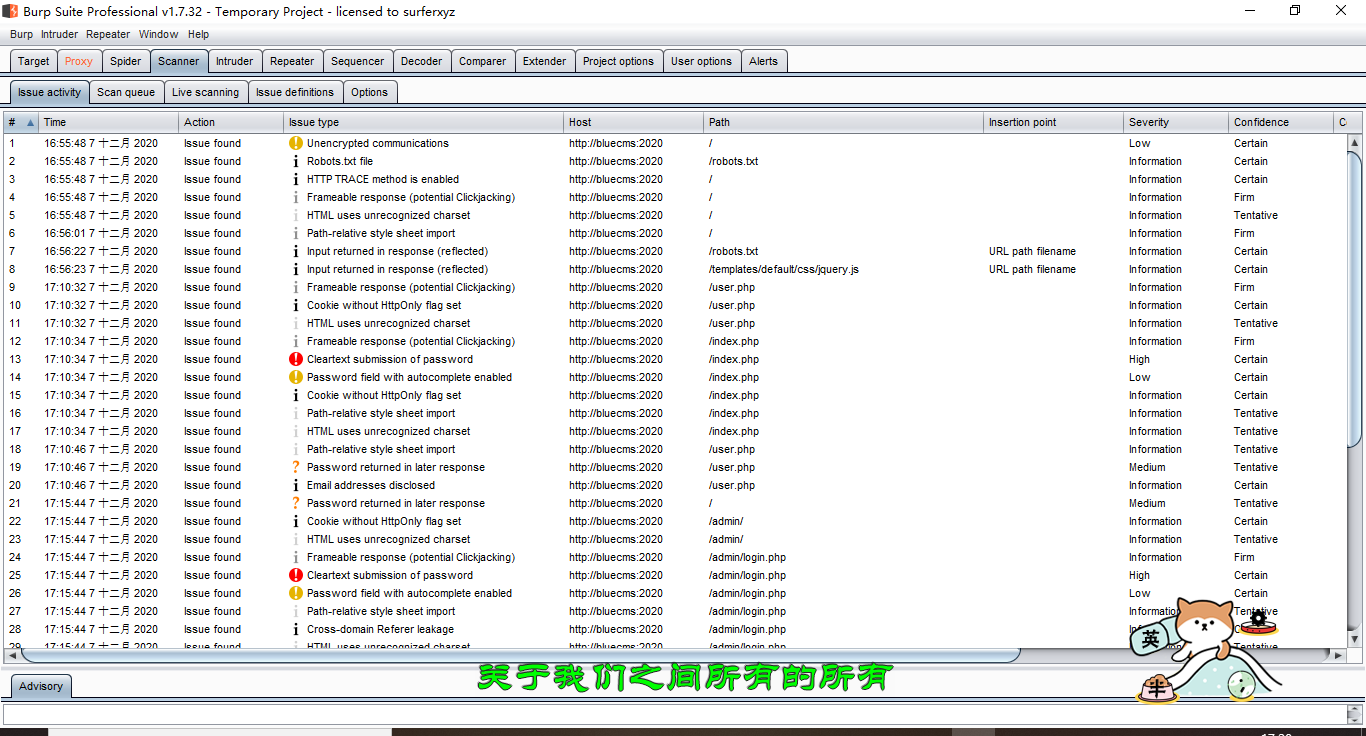
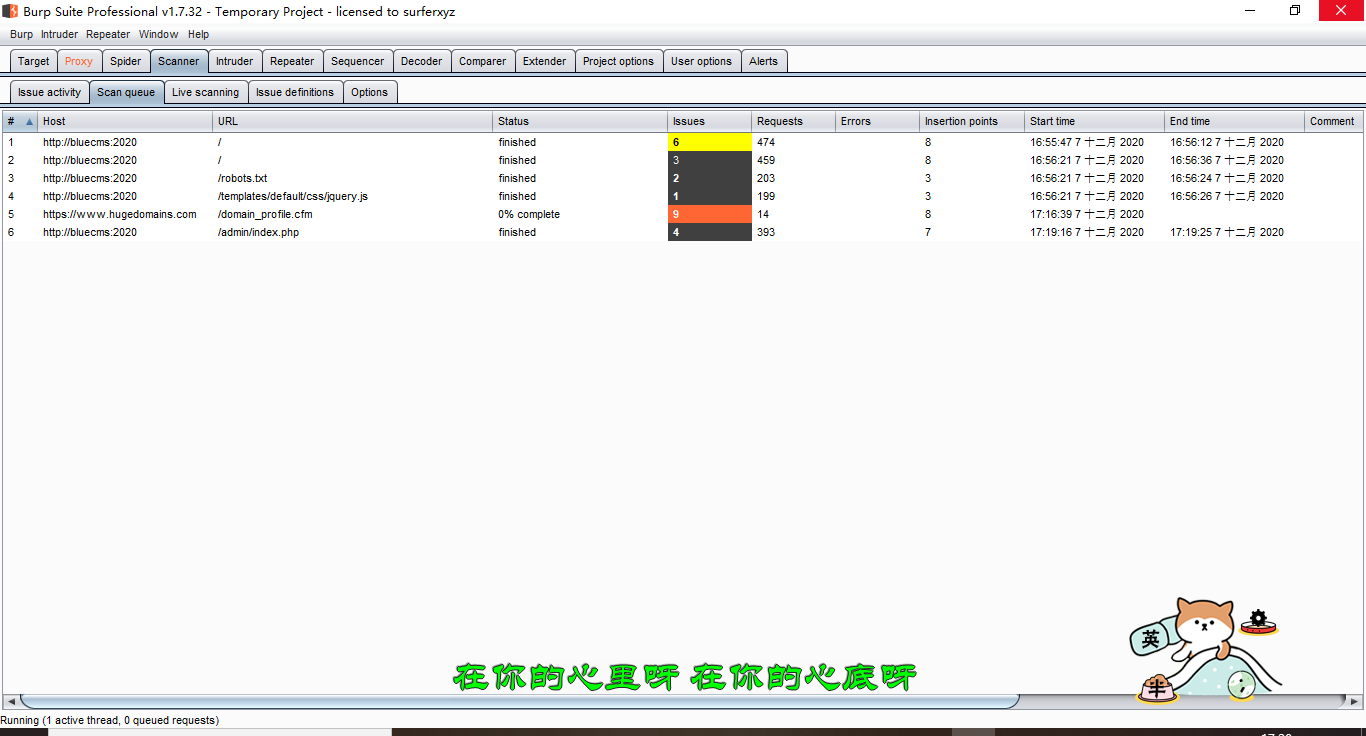
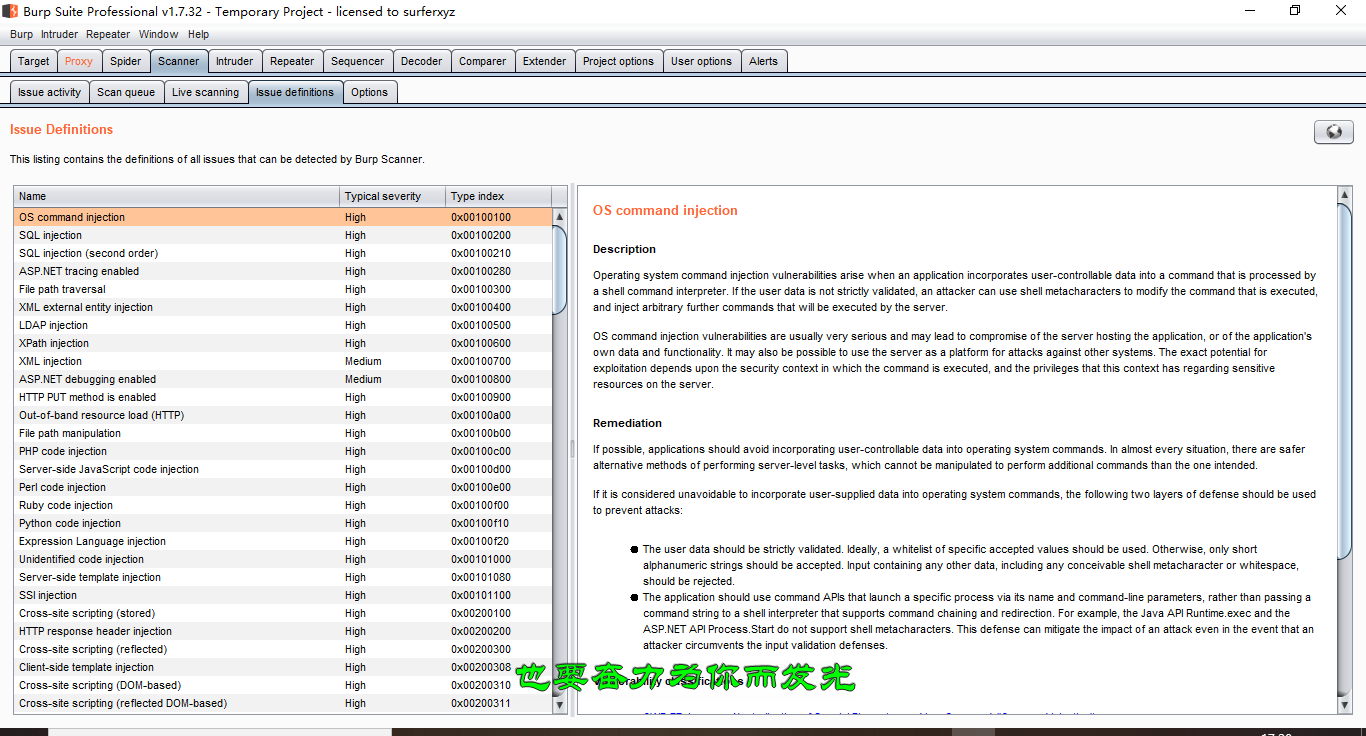
网站：http://bluecms:2020/admin/index.php

BurpSuit漏洞扫描：



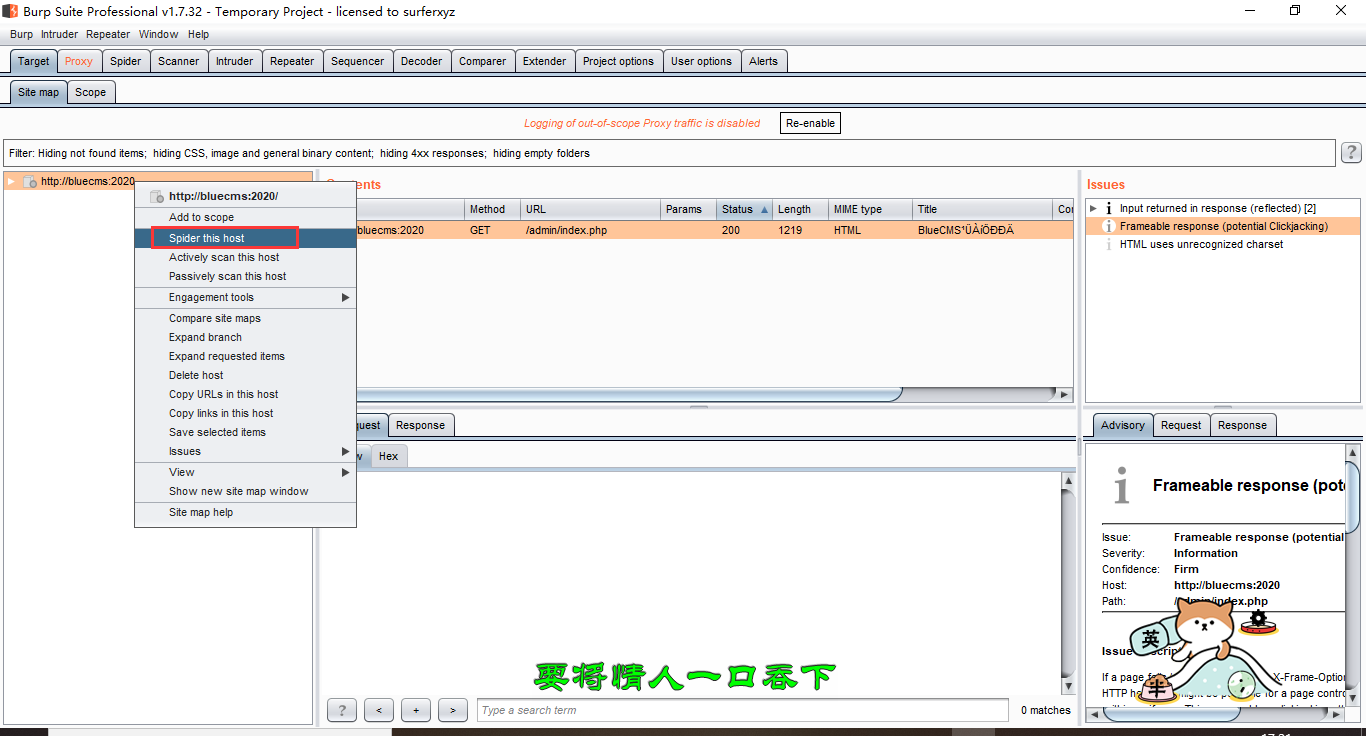


漏洞列表，详情：

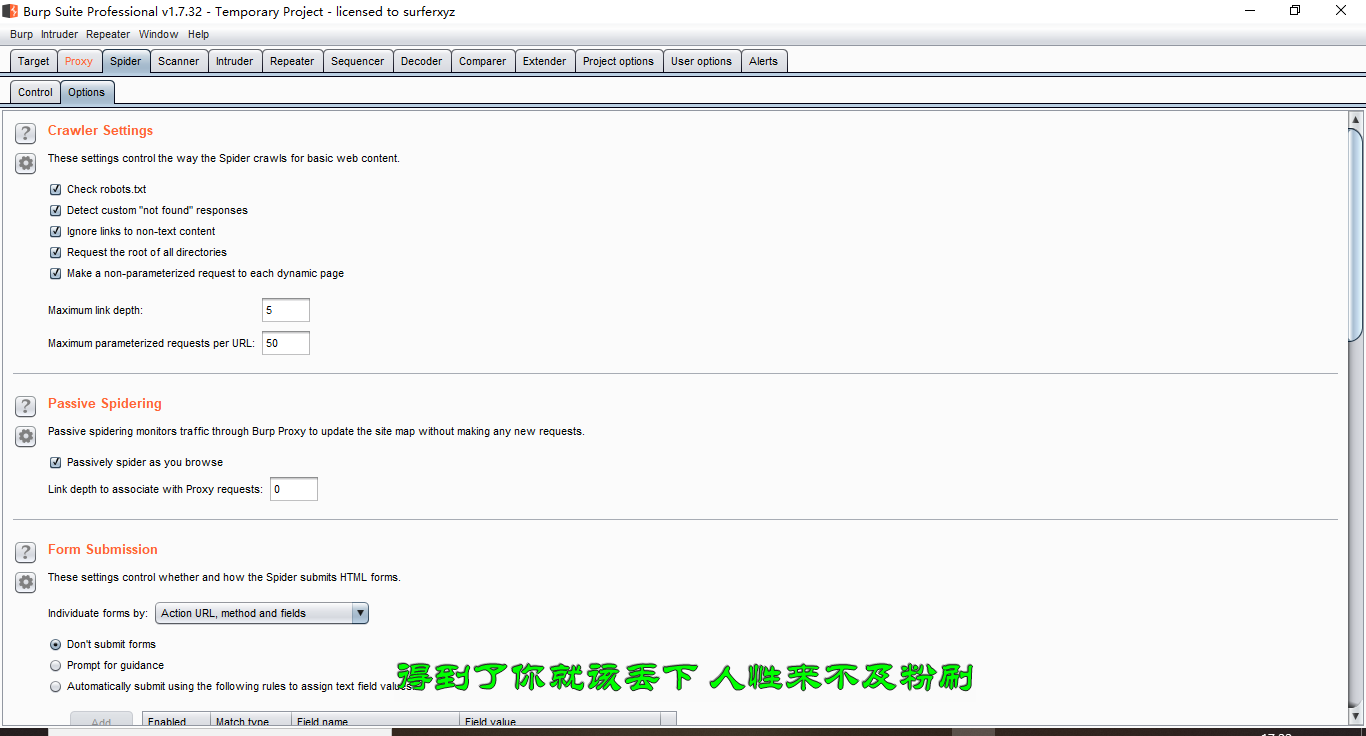


BurpSuit网站爬取：

选择网站：



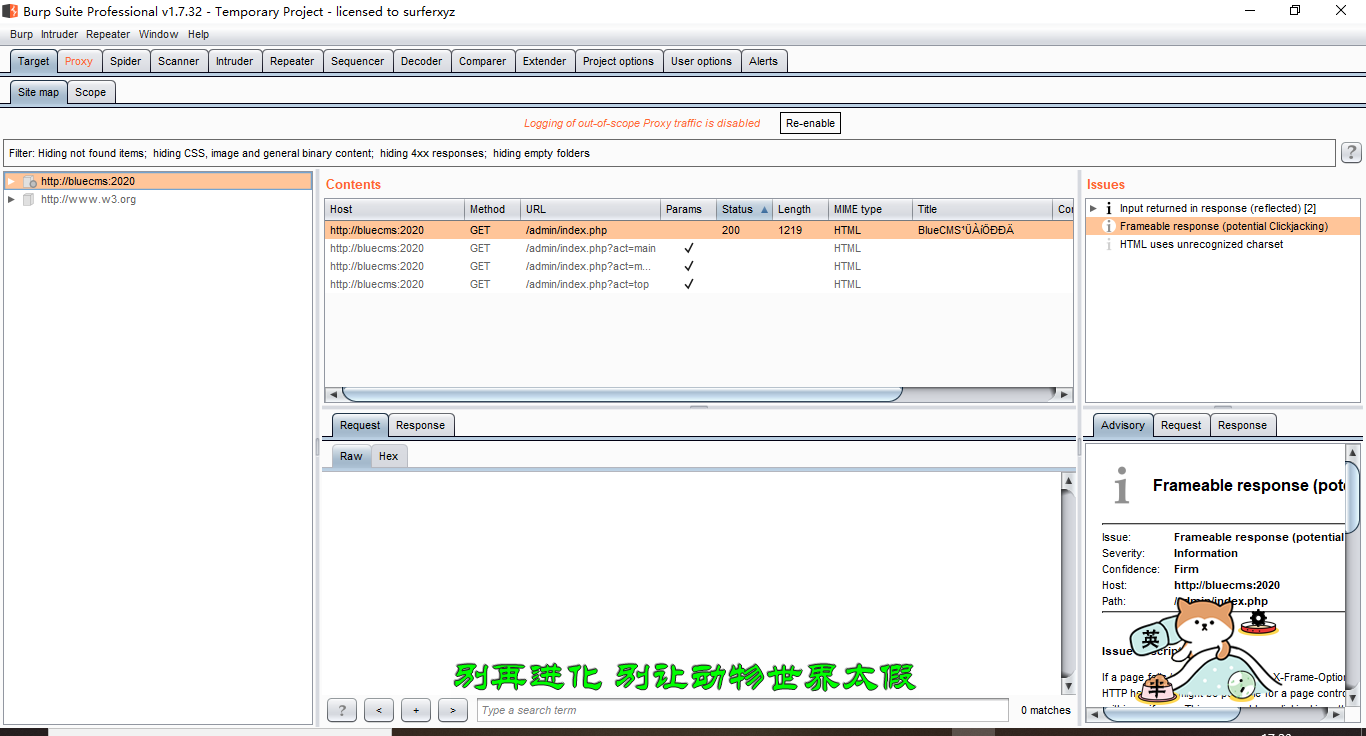
选择爬取操作：



查看爬取情况：

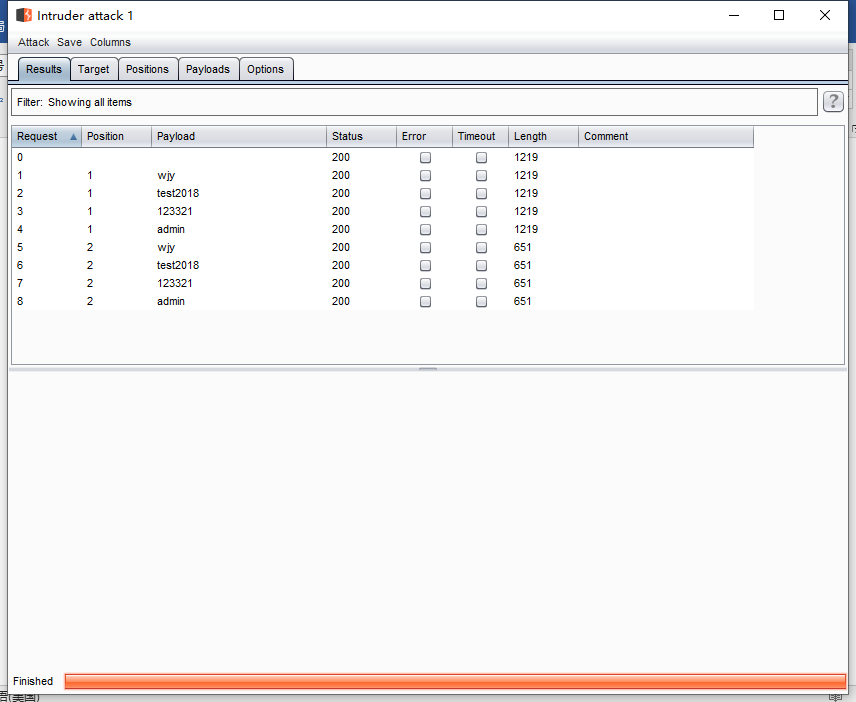


查看Target目录：

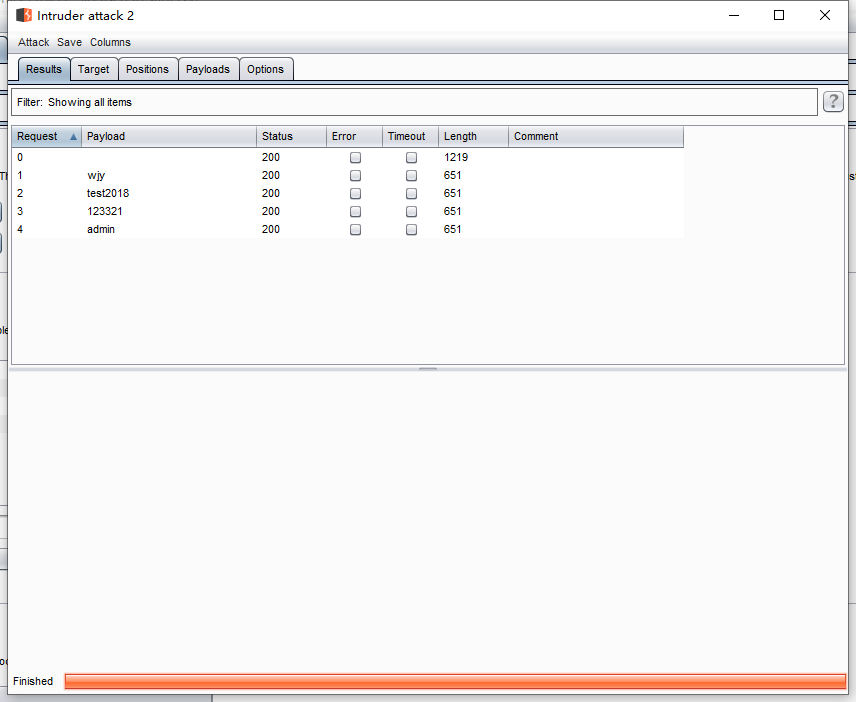


BurpSuit自动化攻击：

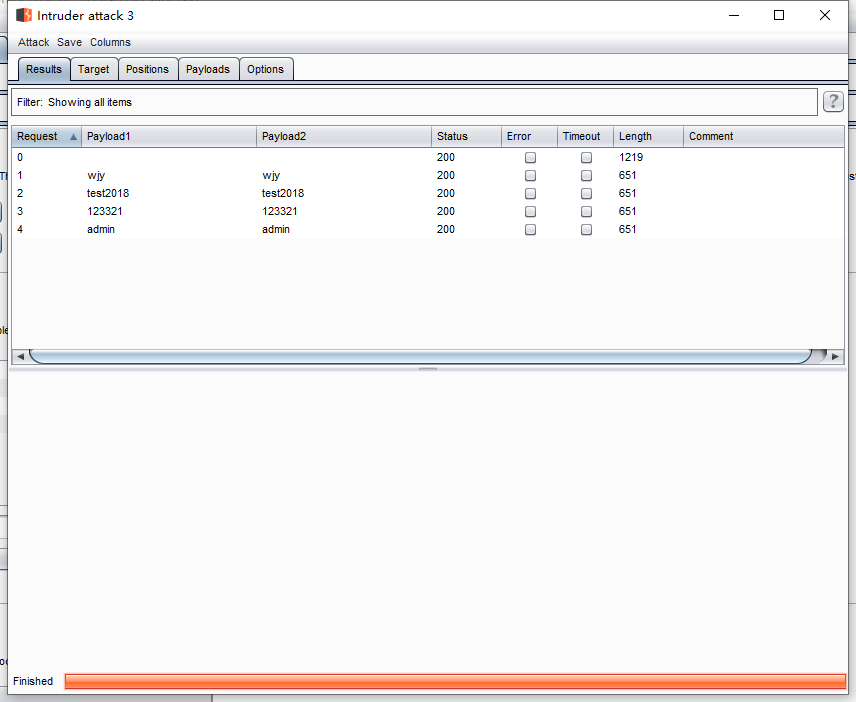
Sniper



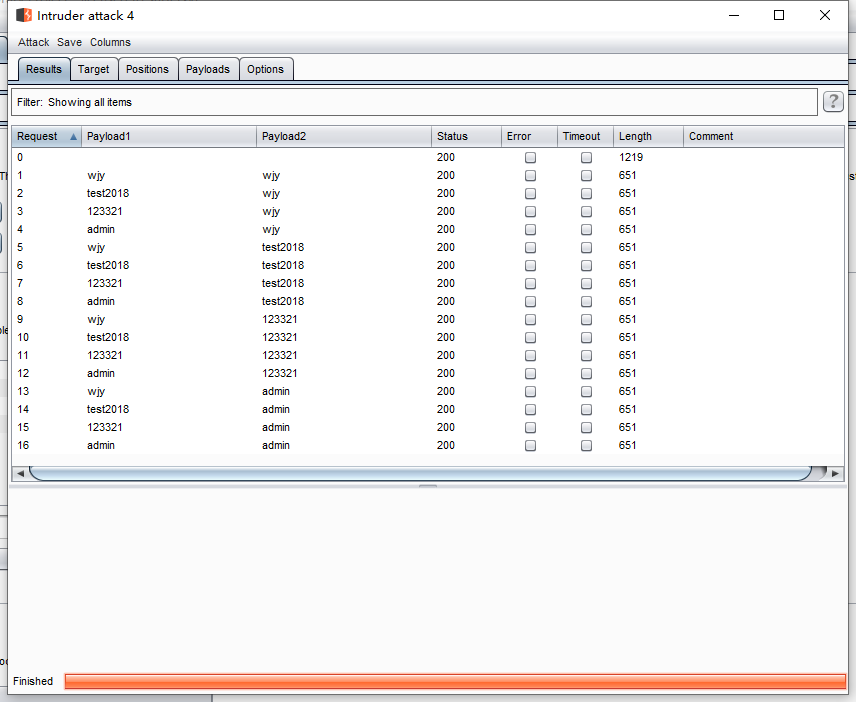
Battering ram：



Pitch fork：

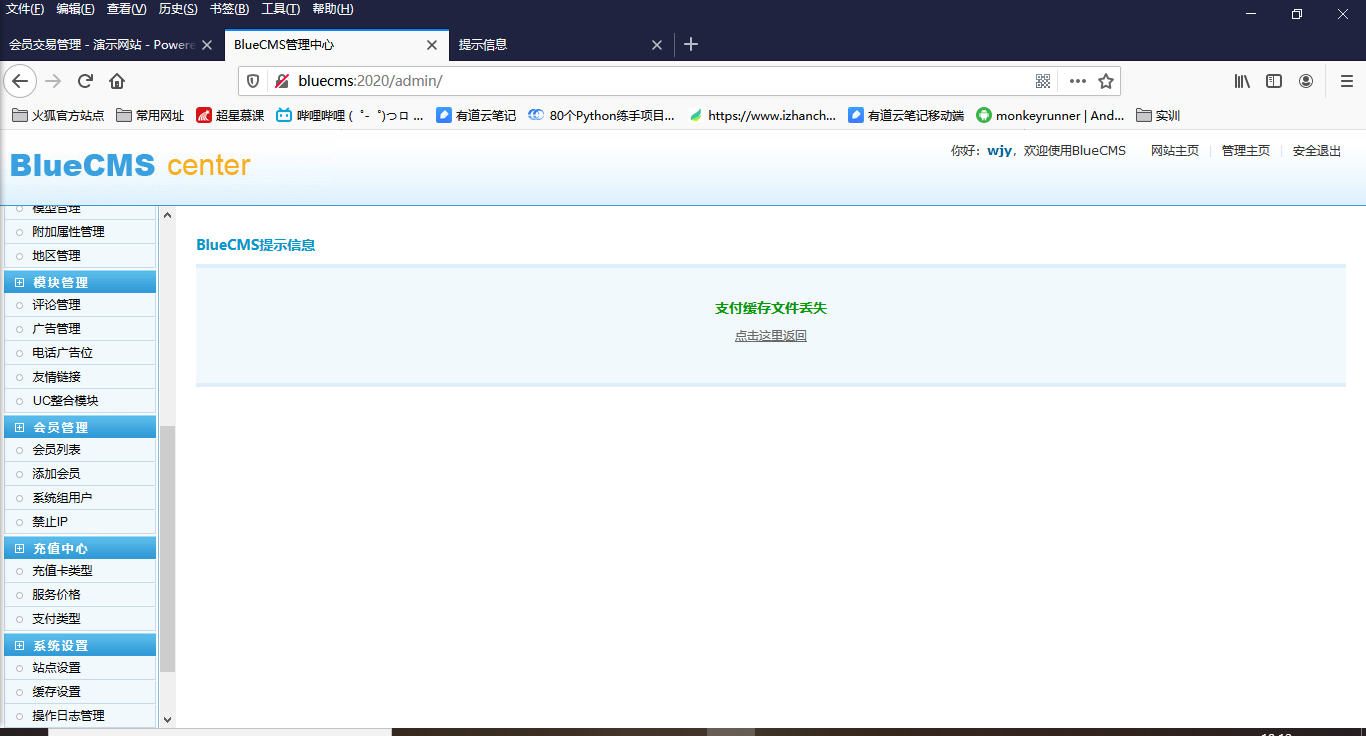


Cluster bomb：

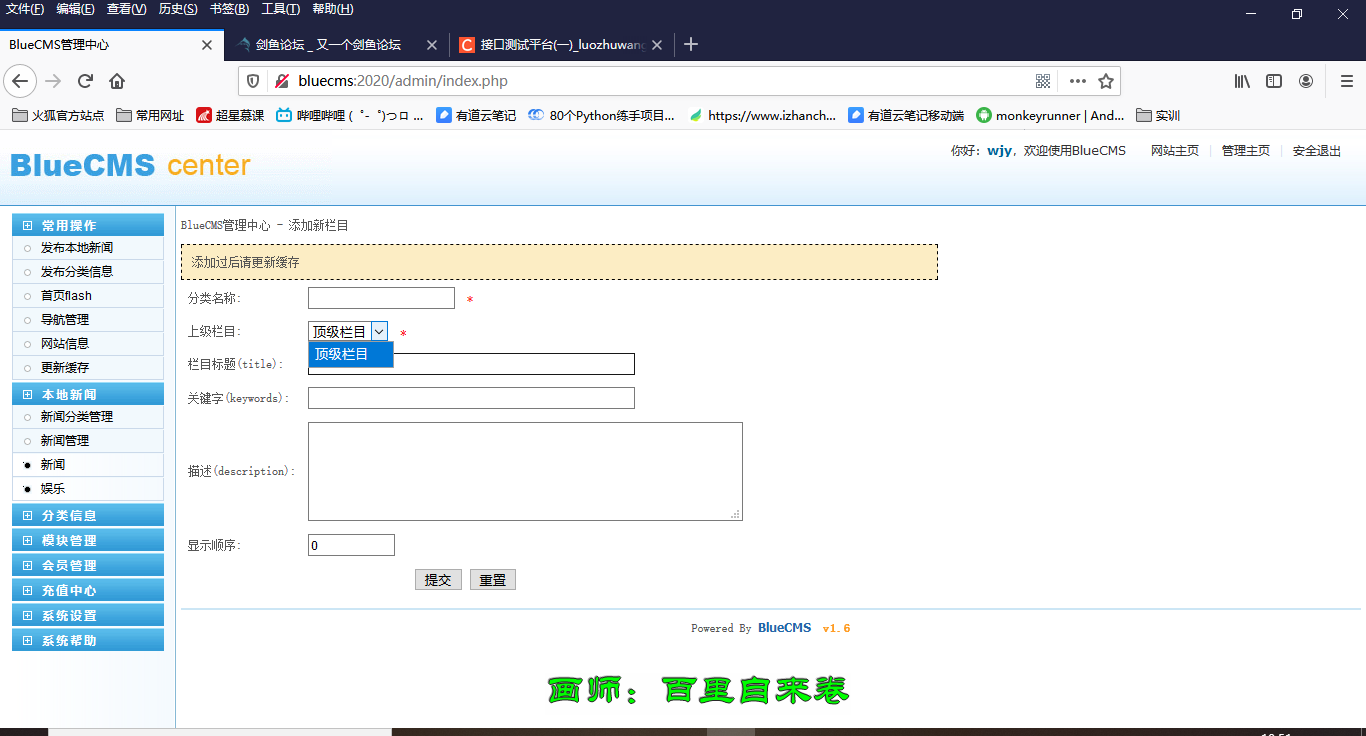


手工测试：

1、支付类型文件丢失：



2、新闻分类管理不能添加下级栏目：

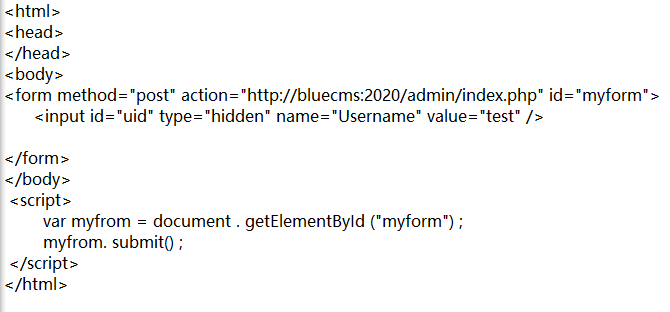


3、CSRF

可以进行跨站点请求伪造

登录时用的是post方法，所以可以构建post.html文件，里面写一个form表单，利用JavaScript自动提交表单，这样打开post.html后，就会自动提交，这时如果用户名为test的用户刚刚登录过此网站，那么打开post.html文件后就会自动登录admin用户账号

Post.html文件内容如下：



预期结果：无法打开test用户登录界面

实际结果：成功打开test用户登录界面

4、探索性测试发现，常用便民电话的详情描述无法查看