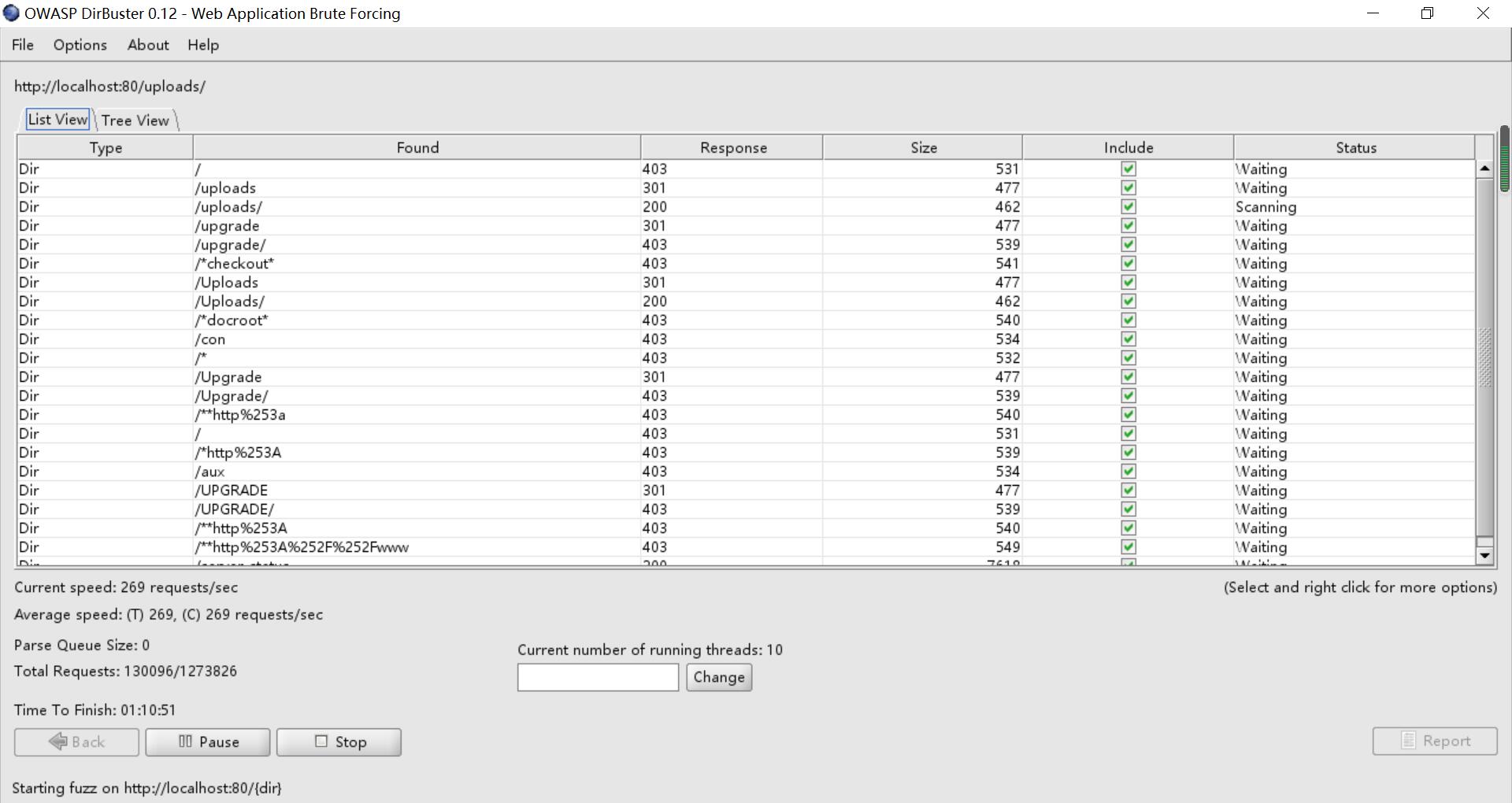
# 信息收集

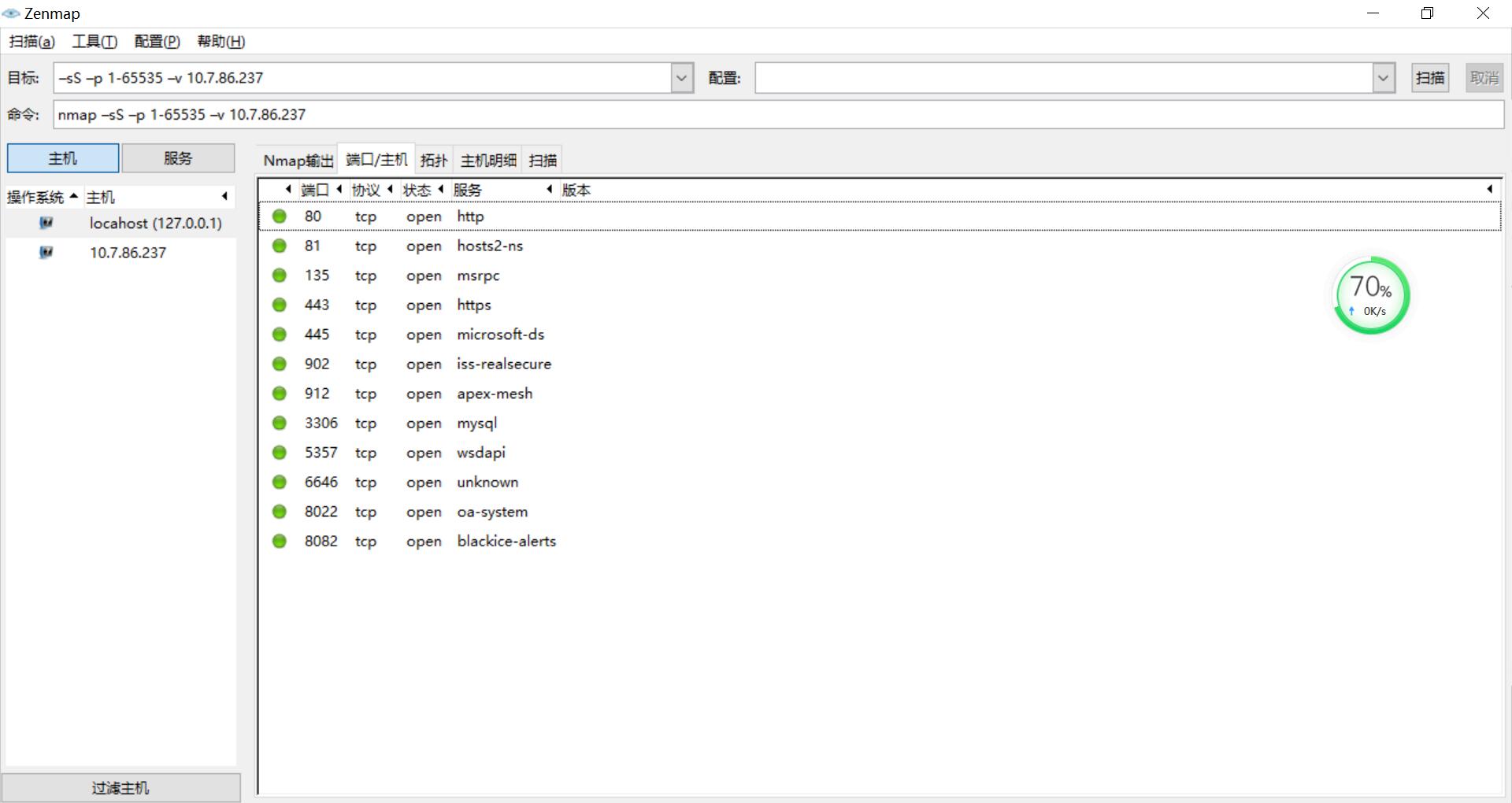
1. 域名信息

Bluecms环境构建在本机，无域名信息

1. 敏感目录



1. 端口扫描



1. 整站分析

服务器的操作系统：Windows系统

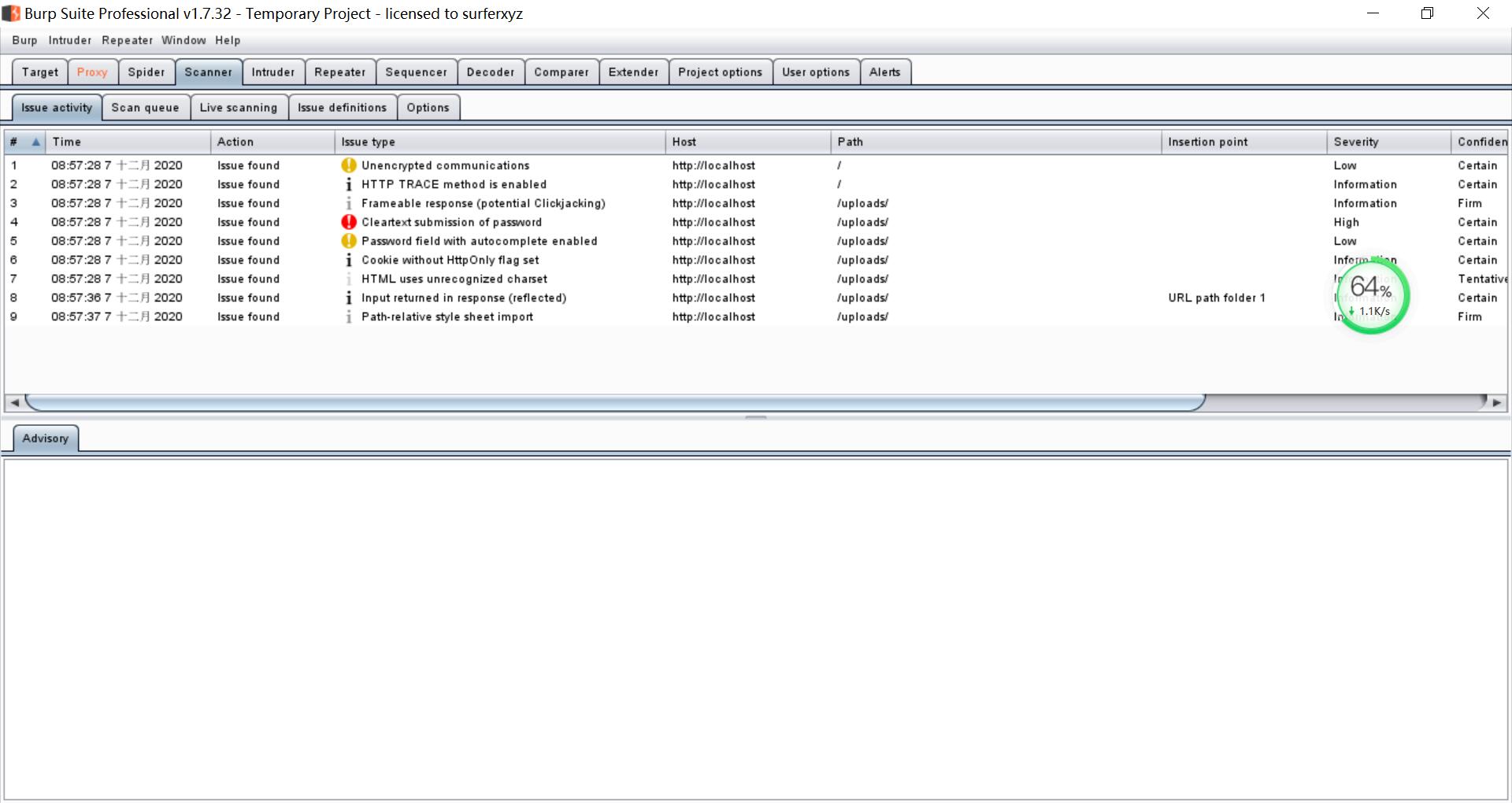
网站容器：Apache

脚本类型：php

数据库类型：MySql

# 漏洞扫描

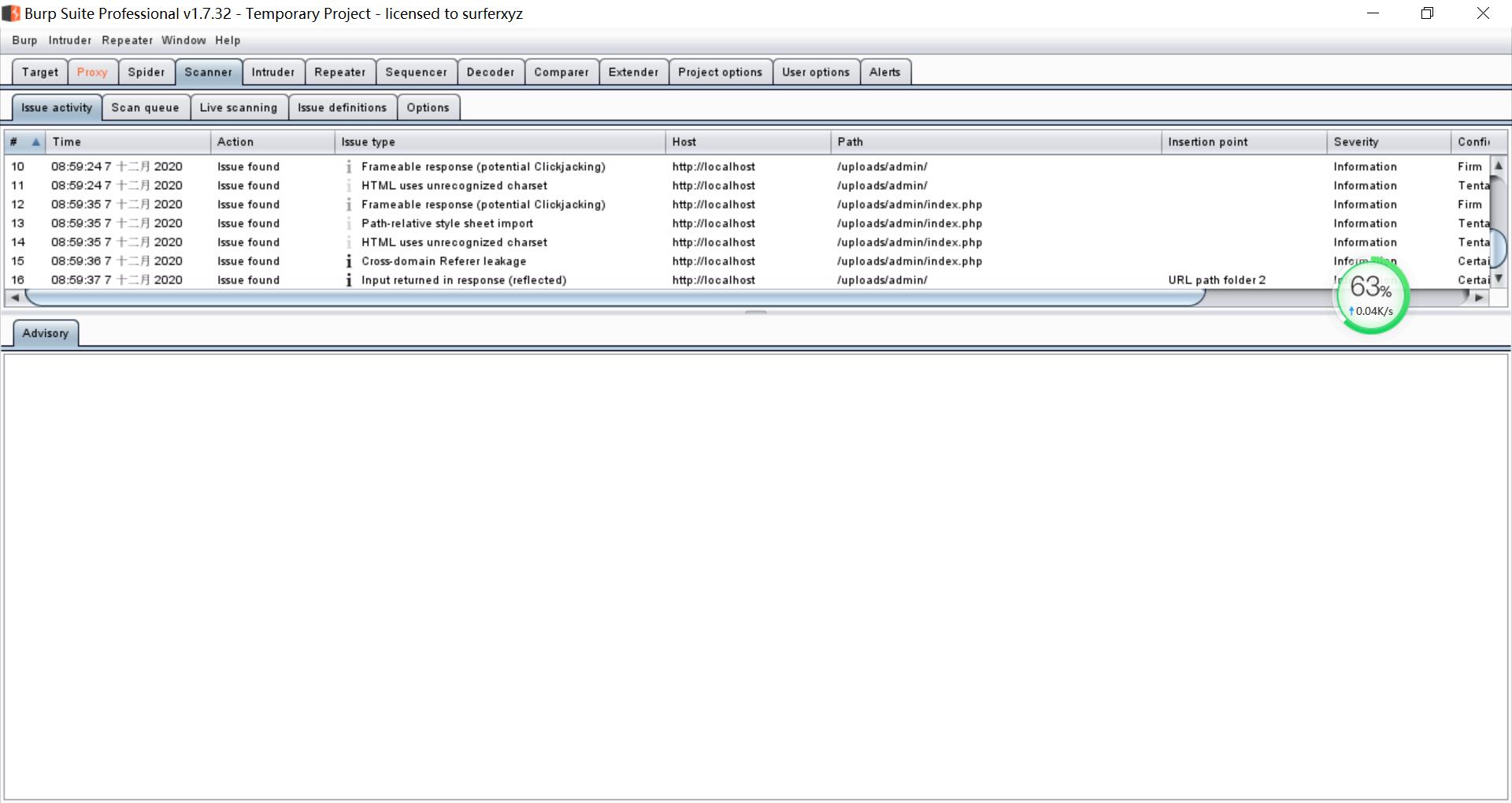
1.前台



漏洞分析：

1. Unencrypted communications ：未加密通信
2. HTTP TRACE method is enabled ：已启用 HTTP TRACE 方法
3. Frameable response (potential Clickjacking)：可框架响应（潜在的点击劫持）
4. Cleartext submission of password：密码的明文提交
5. Password field with autocomplete enabled：启用自动完成功能的密码字段
6. Cookie without HttpOnly flag set：没有 Httponly 标志集的 Cookie
7. HTML uses unrecognized charset：HTML 使用无法识别的字符集
8. Input returned in response (reflected)：响应返回的输入（反射）
9. Path-relative style sheet import：路径相关样式表导入

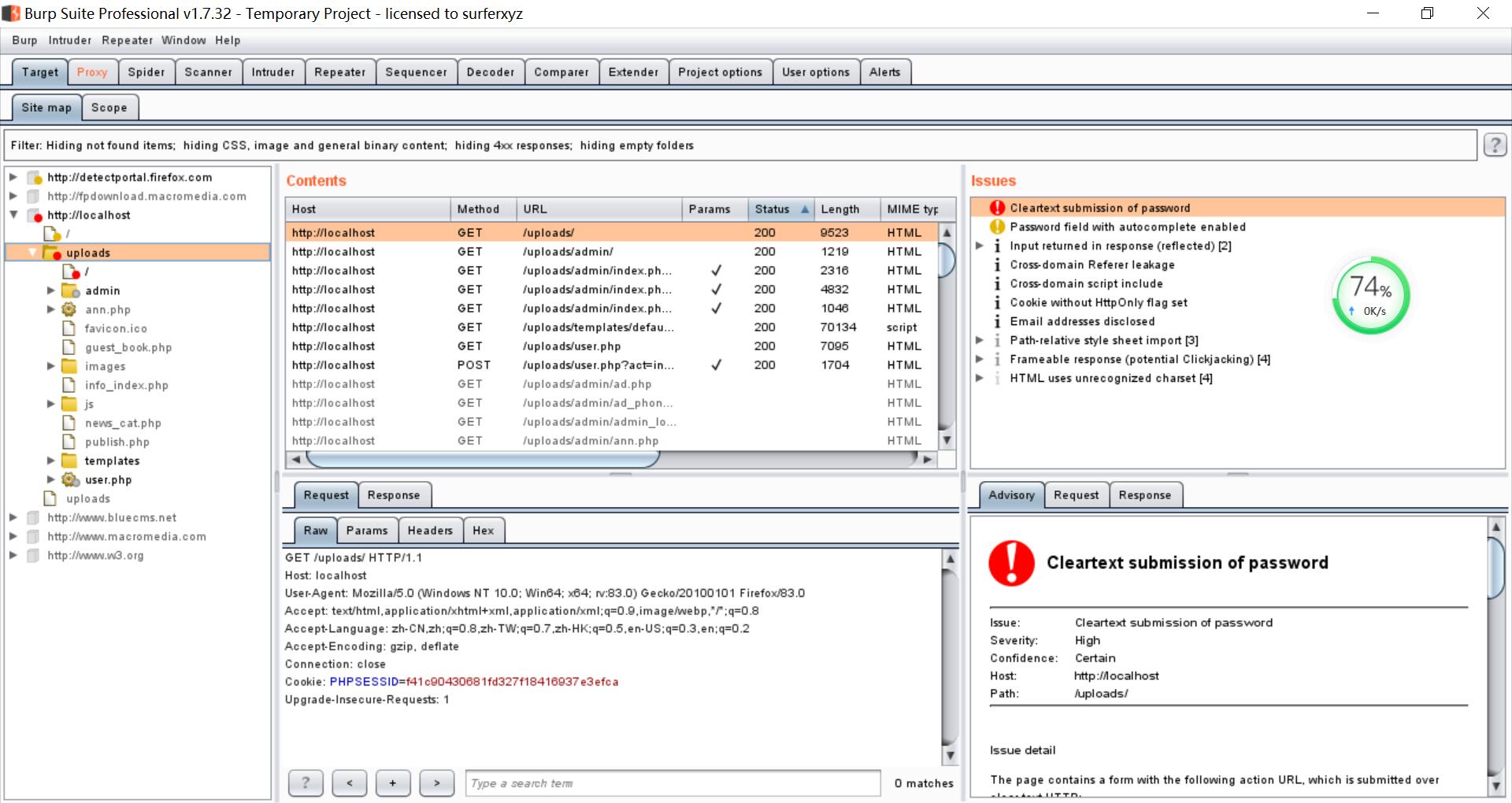
2.后台



漏洞分析：

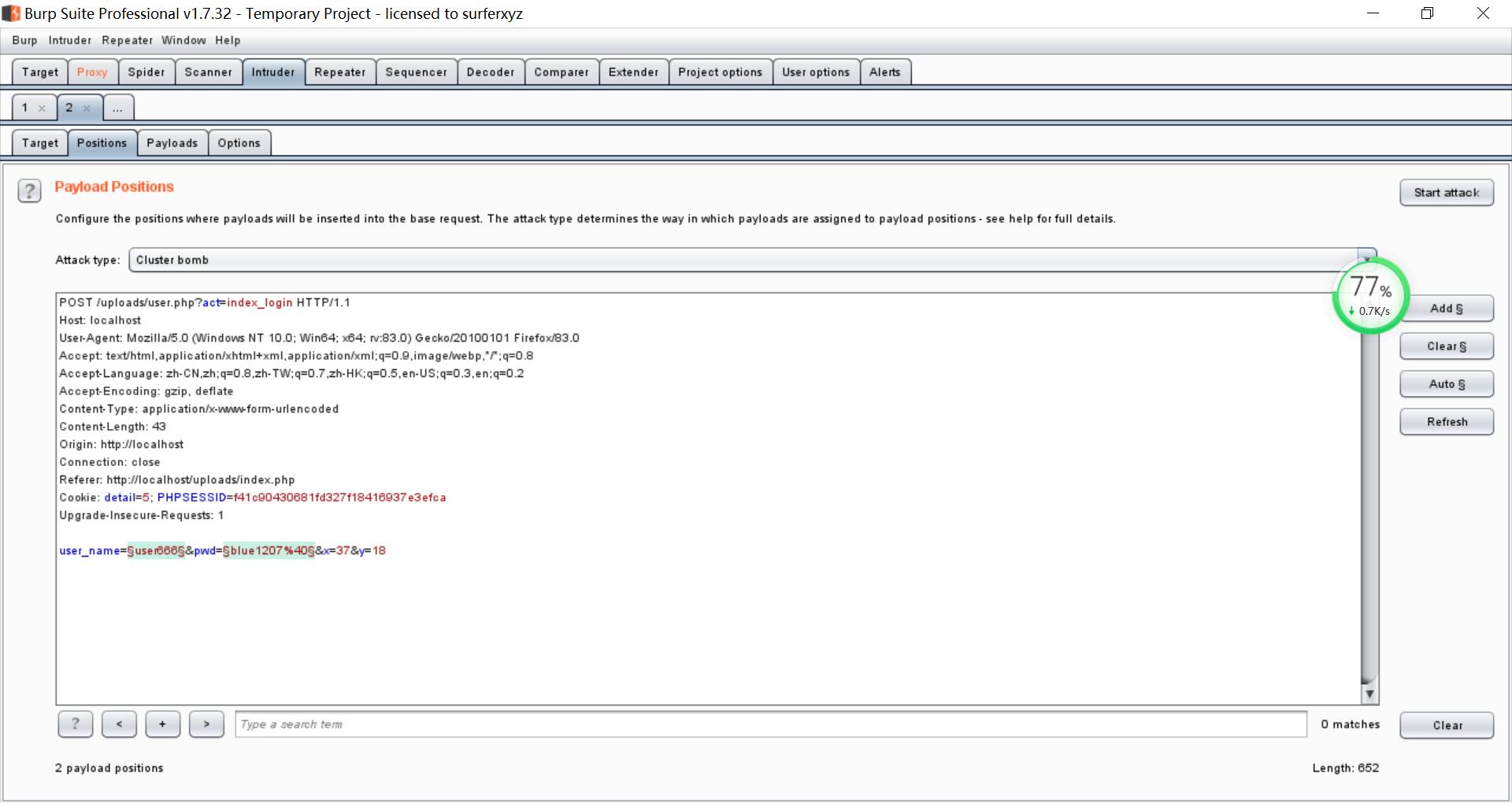
1. Frameable response (potential Clickjacking)：可框架响应（潜在的点击劫持）
2. HTML uses unrecognized charset：HTML 使用无法识别的字符集
3. Path-relative style sheet import：路径相关样式表导入
4. Cross-domain Referer leakage：跨域引用器泄漏
5. Input returned in response (reflected)：响应返回的输入（反射）

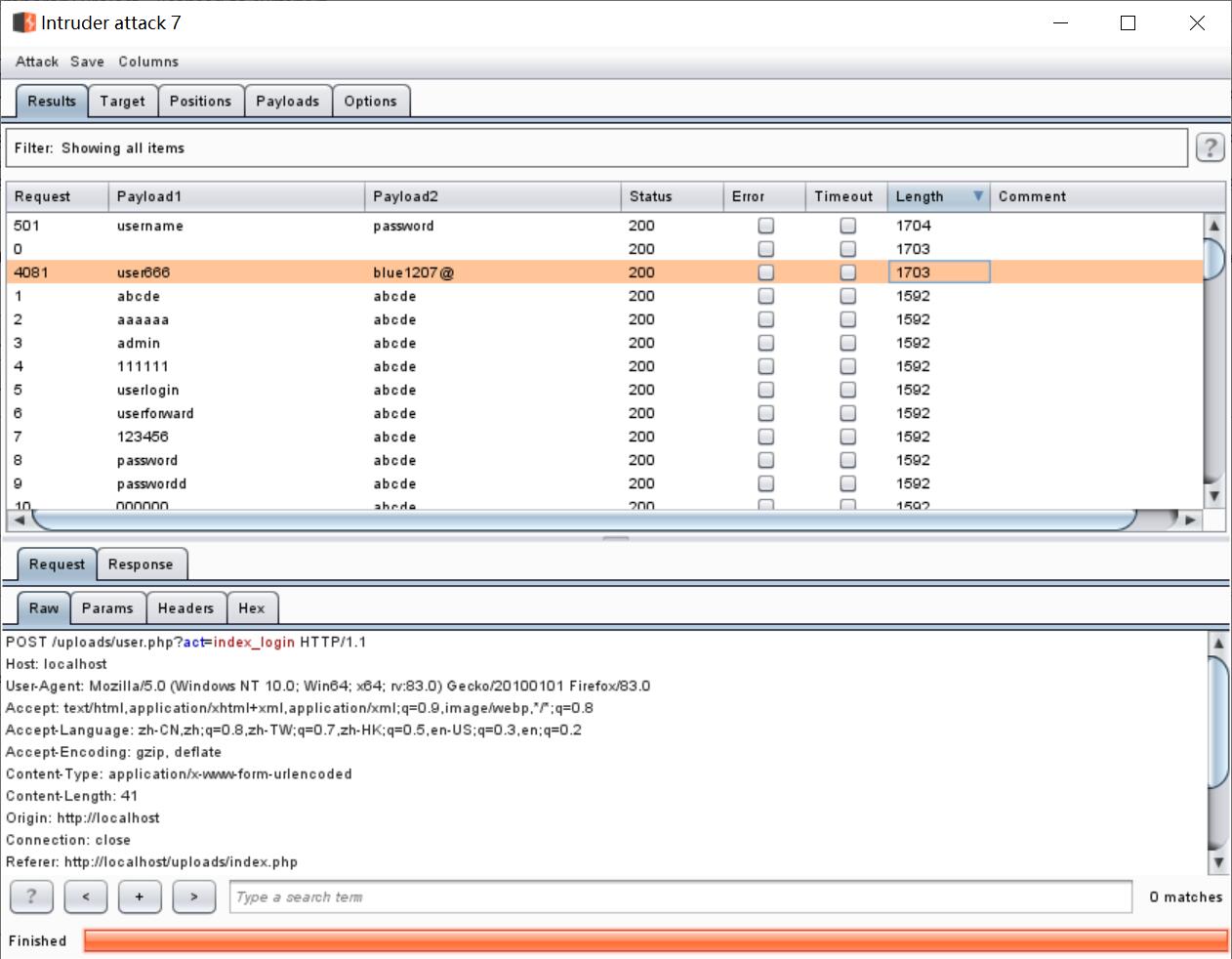
# 网站爬取



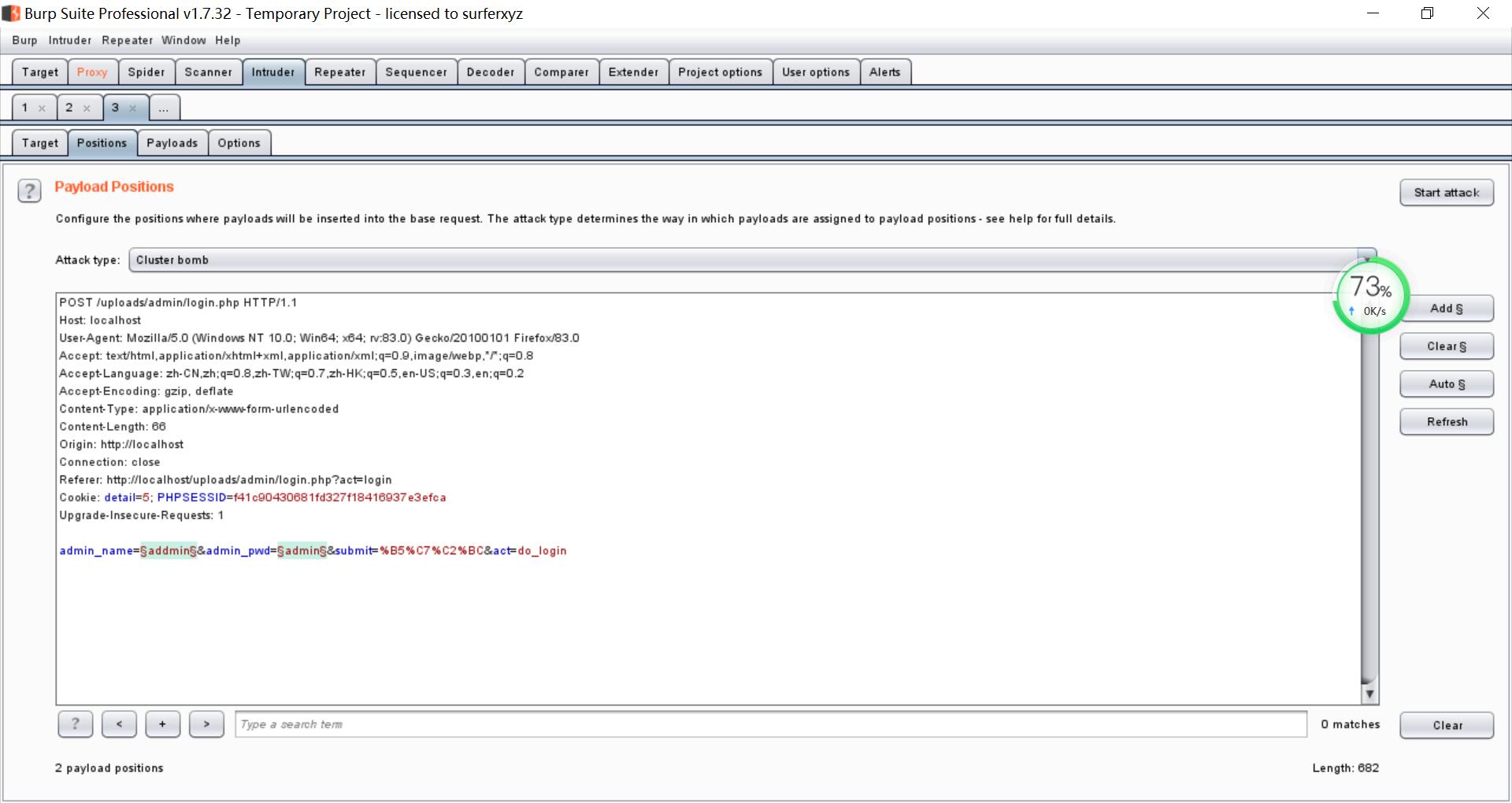
# 自动化攻击

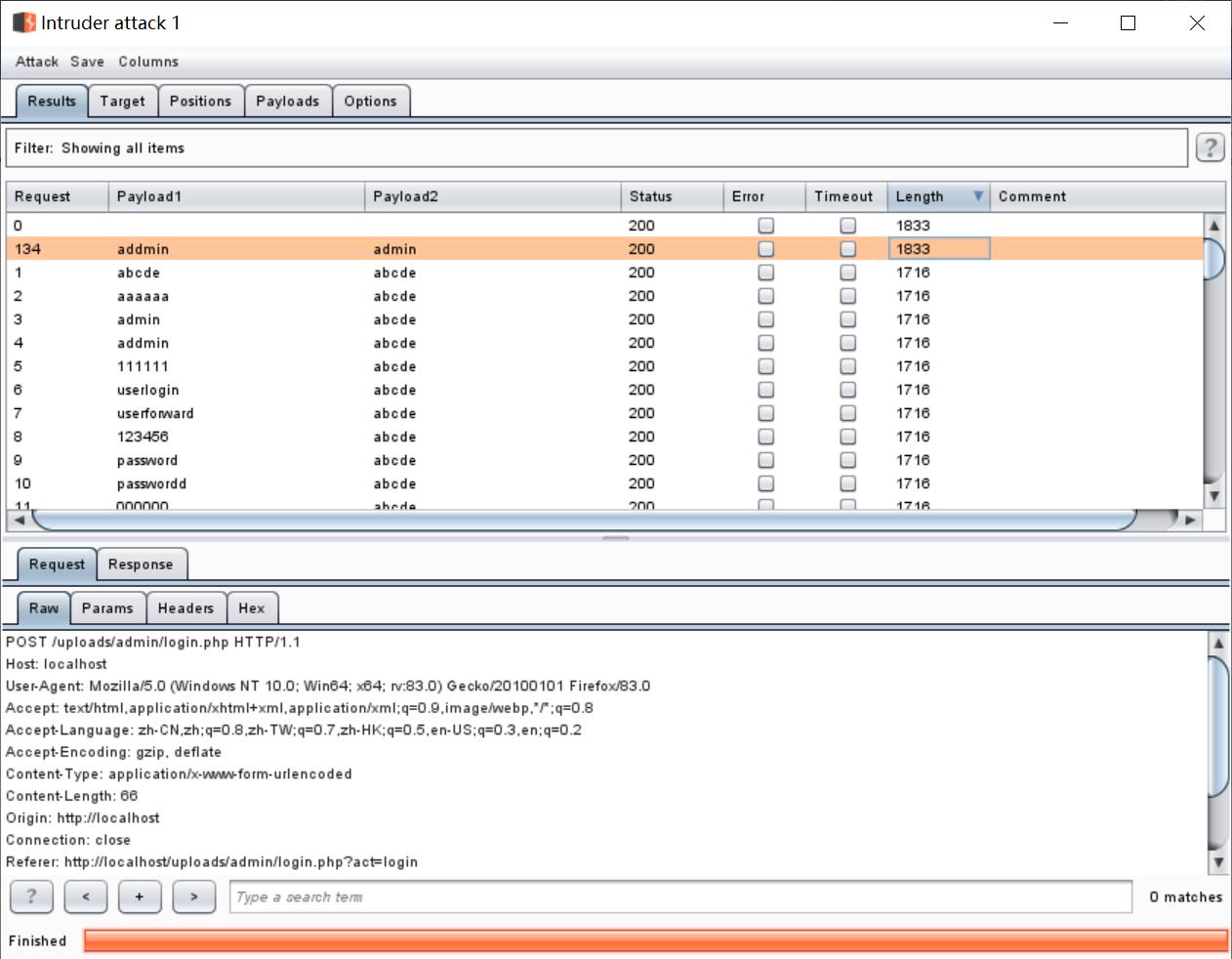
1.前端 用户名：user666 密码：blue1207@





2.后台 用户名：addmin 密码：admin





# 手工测试

XSS漏洞

1.前端

在搜索框、登录框、留言框中输入xss漏洞语句，没有出现alert提示框，说明前端没有xss漏洞。

2.后台-存在存储型xss漏洞

发布本地新闻-新闻标题框中输入xss漏洞语句，出现了alert提示框，说明此处有存储型xss漏洞。

