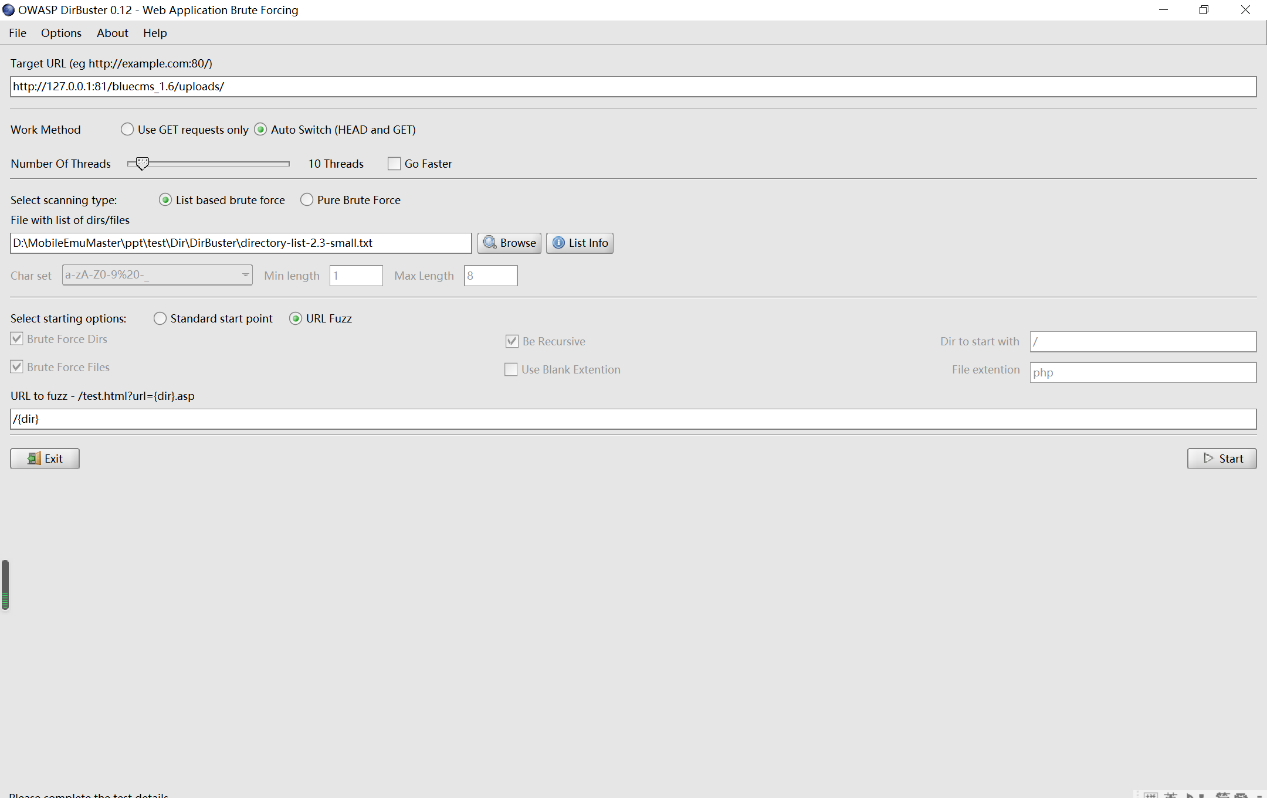
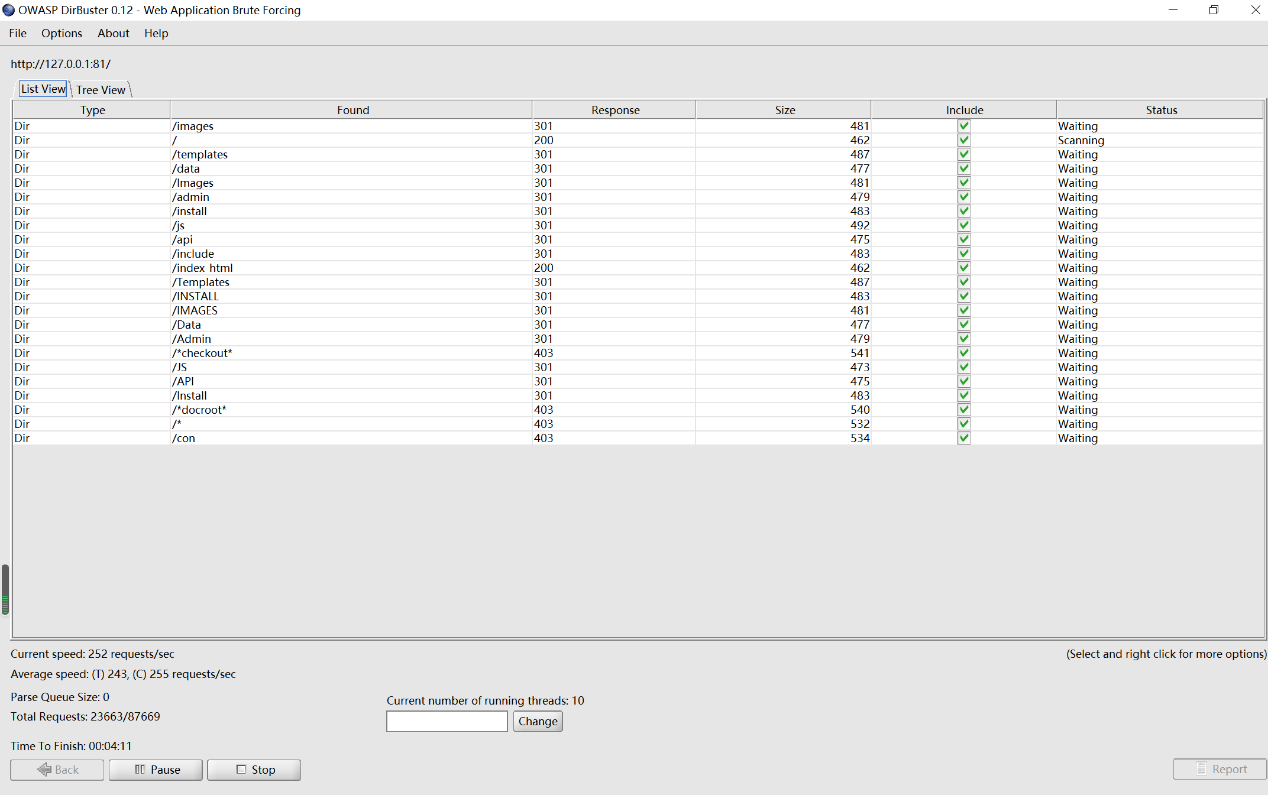
信息收集

域名信息

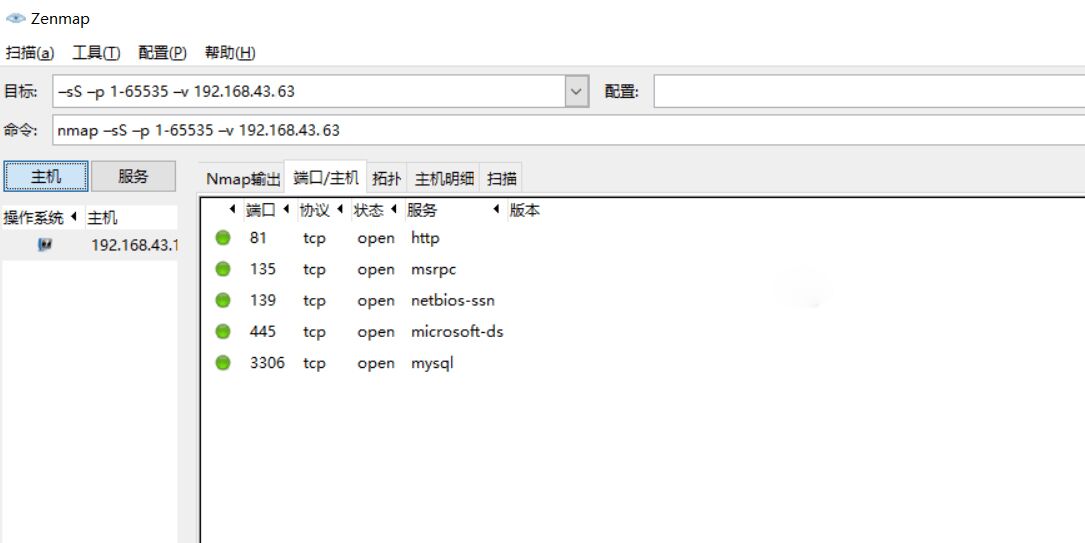
网站搭建再本机，没有域名信息

敏感目录





端口扫描：



整站分析：

服务器的操作系统为windows

网站容器为apache

脚本类型php

数据库为mysql

漏洞扫描：

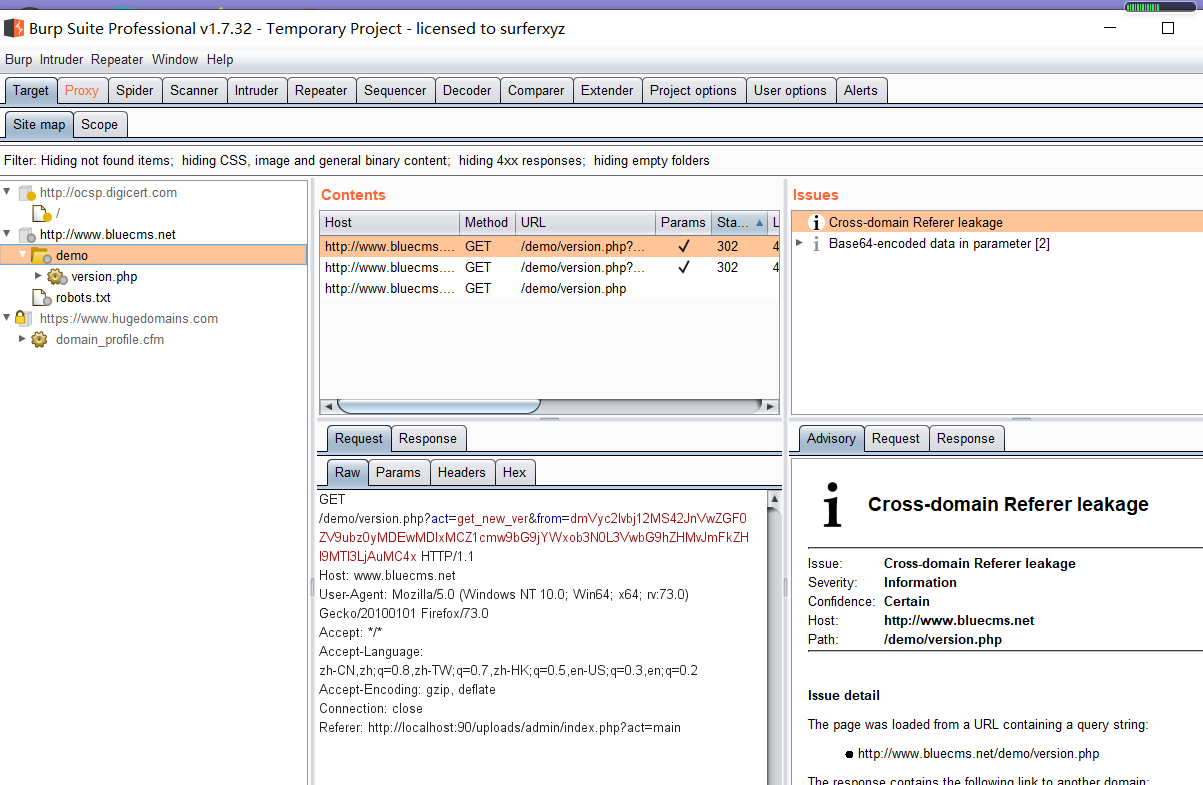
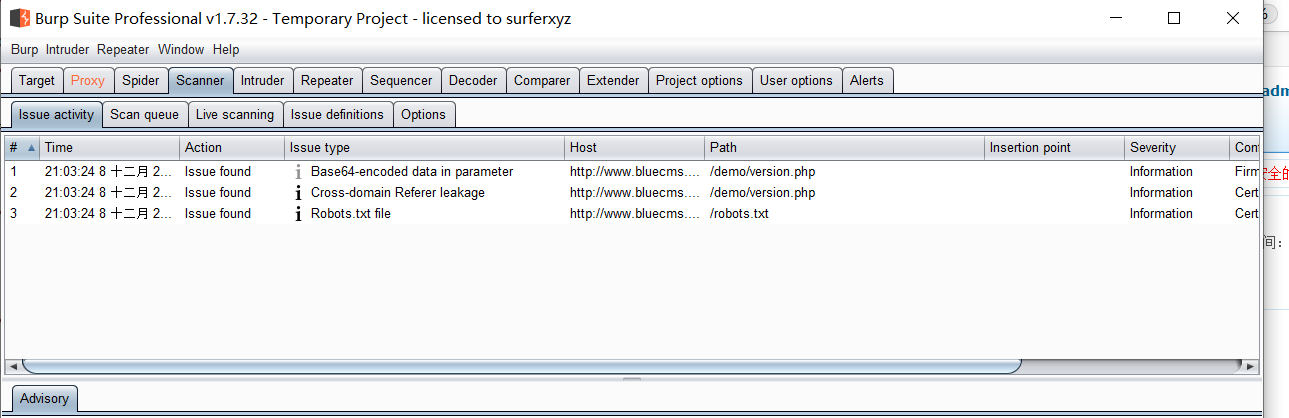




漏洞：

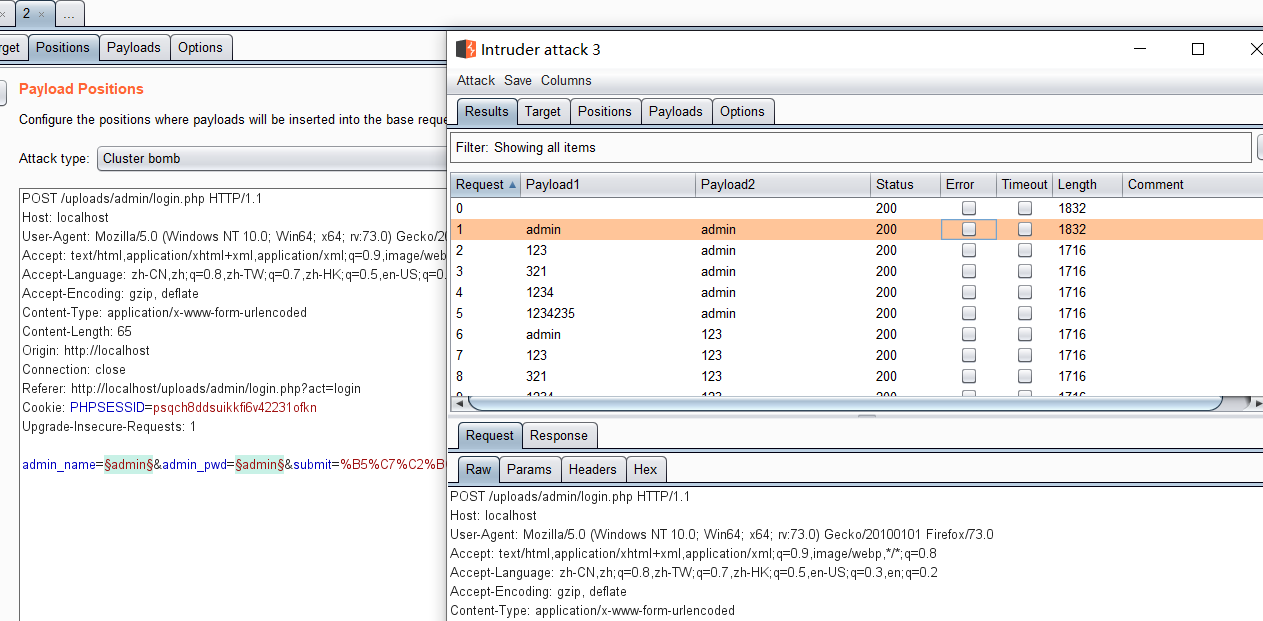
1. unencrypted communications:未加密通信
2. Cookie without HttpOnly flag set:未设置HttpOnly标志的Cookie
3. Password field with autocomplete enabled：用户输入的凭据将存储在本地计算机上，攻击者可以捕获存储的凭据，攻击者可以控制用户的计算机。
4. Cookie without HttpOnly flag set：未设置httponly的cookie，许多其他严重的攻击也可以通过客户端脚本注入来实现
5. Input returned in response(reflected):相应返回的输入
6. unencrypted communications:未加密通信
7. Frameable response (potential Clickjacking)：可Frameable响应、潜在点击劫持
8. HTML uses unrecognized charset：HTML使用未识别的字符集
9. Cross-domain Referer leakage：跨域引用泄露
10. password filed with autocomplete enable:密码字段自动完成启用

爬取网站:



自动化攻击：

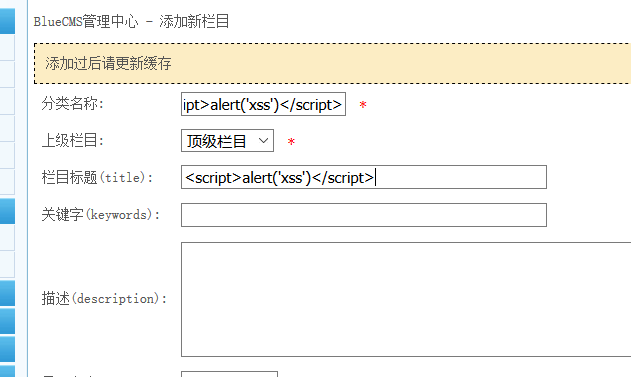
在前台登录界面，进行密码爆破，找了一个密码字典，采用cluster bomb



手工测试：

在登录界面，输入SQL语句**'or 1=1--**，没有成功

添加新闻分类，存在xss漏洞



发布本地新闻，有xss漏洞



添加栏目有xss漏洞

