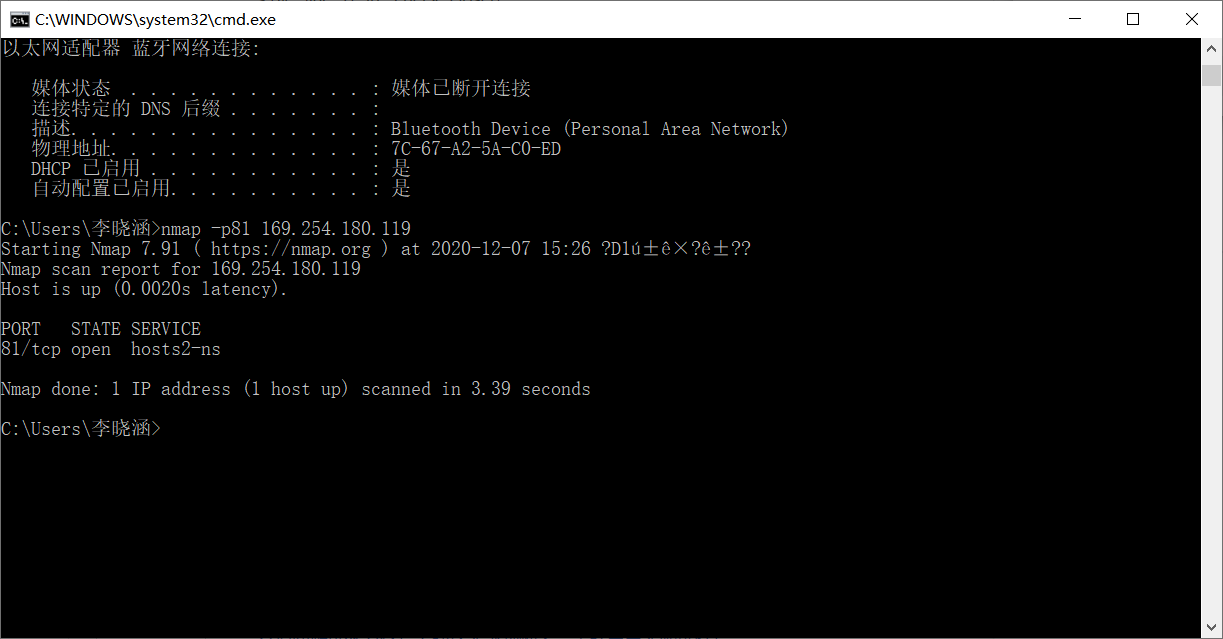
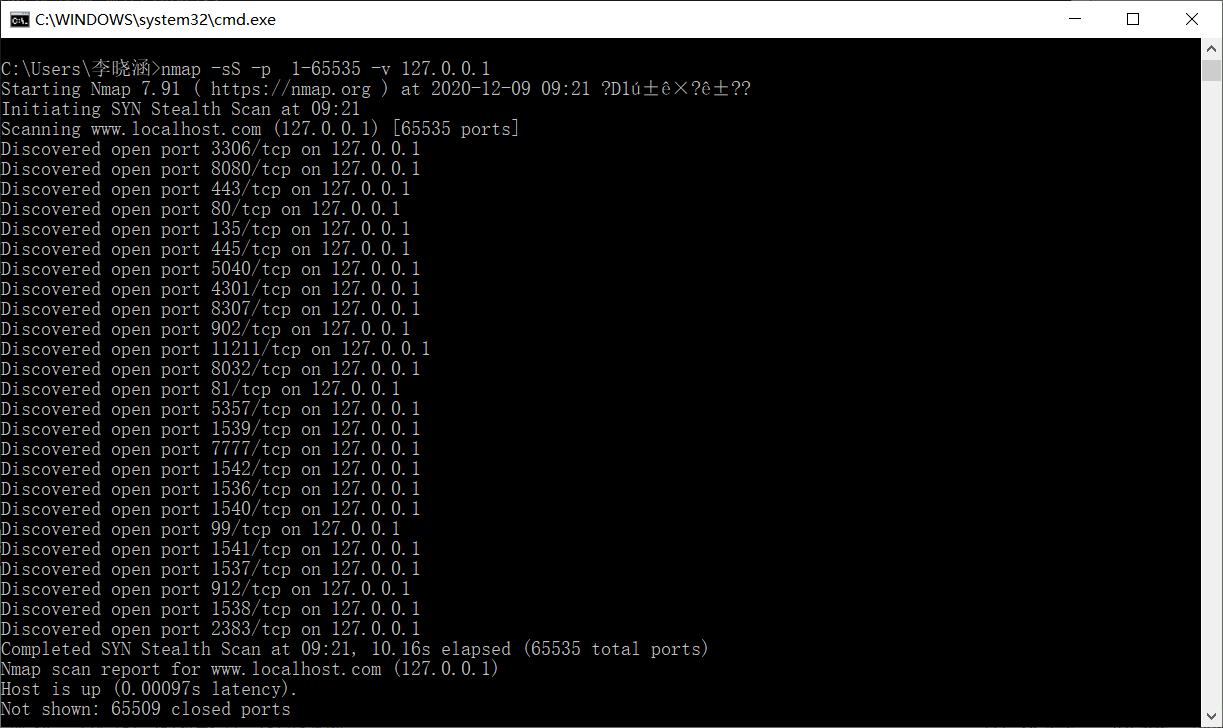
一、信息收集

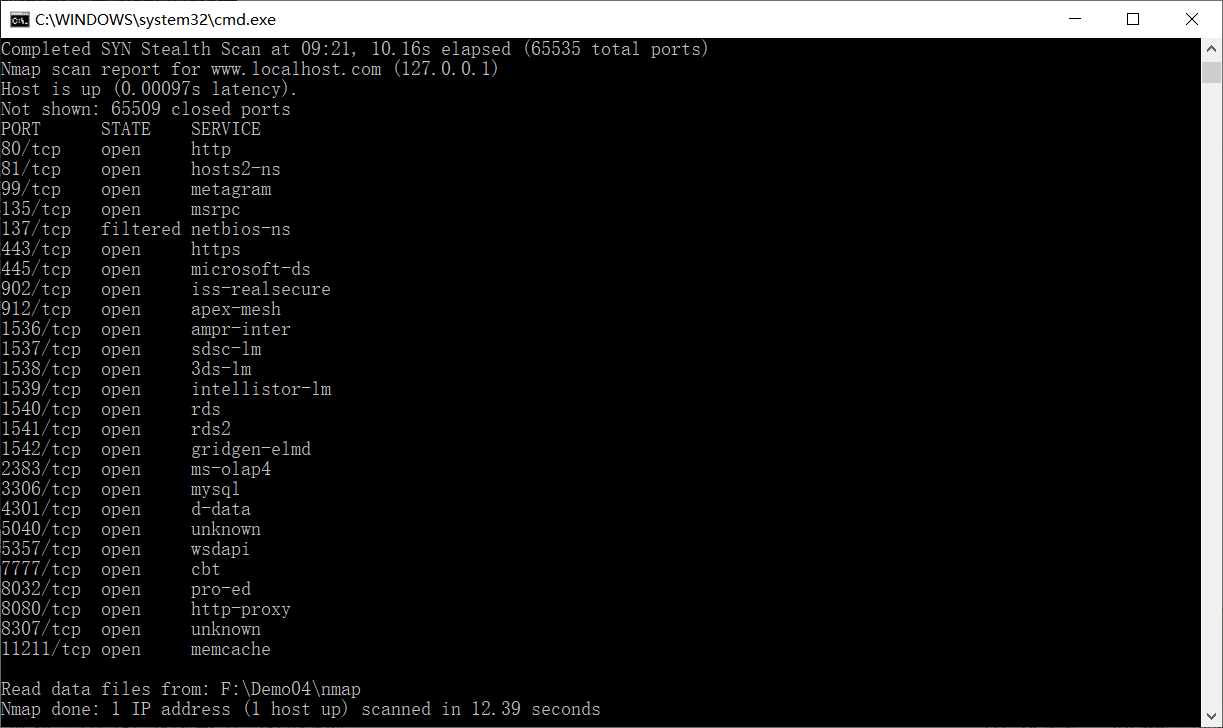
为burpsuit网站分配端口号为81，并扫描81端口：





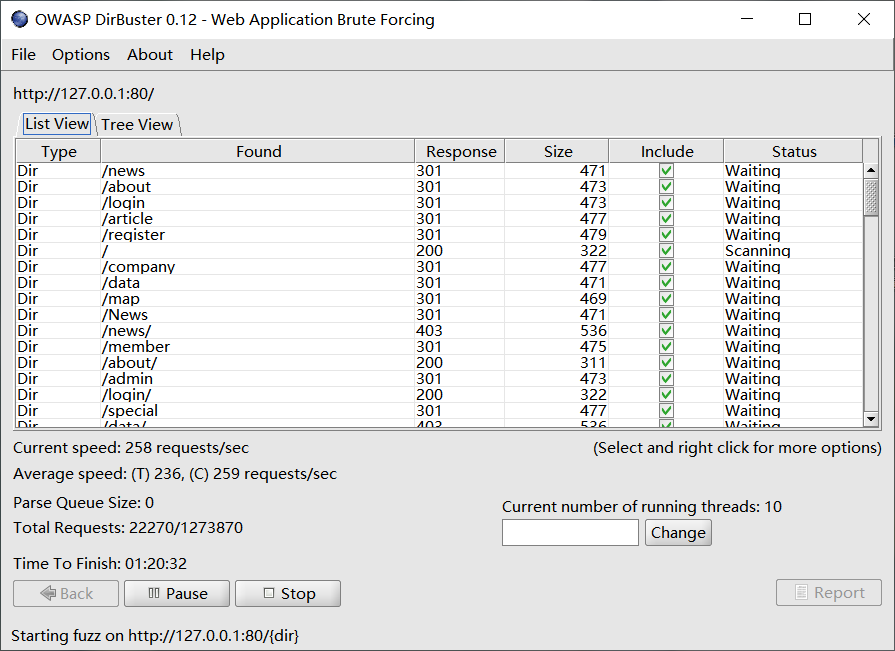
命令行执行结果显示：端口号81 协议tcp 状态open 服务hosts2-ns



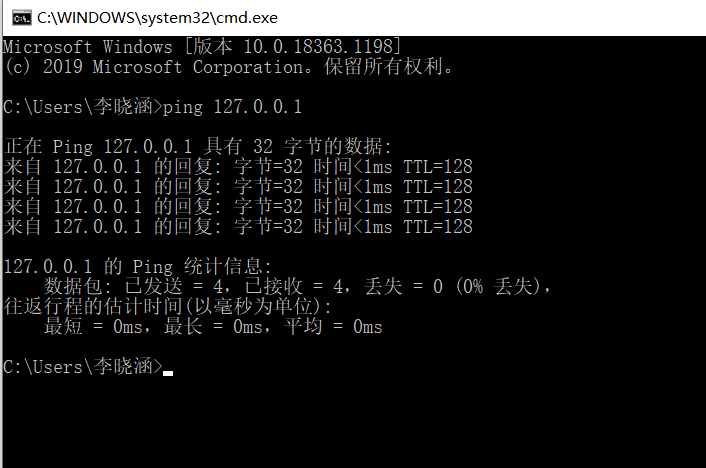


敏感信息扫描

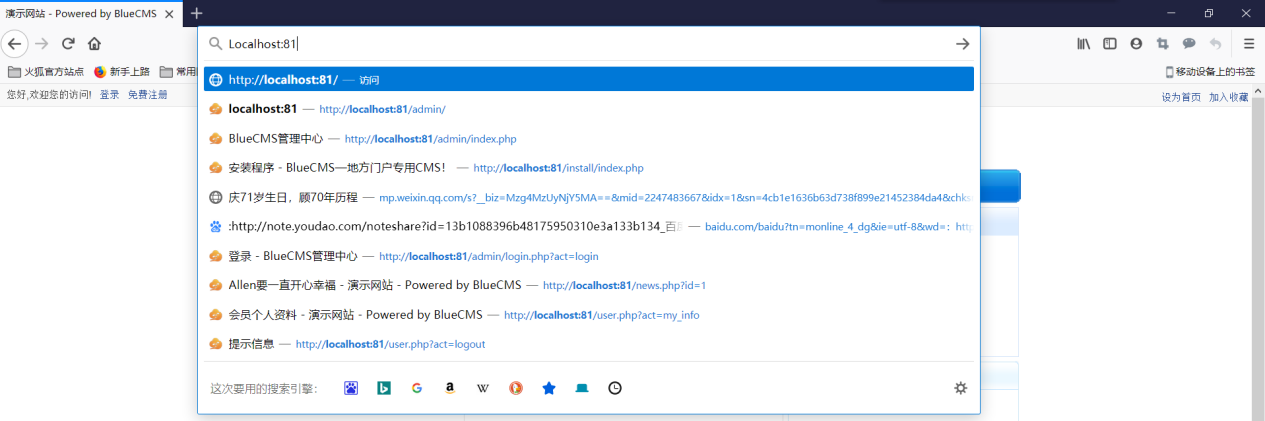
![XQ}0@L~(N[ZQ]`](PTO_C[I](data:image/png;base64,)



整站分析



为windows系统



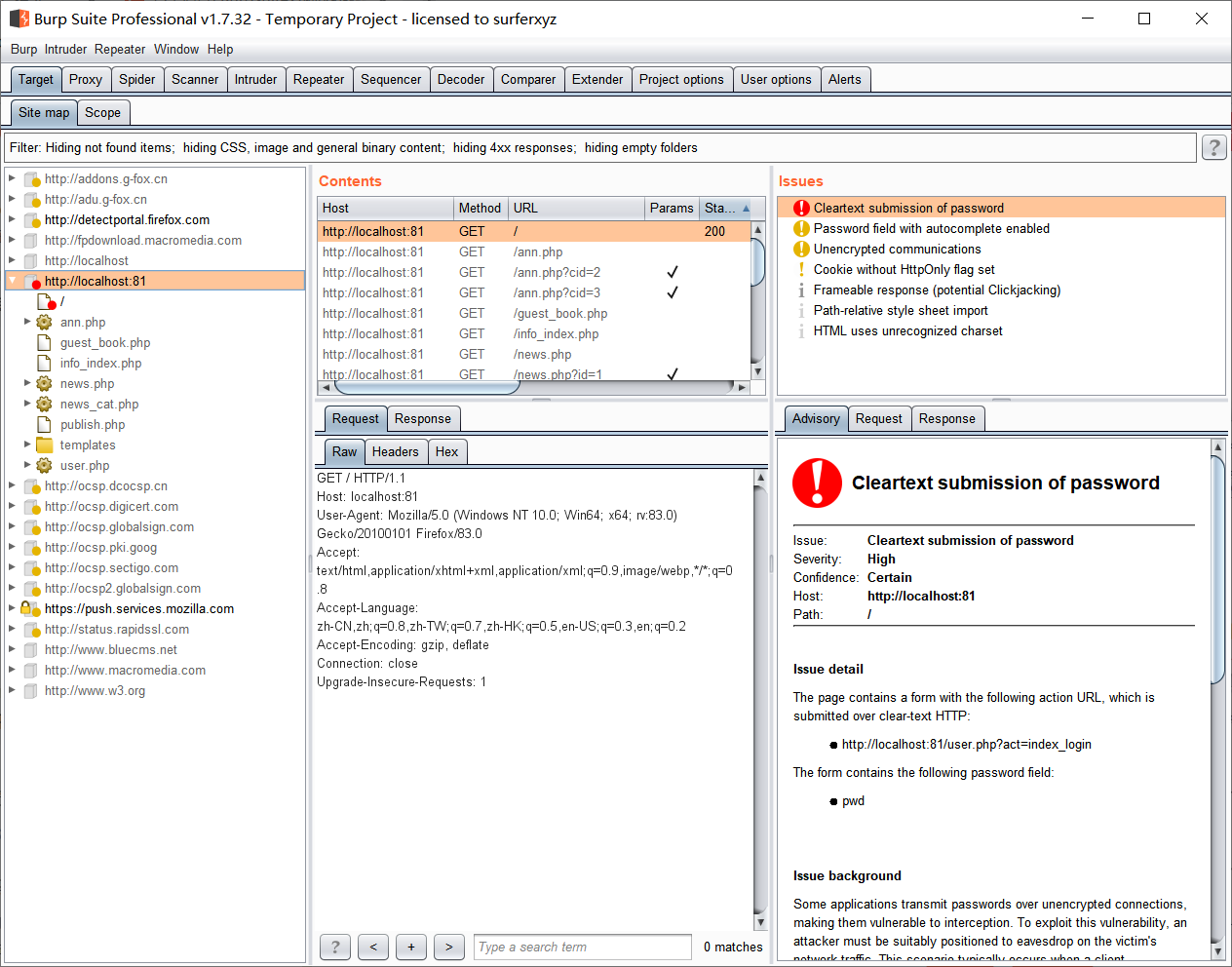


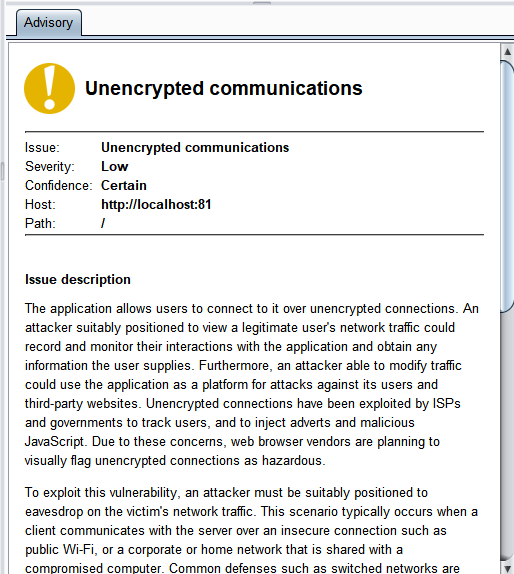
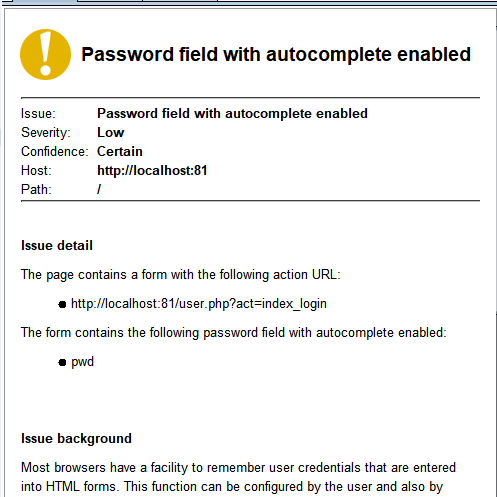
url中某些字母改为大写，仍然能访问，则判断其是Windows系统.

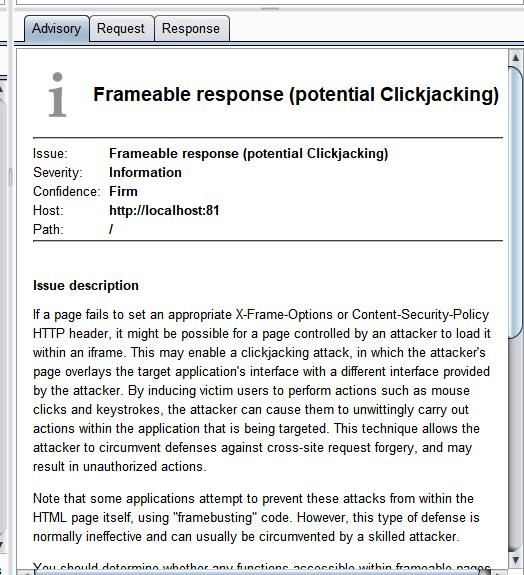
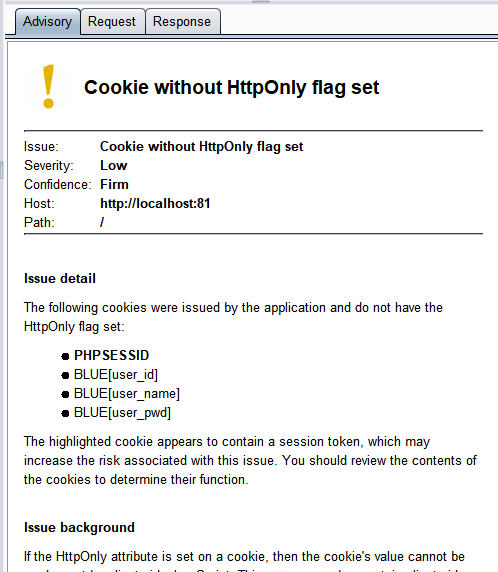


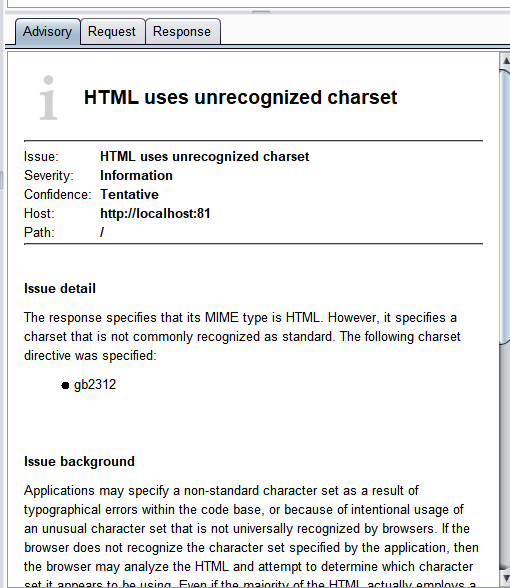
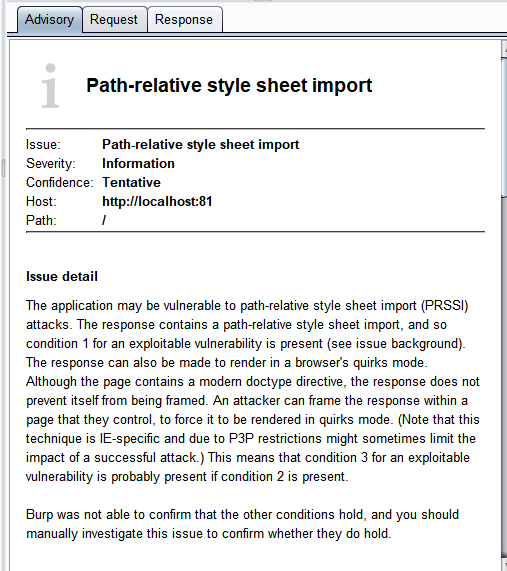
1. 使用burpsuit进行漏洞扫描

1、前端









共有七处漏洞：

①cleartext submission of password明文提交密码（severity：High）

②password field with autocomplete enabled启用自动完成功能的密码字段（severity：Low）

③unencrypted communication未加密通信（severity：Low）

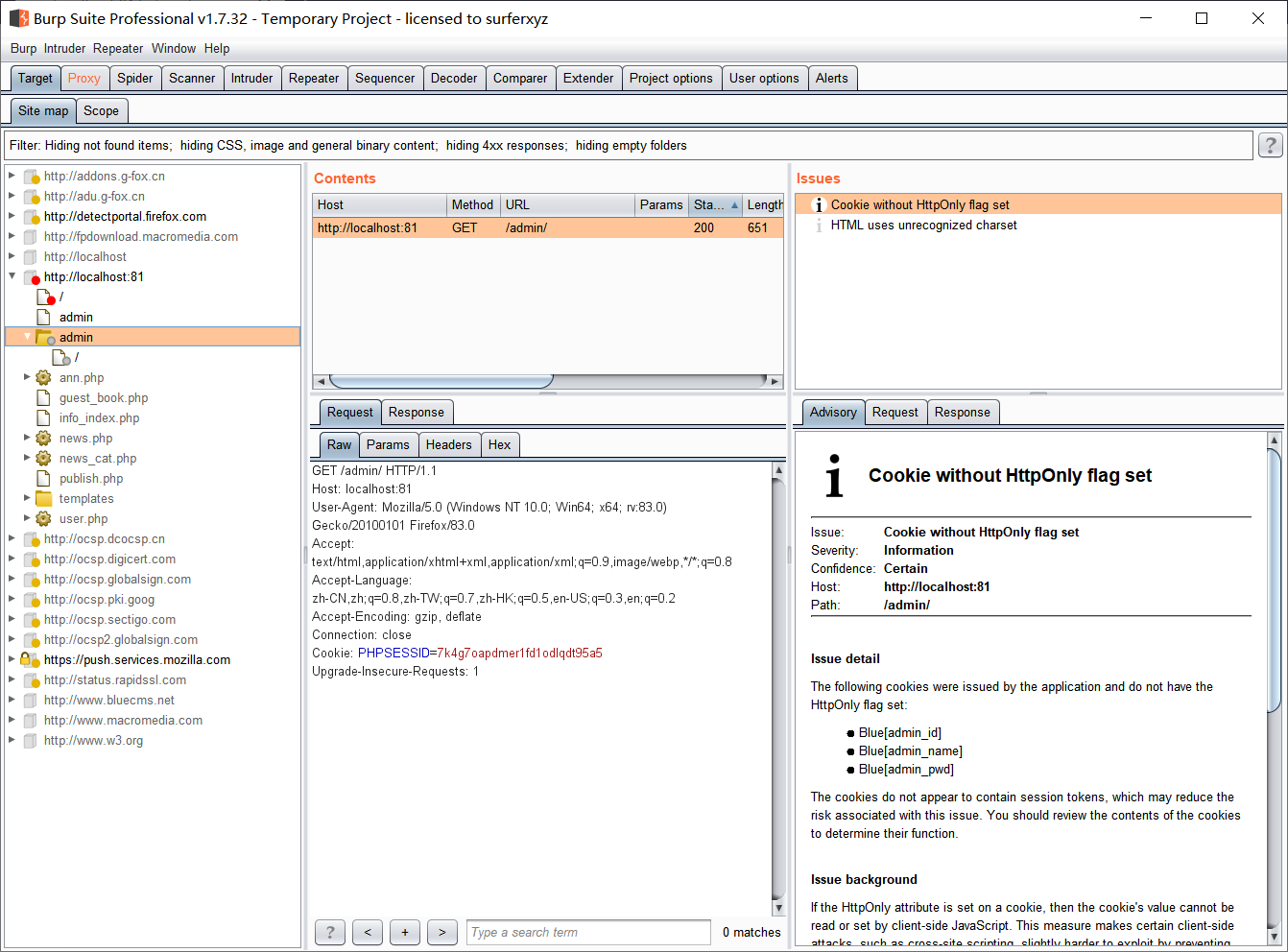
④cookie without HttpOnly flag set未设置HttpOnly标志的cookie（severity：Low）

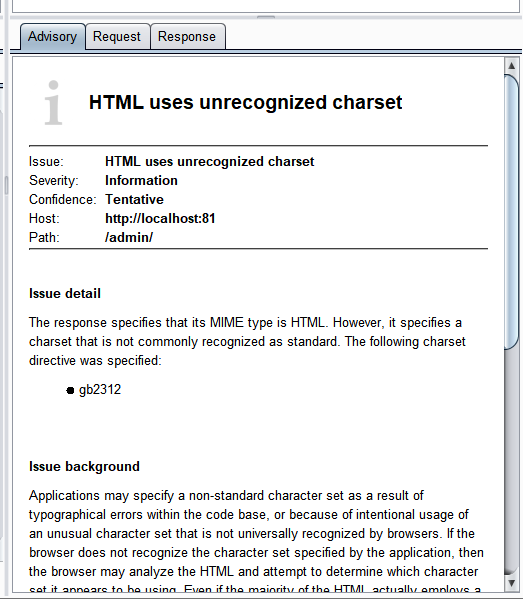
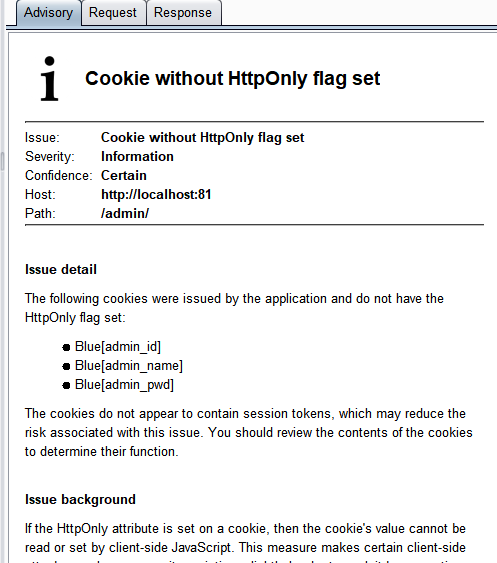
⑤frameable response(potencial clickjacking)框架响应（潜在点击劫持）（severity：information）

⑥path-relative style sheet import路径相关样式表导入（severity：information）

⑦HTML uses unrecognized charset HTML使用未识别的字符集（severity：information）

1. 后台

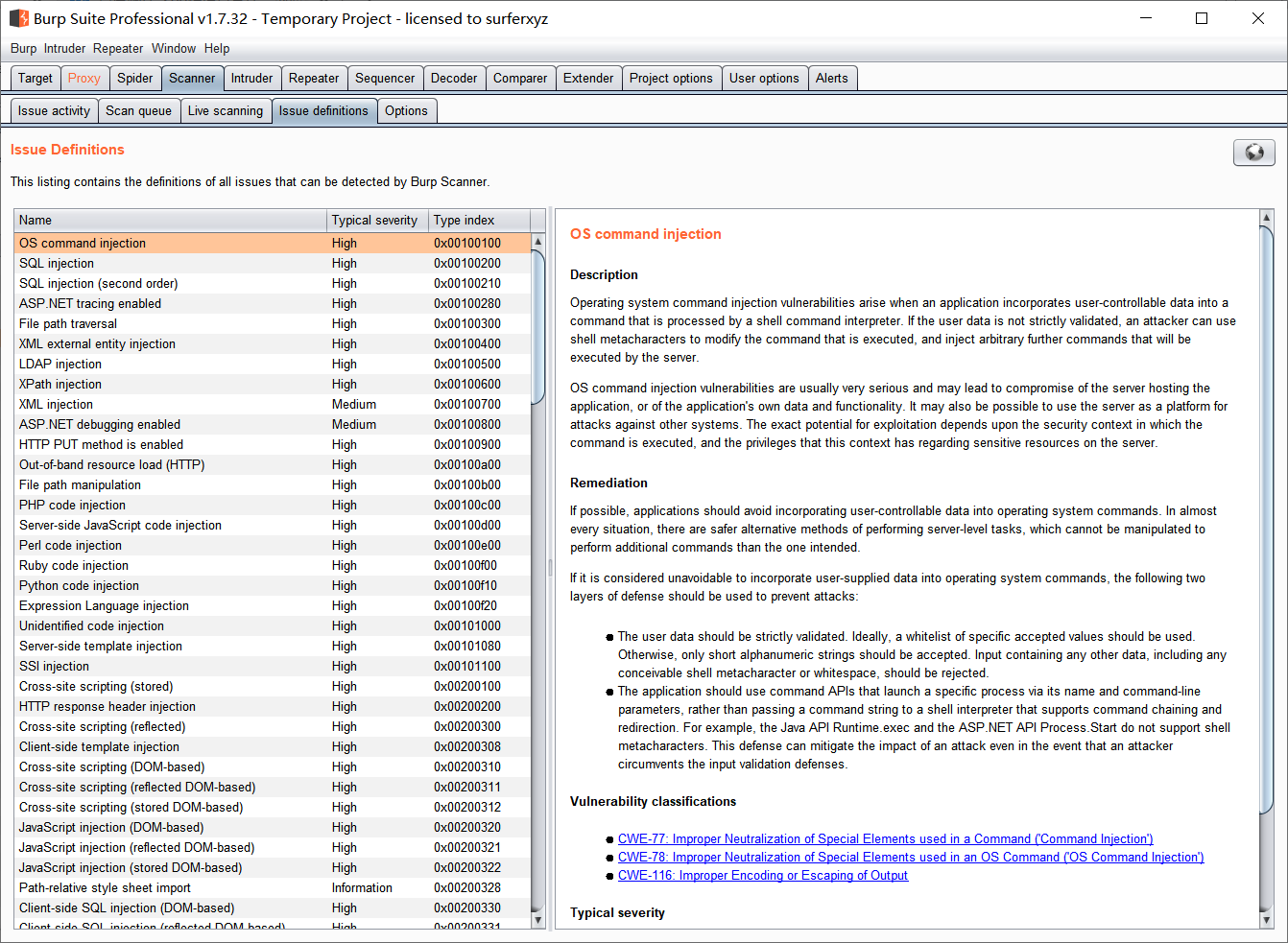




共有两处漏洞：

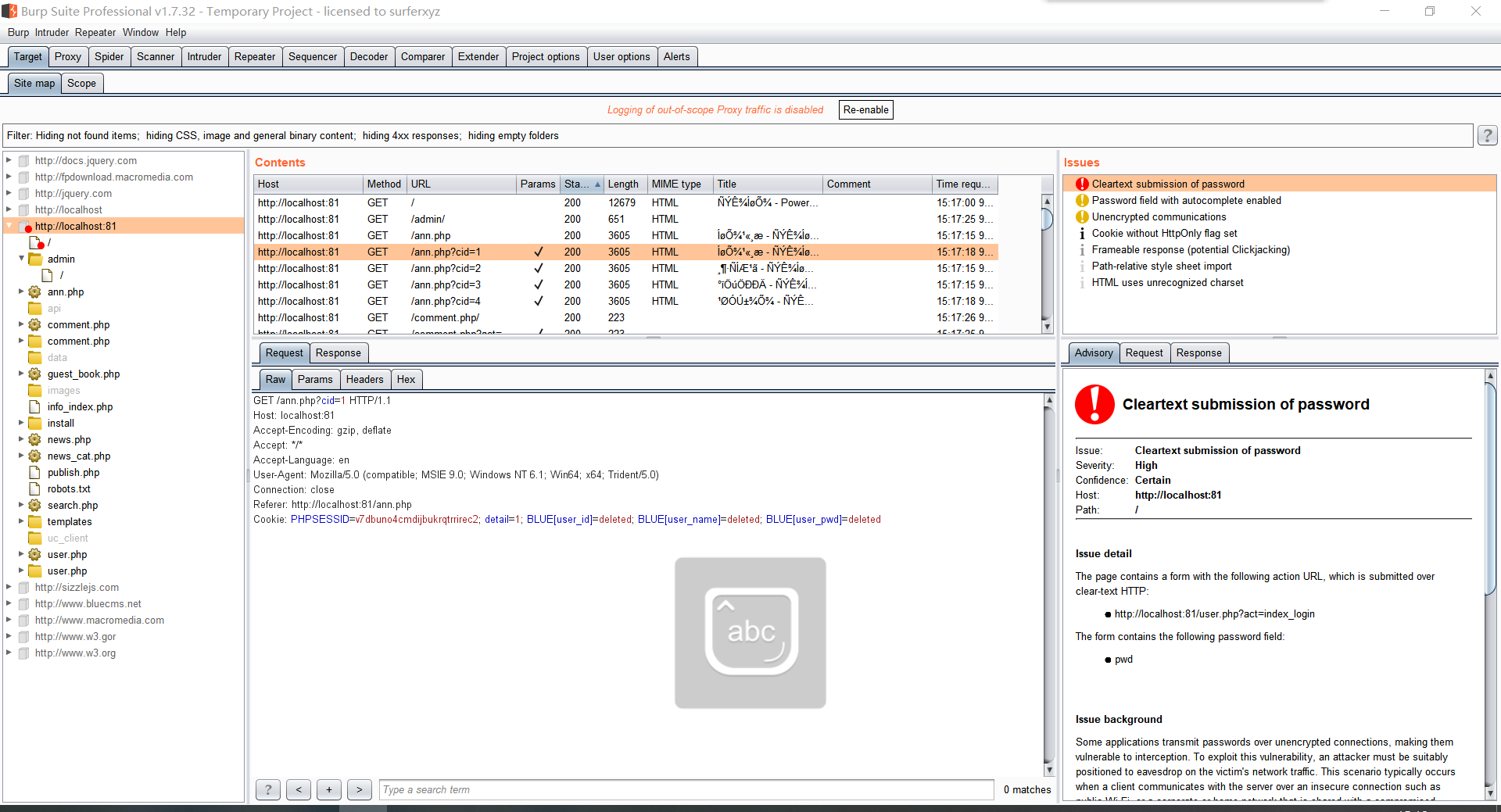
①HTML uses unrecognized charset HTML使用未识别的字符集（severity：information）

②cookie without HttpOnly flag set未设置HttpOnly标志的cookie（severity：information）

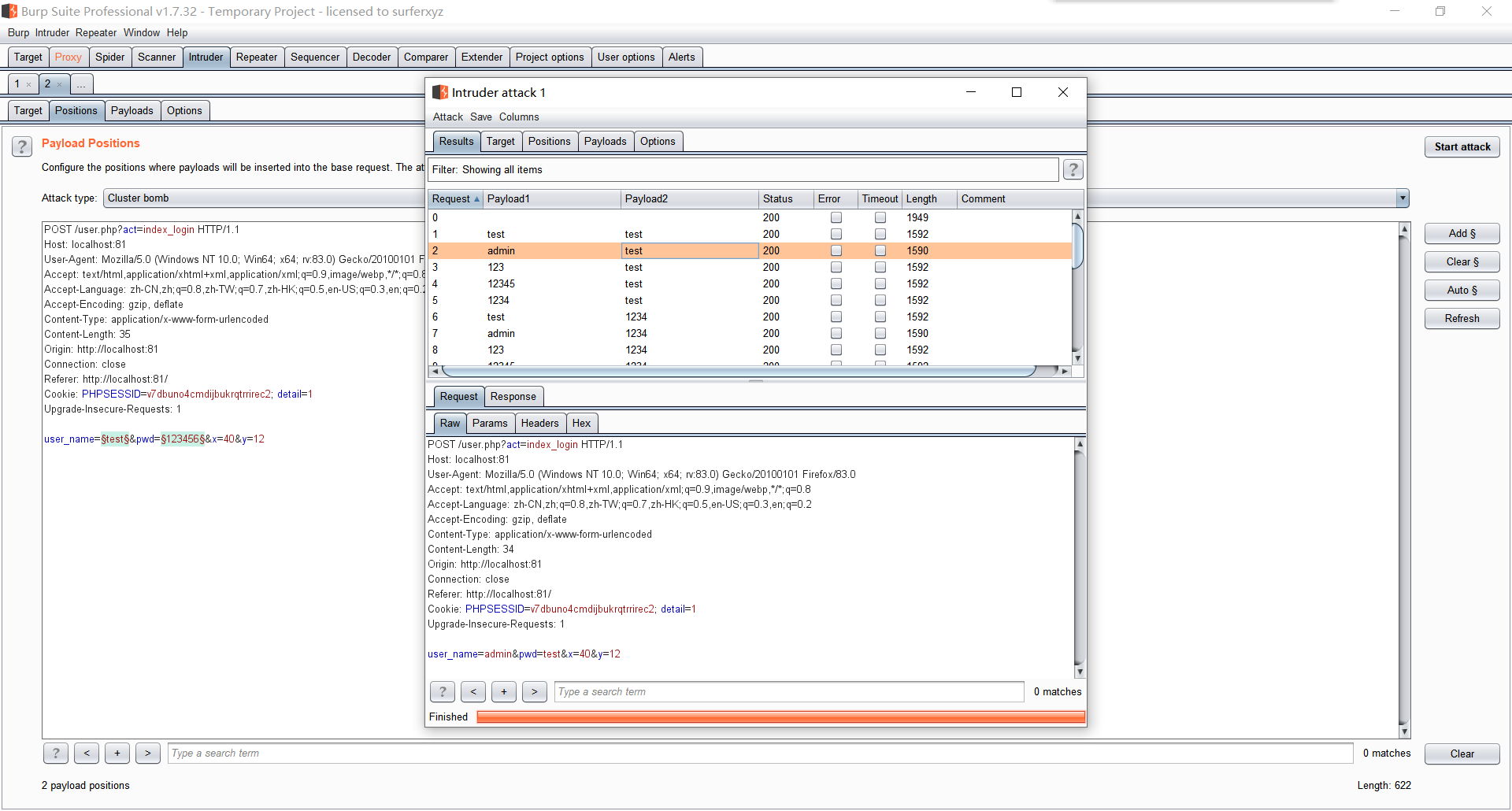


Scan漏洞

漏洞爬取



密码爆破



三、Xss漏洞

