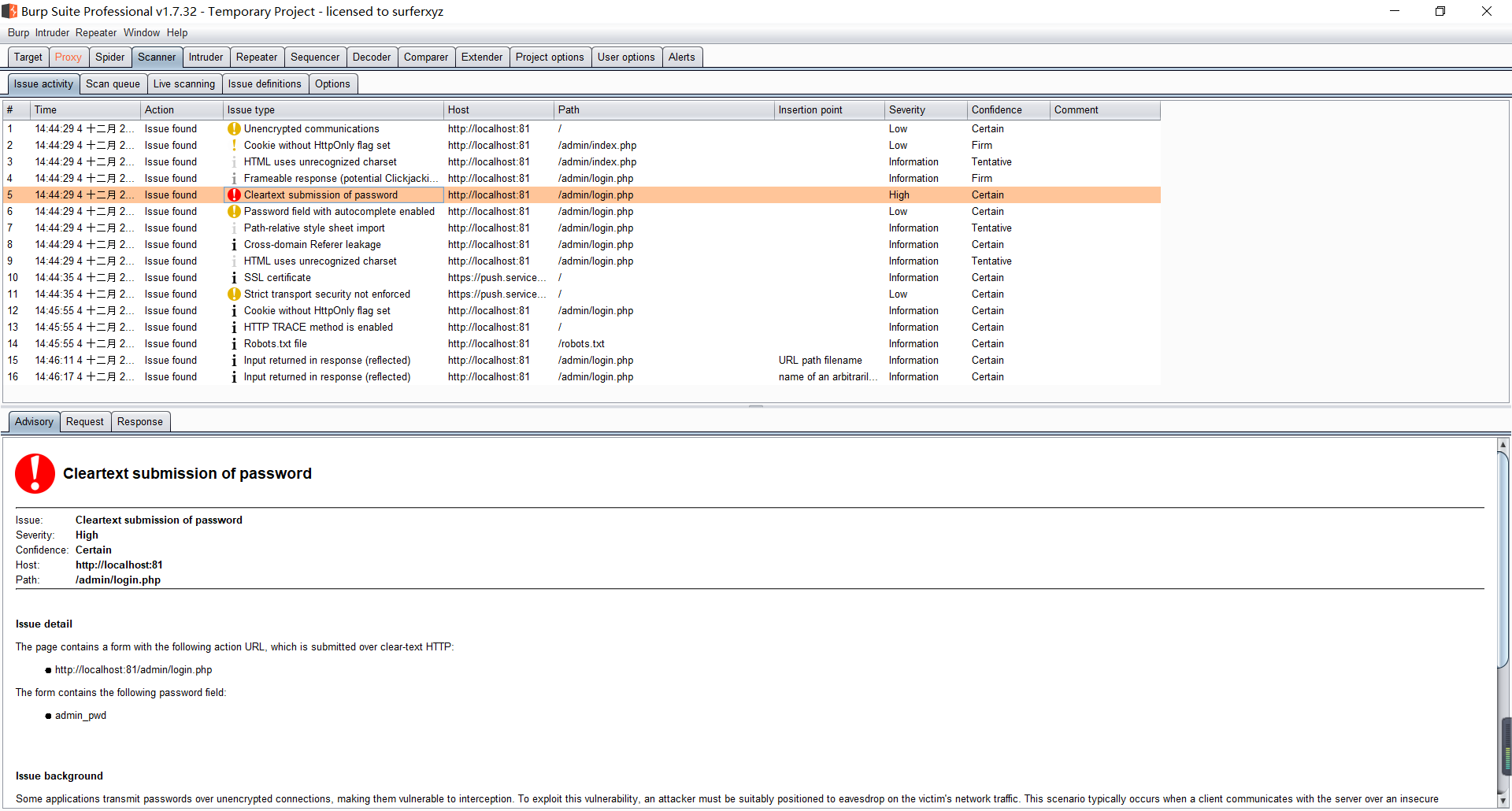
****

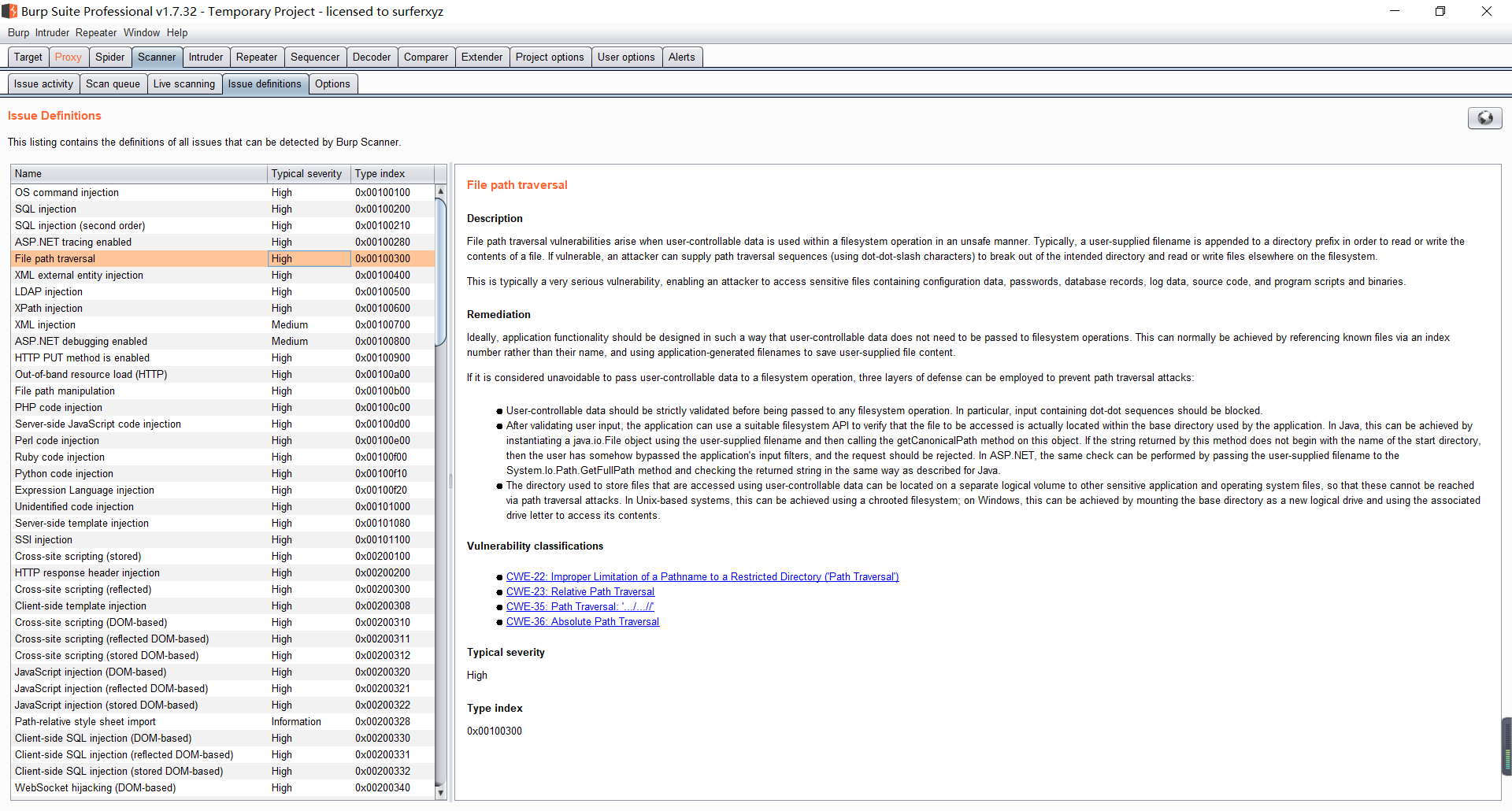
1. **利用burpsuit进行漏洞扫描**

对浏览器设置代理，打开burpsuit

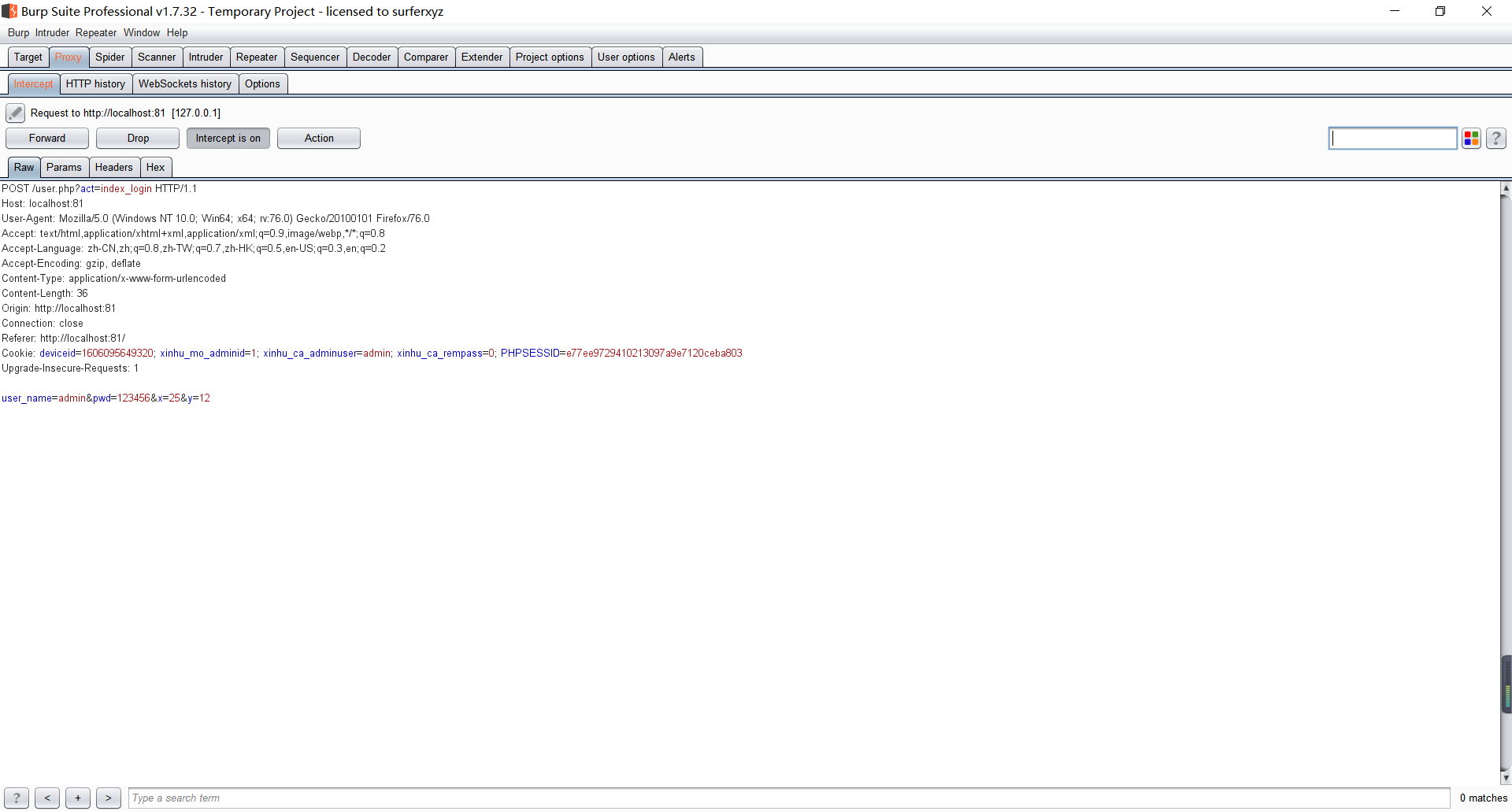
浏览器访问http://localhost:81/admin/index.php，拦截到之后扫描

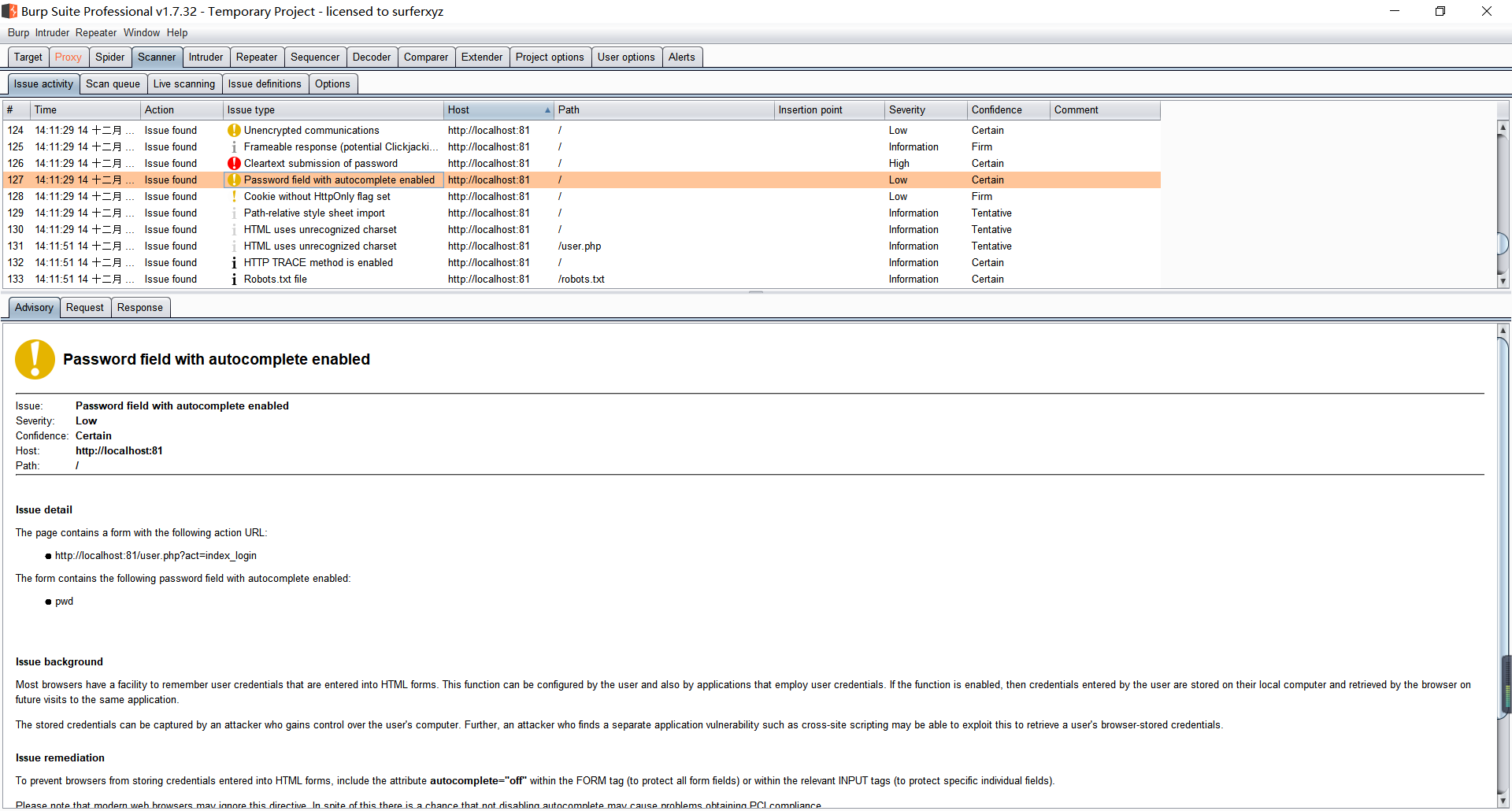
****

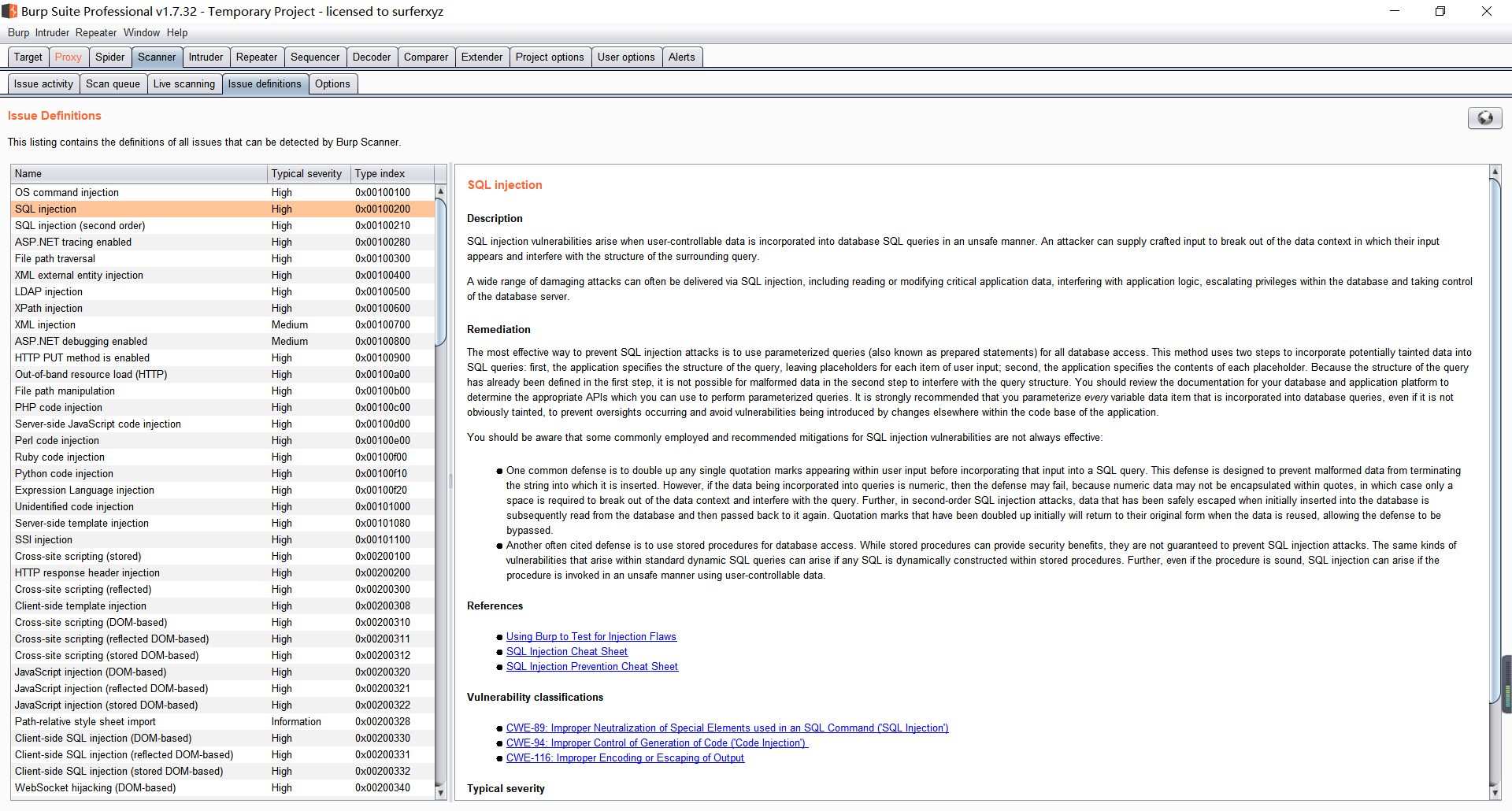
****

****

浏览器访问http://localhost:81/，拦截到之后扫描

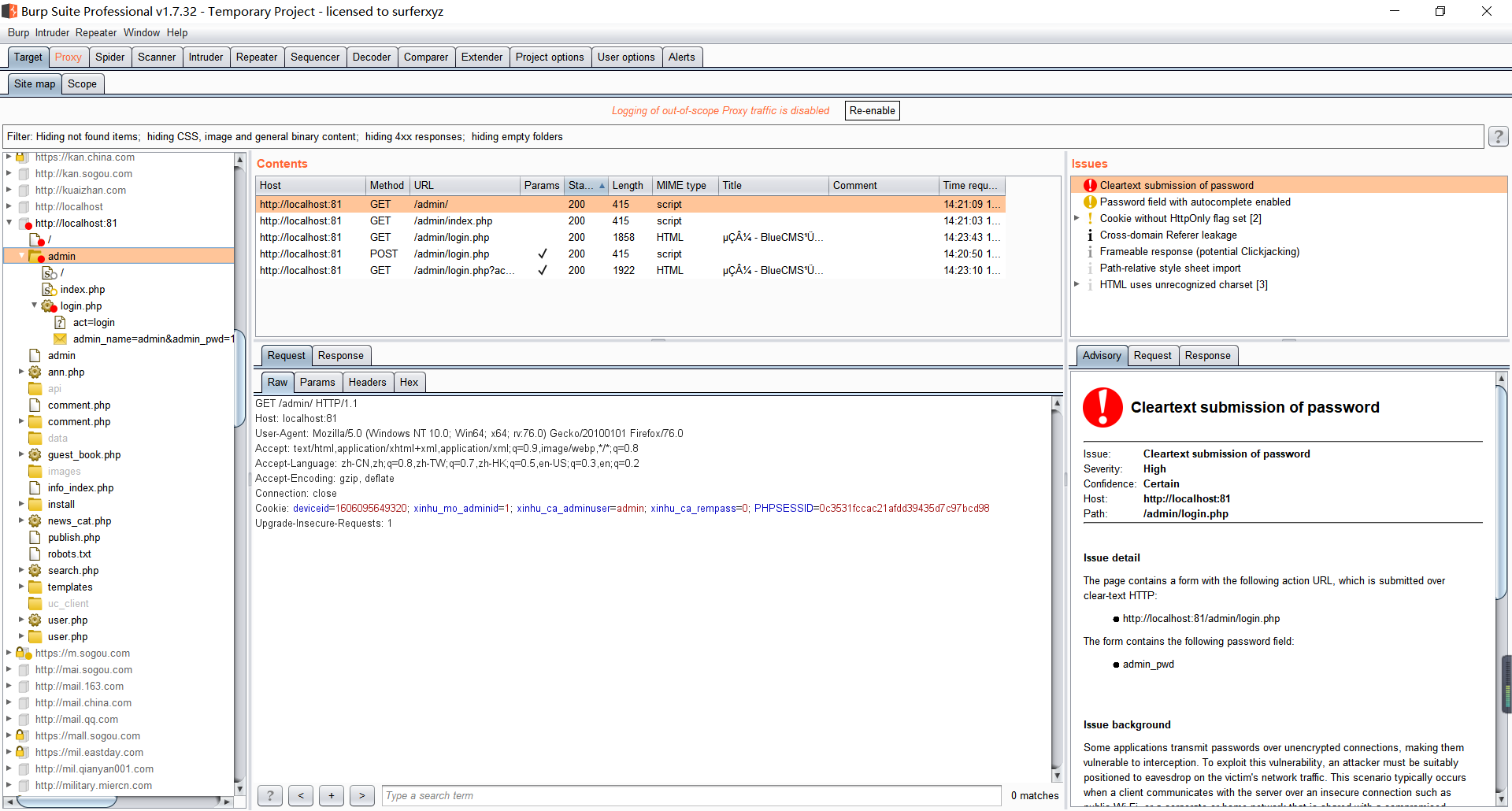


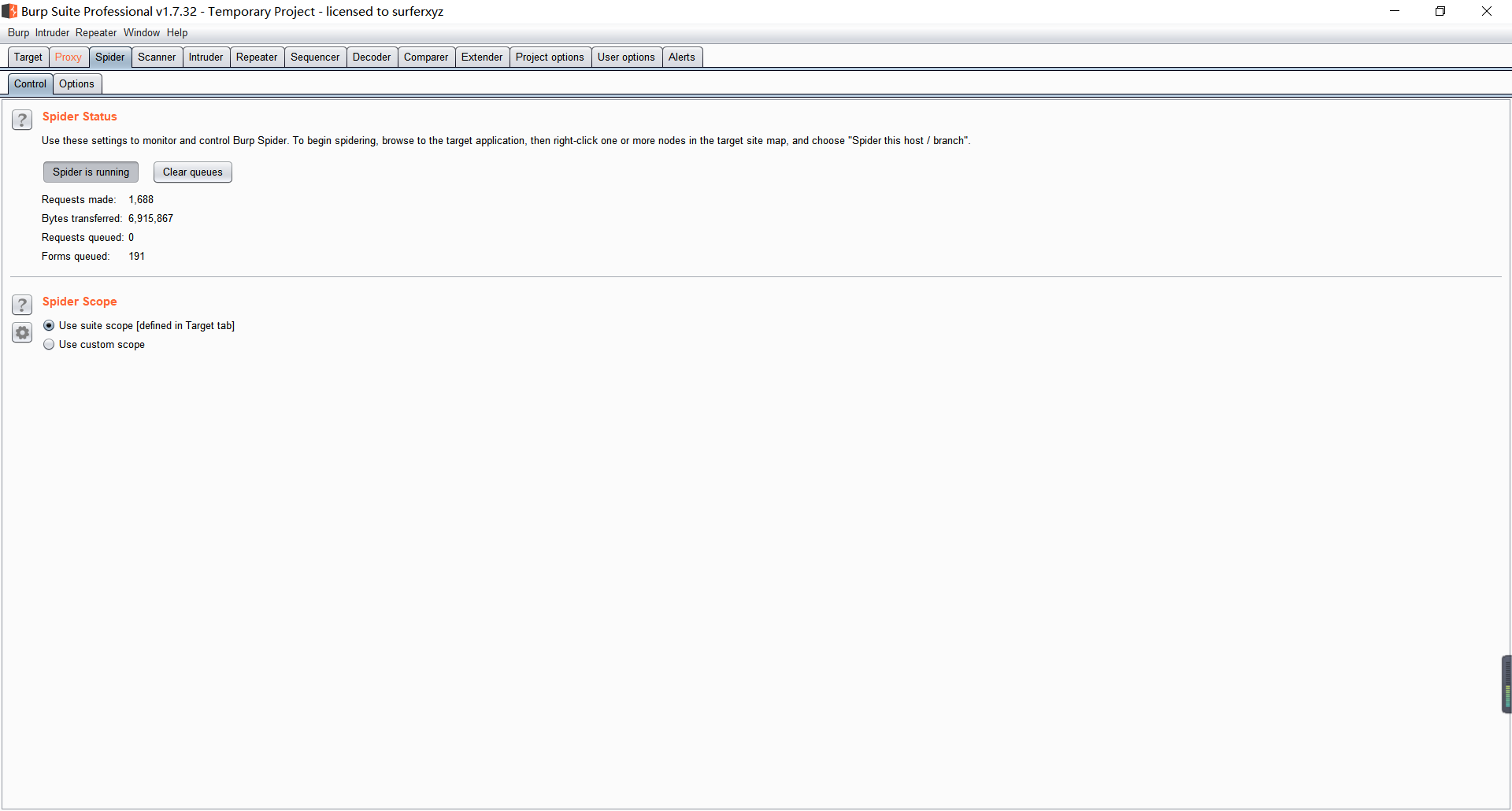




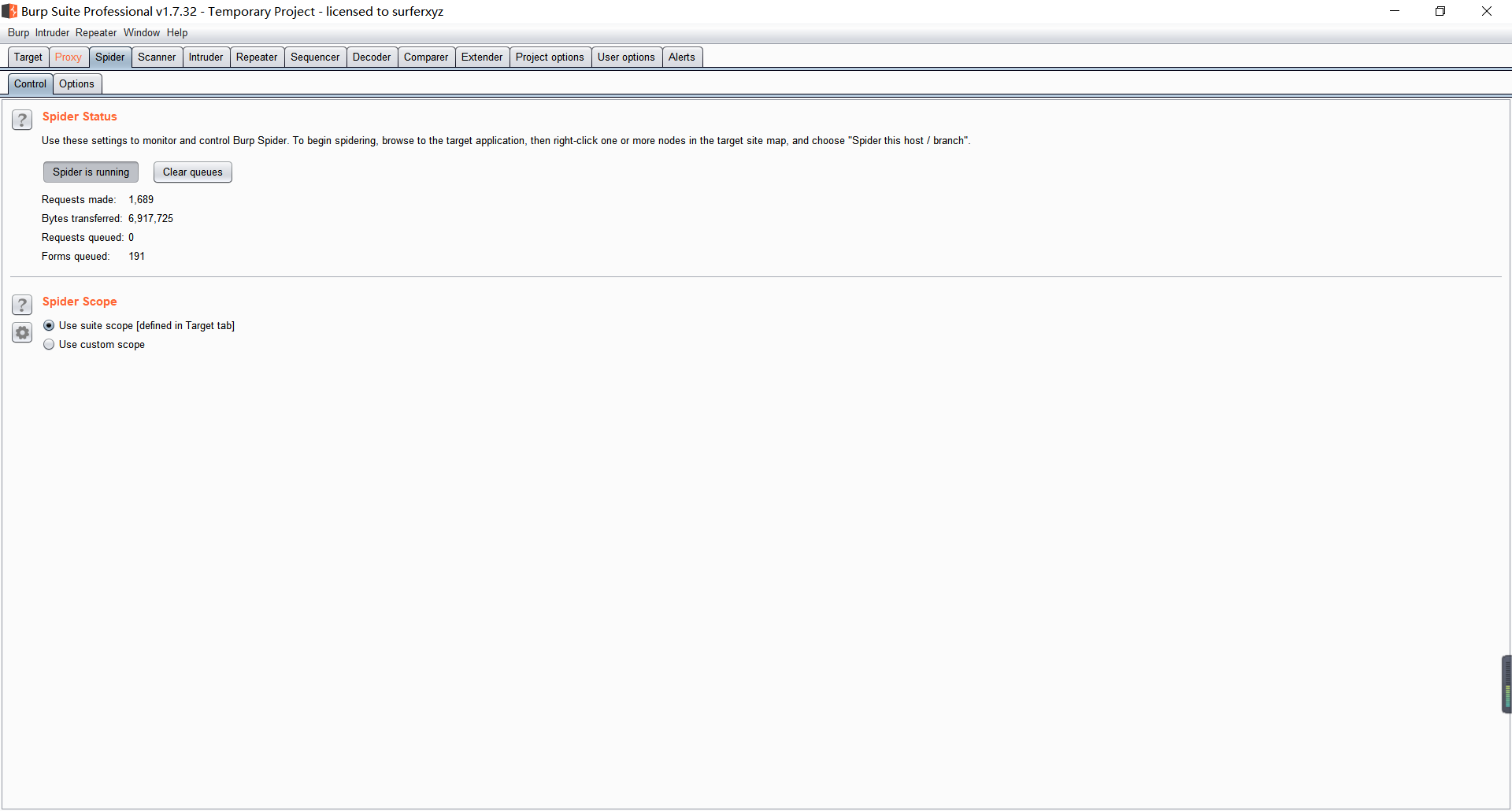
1. **爬取网站**

对前端登录页面（http://localhost:81/）进行爬取



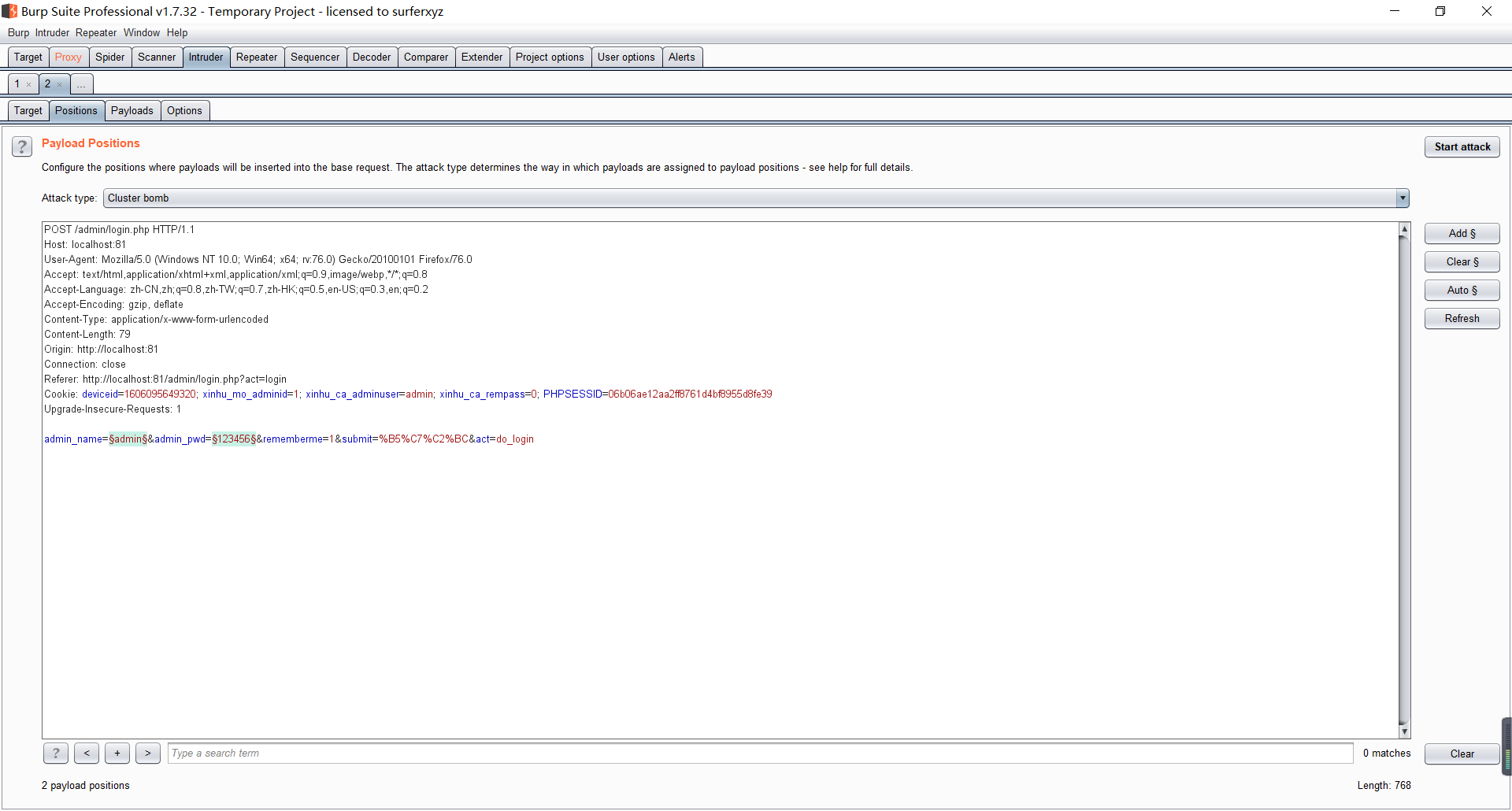


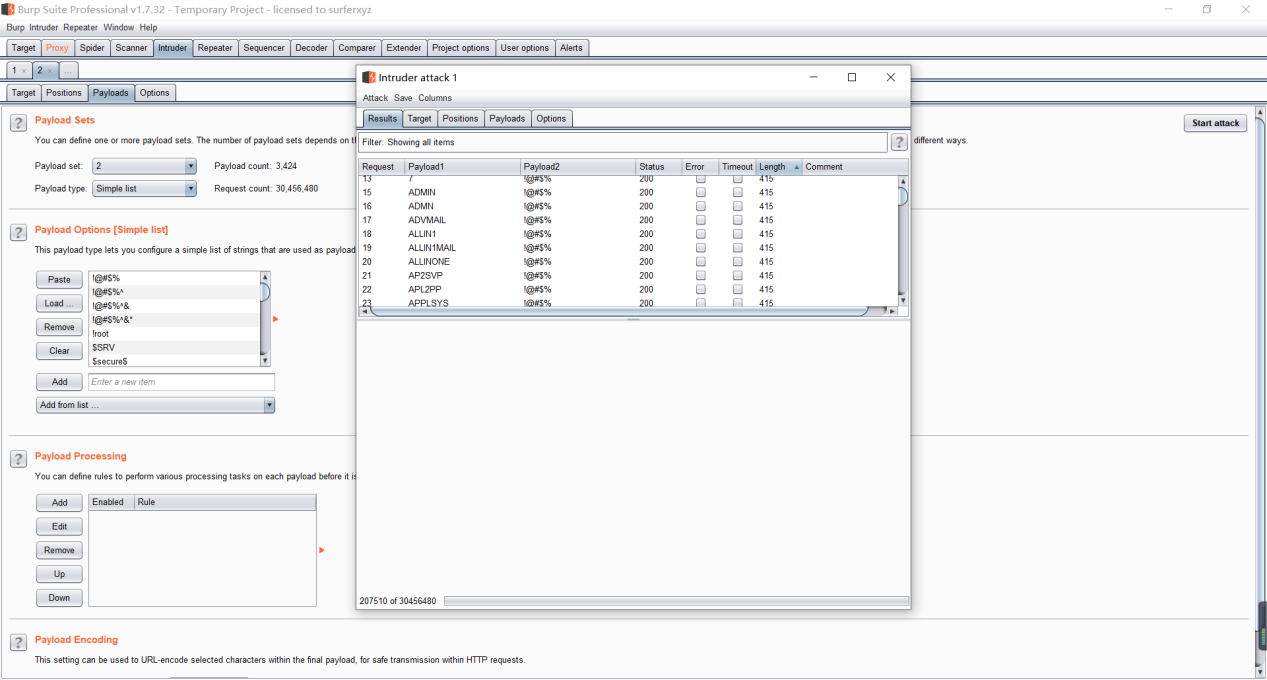
对后端登录页面（http://localhost:81/admin/）进行爬取



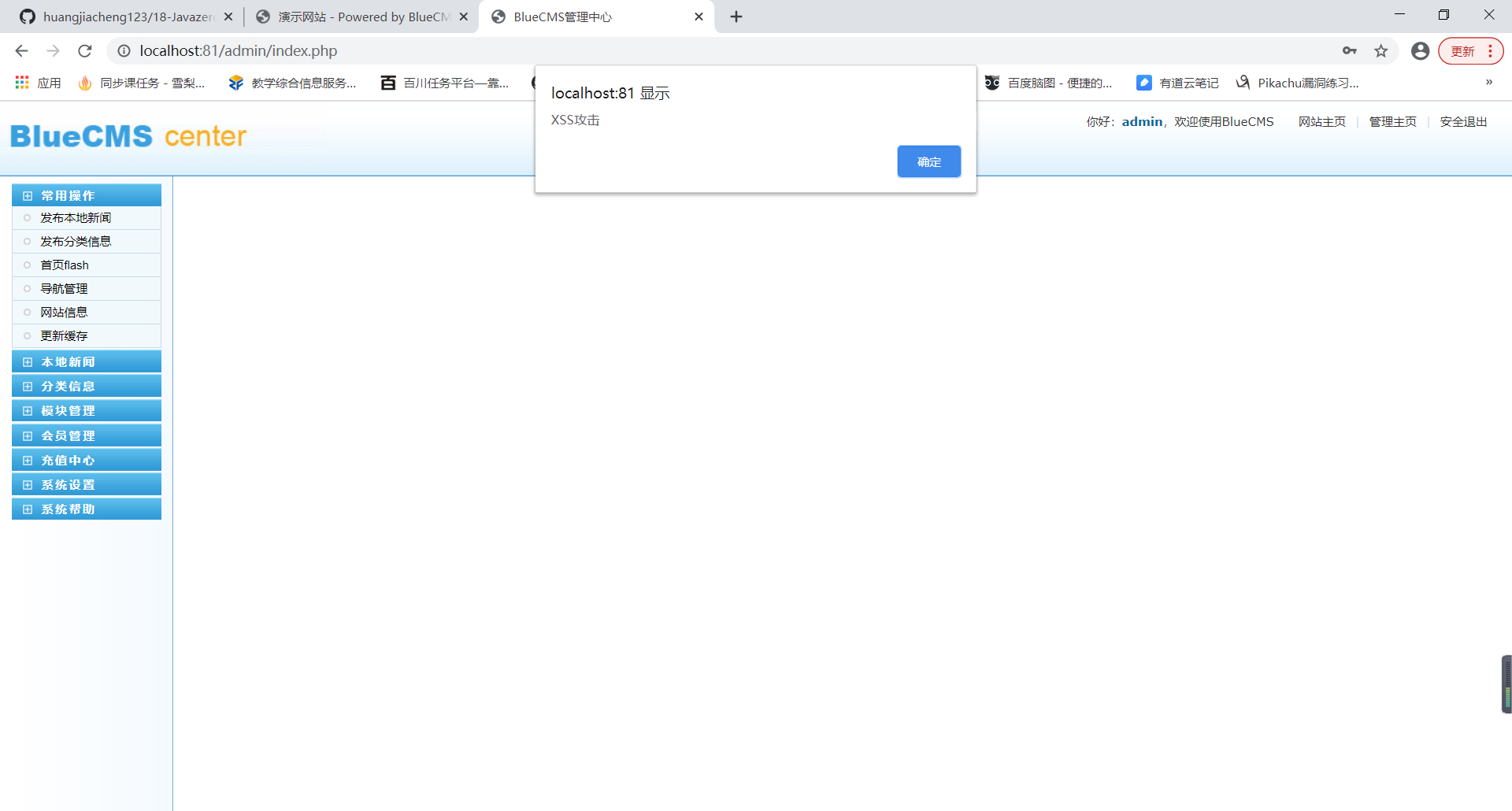
1. **自动化攻击**

**使用 Cluster bomb方法进行后端用户名和密码的攻击**

****

****

1. **手工测试**
2. 拿前台和后台登陆⻚⾯测试，⼿动输⼊了⼀些常⻅数据库的sql注⼊语句，都没有成功登陆，所以不存在sql注入。（formusr = ‘or 1=1-- formpwd = anything；或1' union select user,password from users）
3. xss漏洞：后台发布新闻



3.xss漏洞：后台本地新闻-新闻管理 ； 系统-站点设置； 会员管理-会员列表-添加新会员

