**对网站bluecms\_1.6进行渗透测试**

**信息搜集**

Ip：为本机183.197.98.83

服务器类型：windows

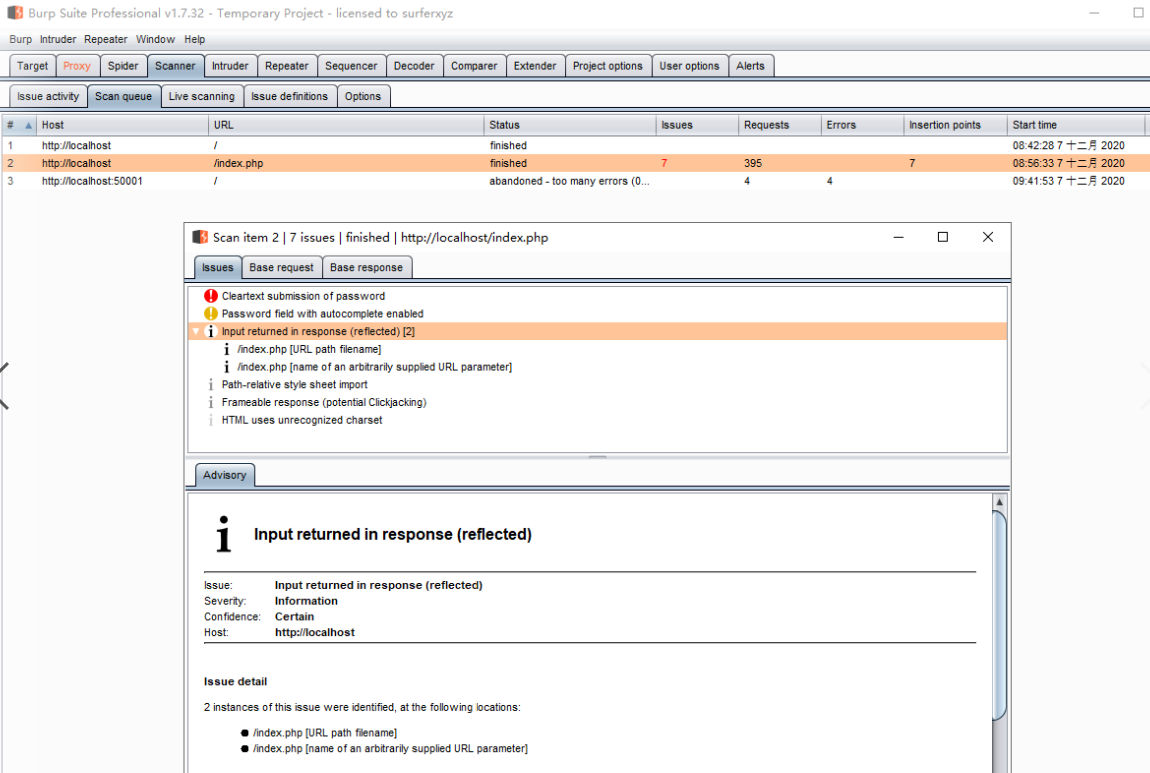
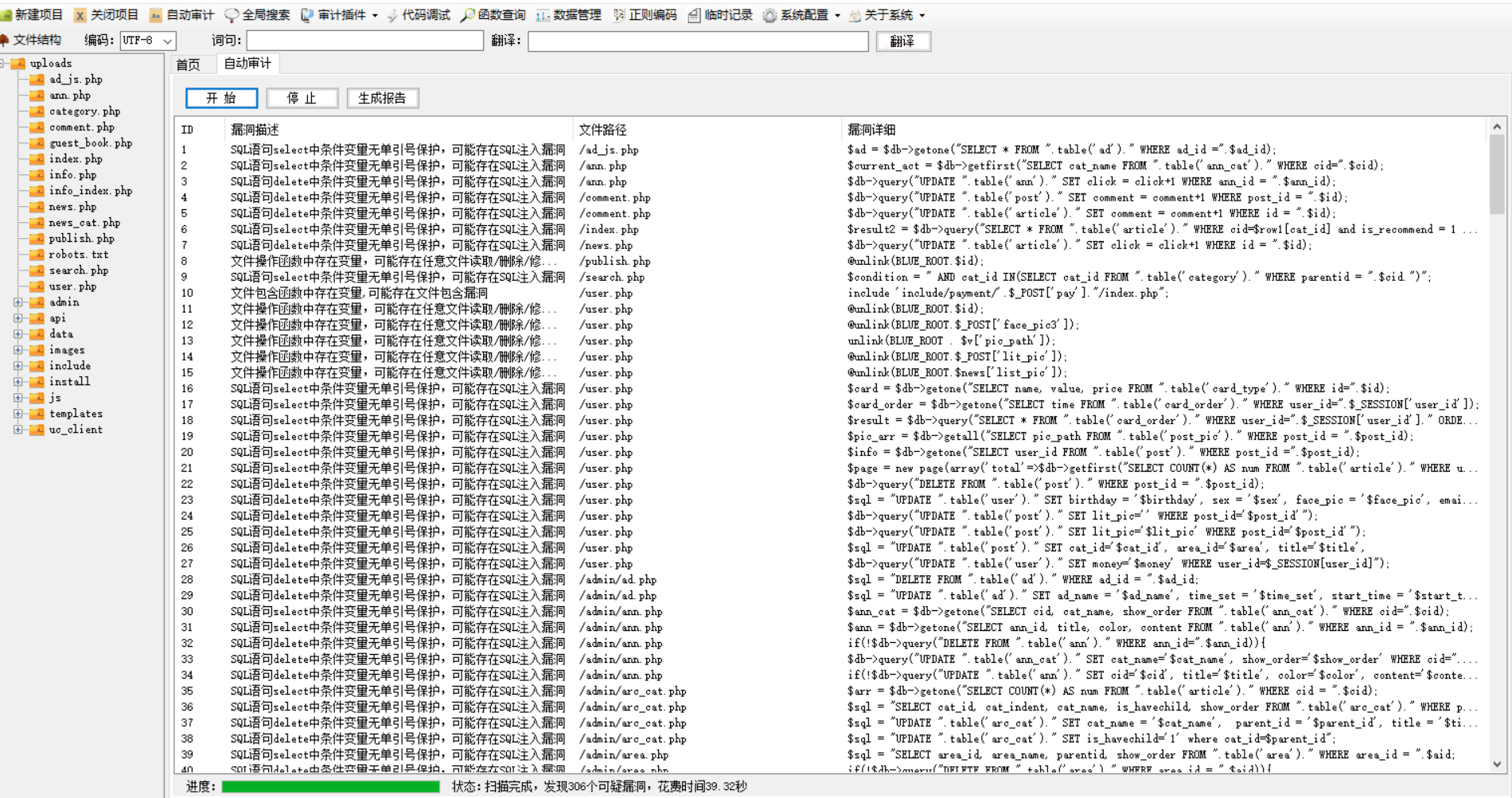
数据库类型：mysql

脚本类型：php

网站类型：apache

端口：MySQL3306

**漏洞扫描**



1.cleartext submission of password 明文提交密码

2.password field with autocomplete enable 启用自动完成功能的密码字段

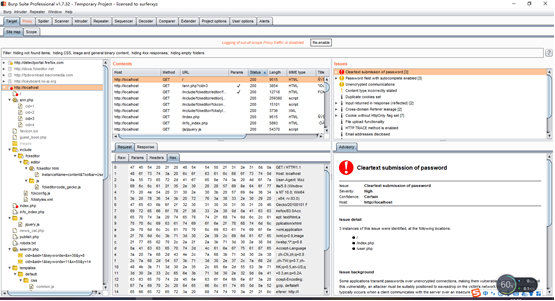
3,4 Input returned inresponse（reflectly）响应中返回的输入（反射）

5. Path-relative style sheet import导入相对路径样式表

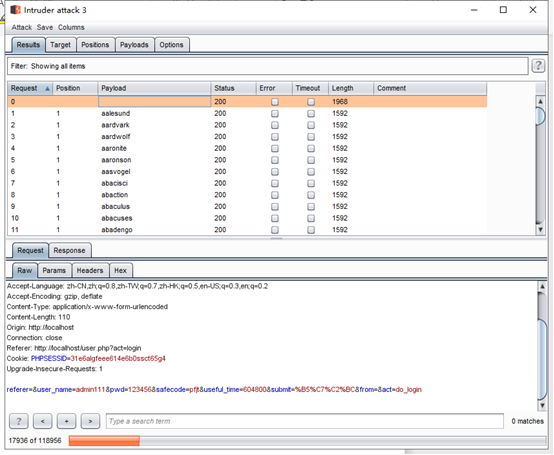
6. Frameable response（potential clickjacking）可帧响应（潜在的点击劫持）

7. HTML uses recongized charets HTML使用重新定义的字符

**爬取网站**



**自动化攻击**



**手工测试**

**Xss漏洞**



