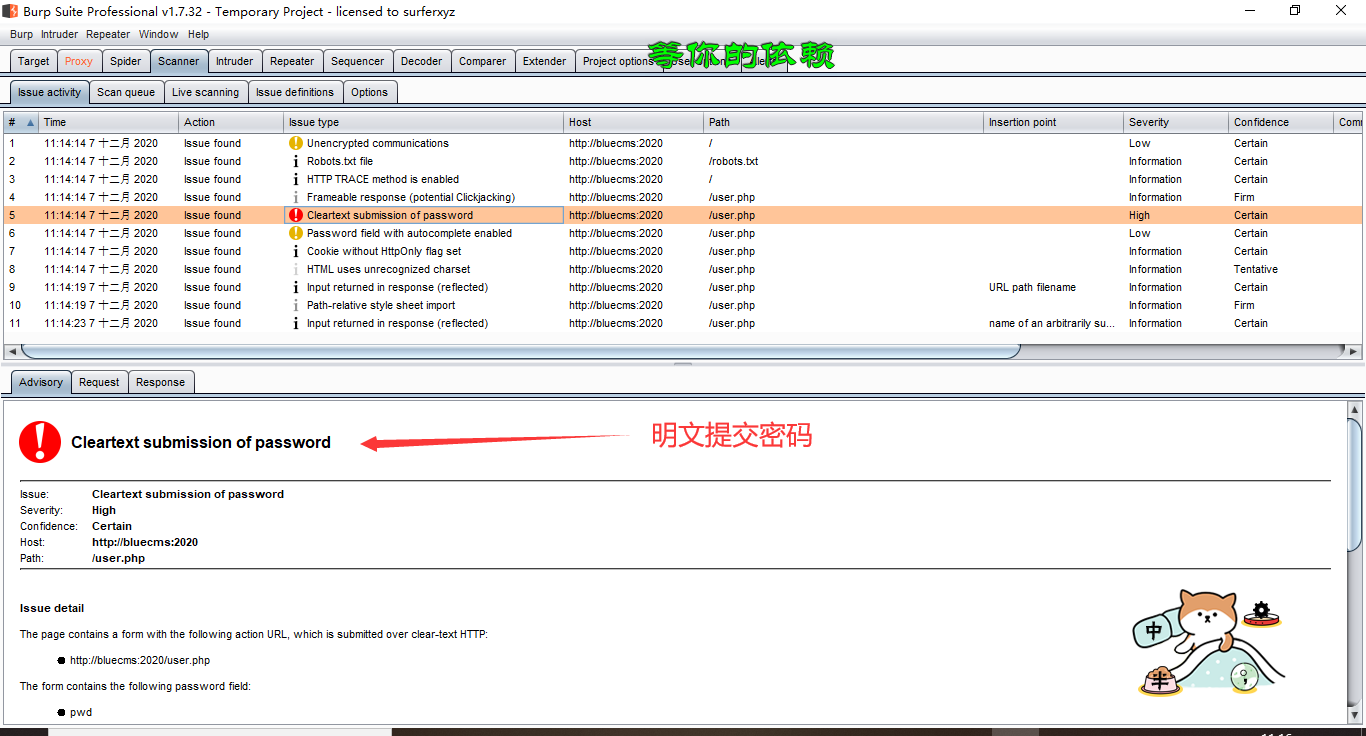
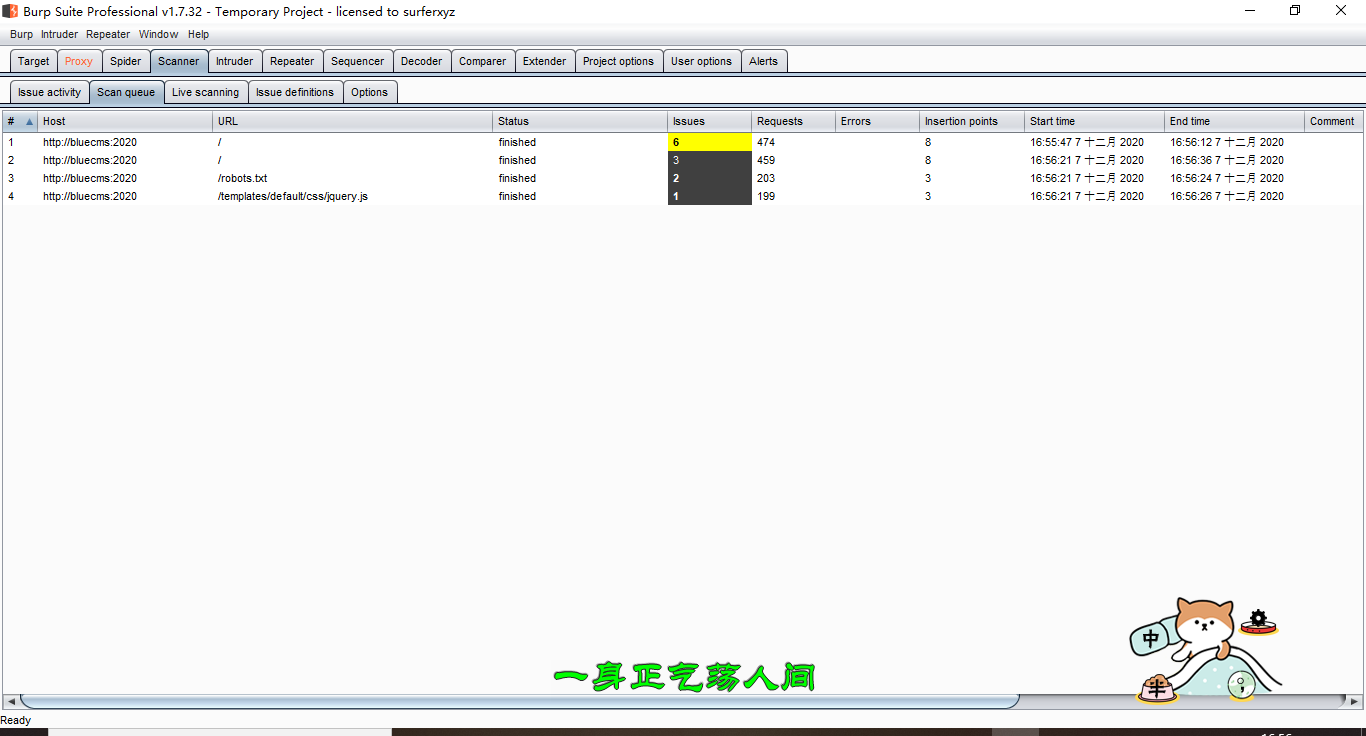
网站：http://bluecms:2020/

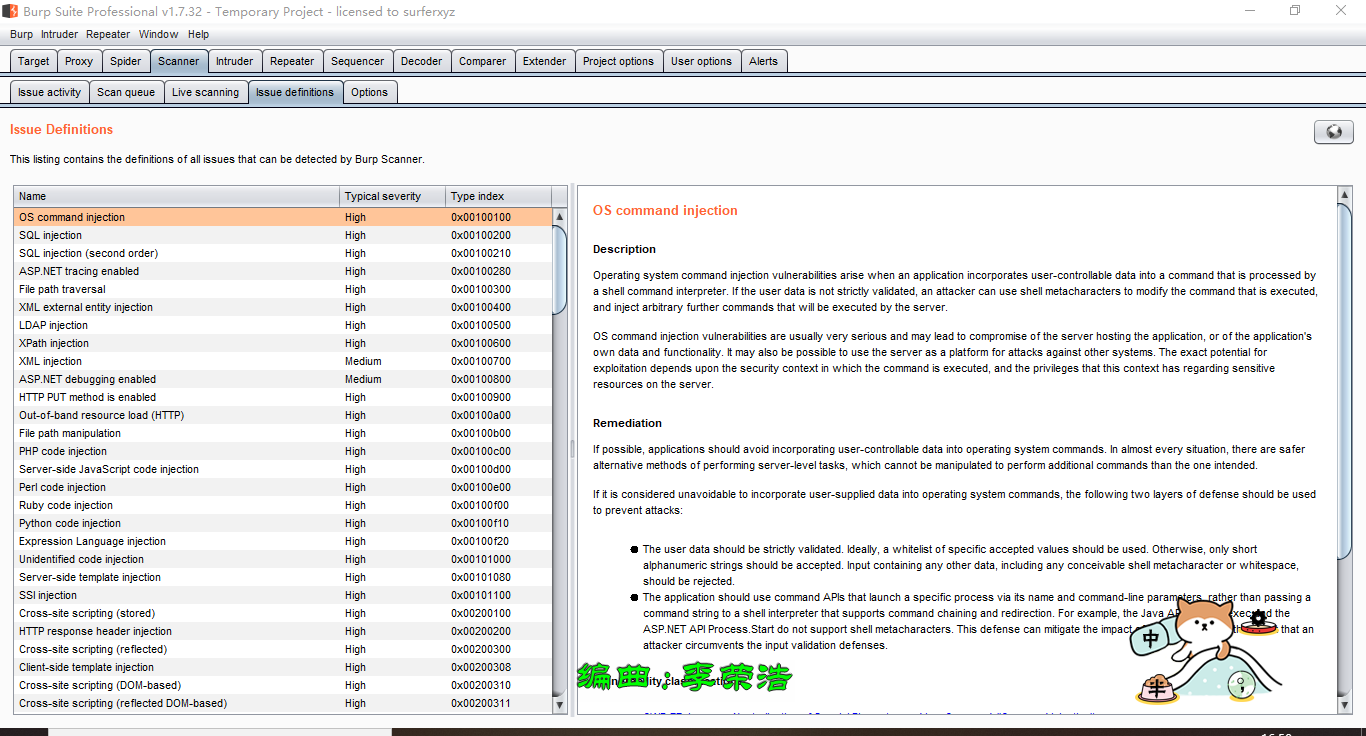
BurpSuit漏洞扫描：（备注：登录注销后再次登录，扫描会出现）



正常情况下的扫描：

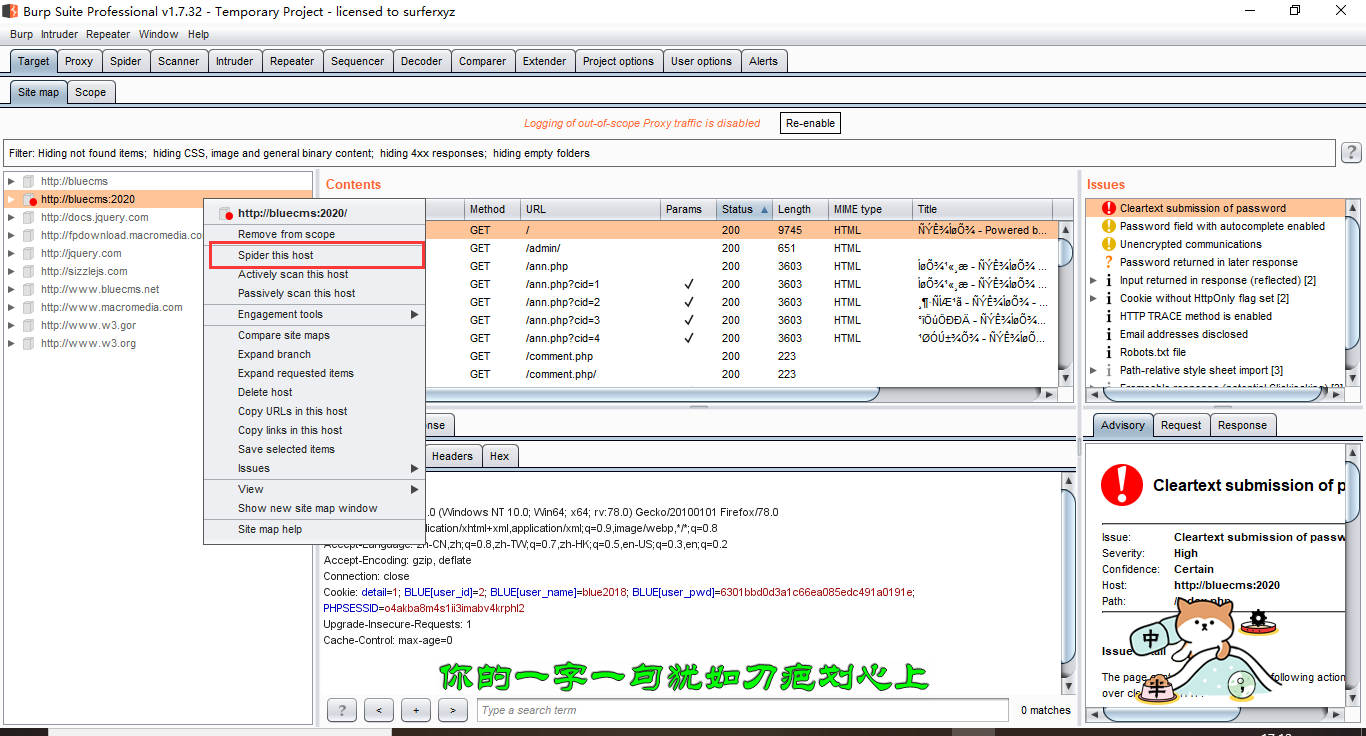


漏洞列表，详情：

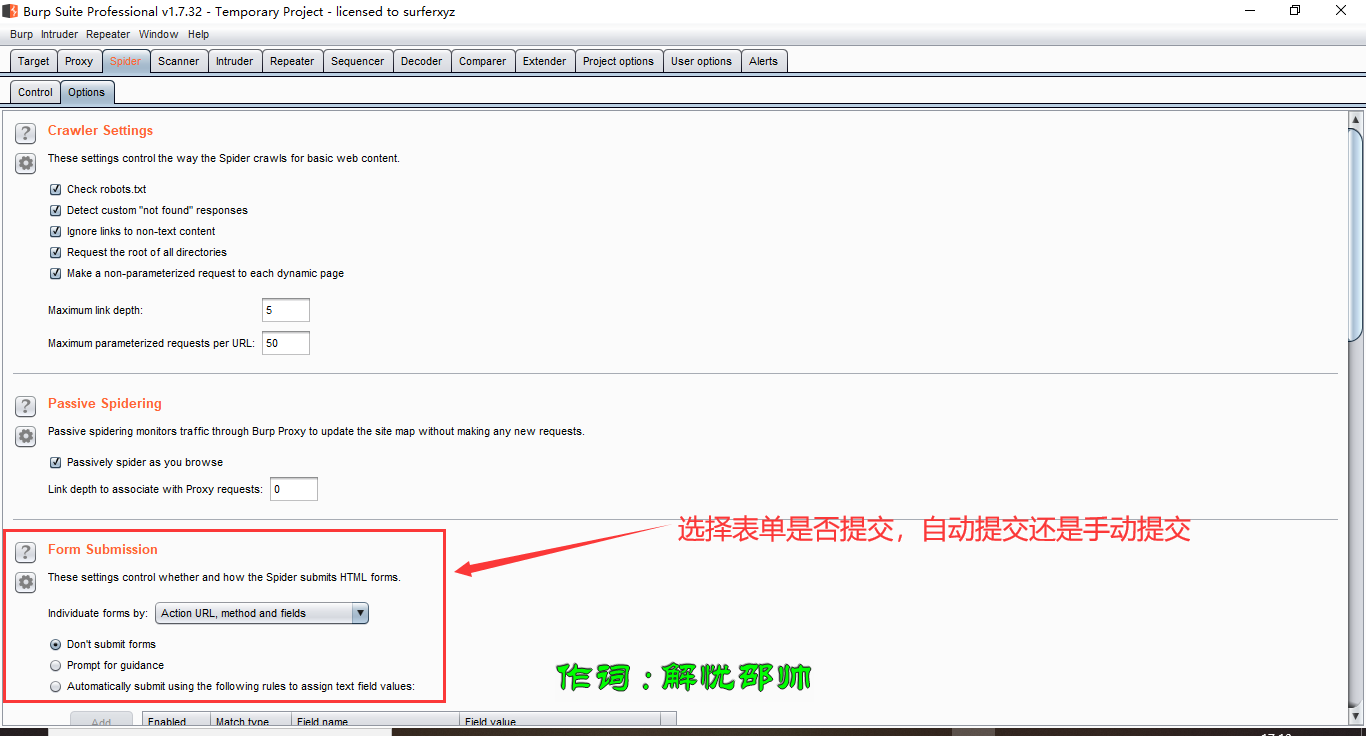


BurpSuit爬取网站：

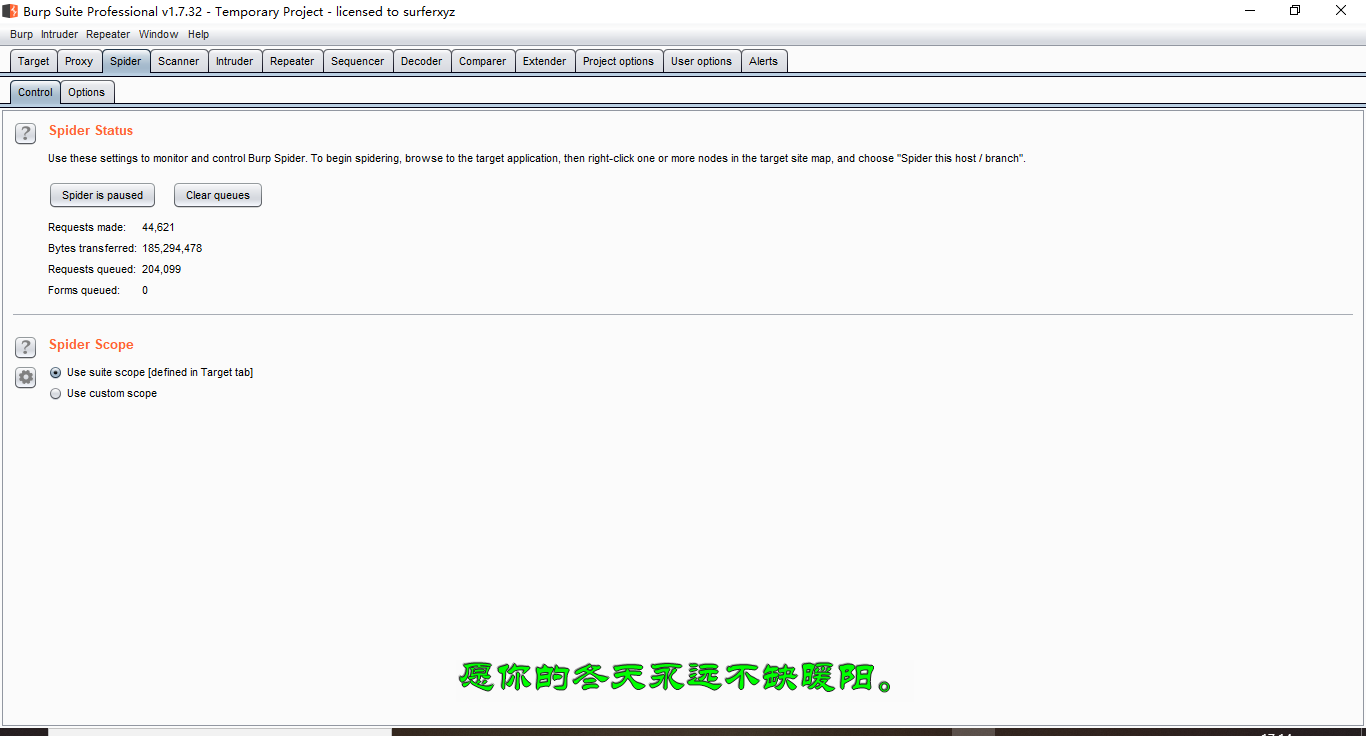
选择网站：



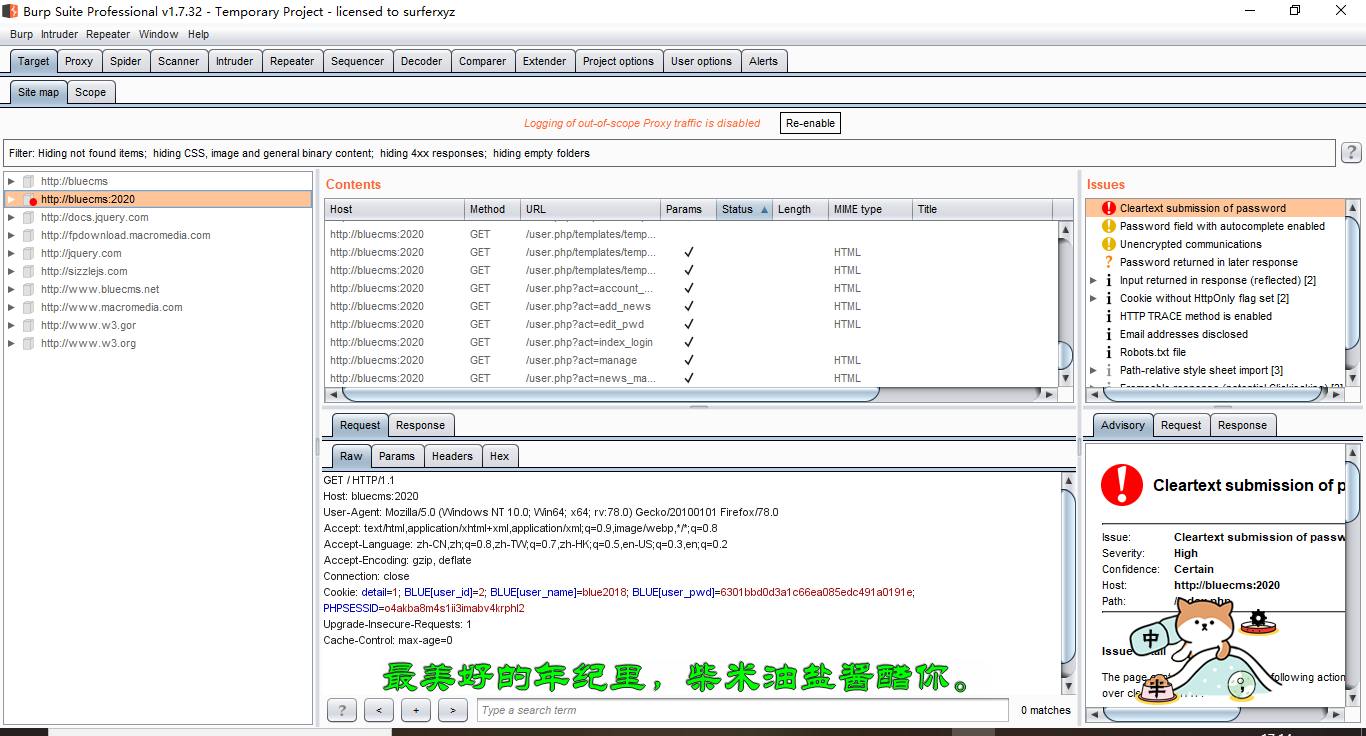
选择爬取操作：



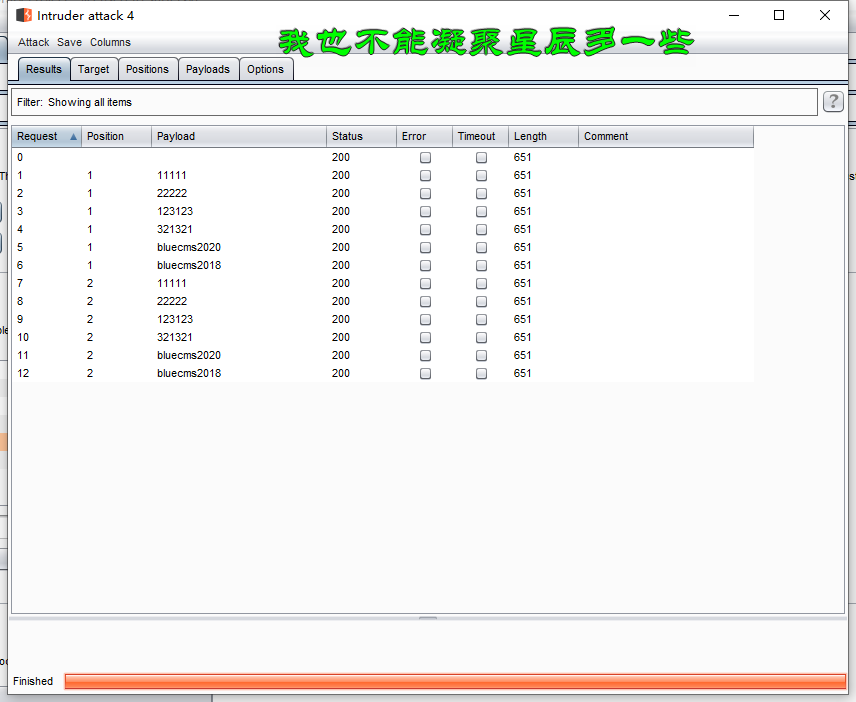
查看爬取情况：



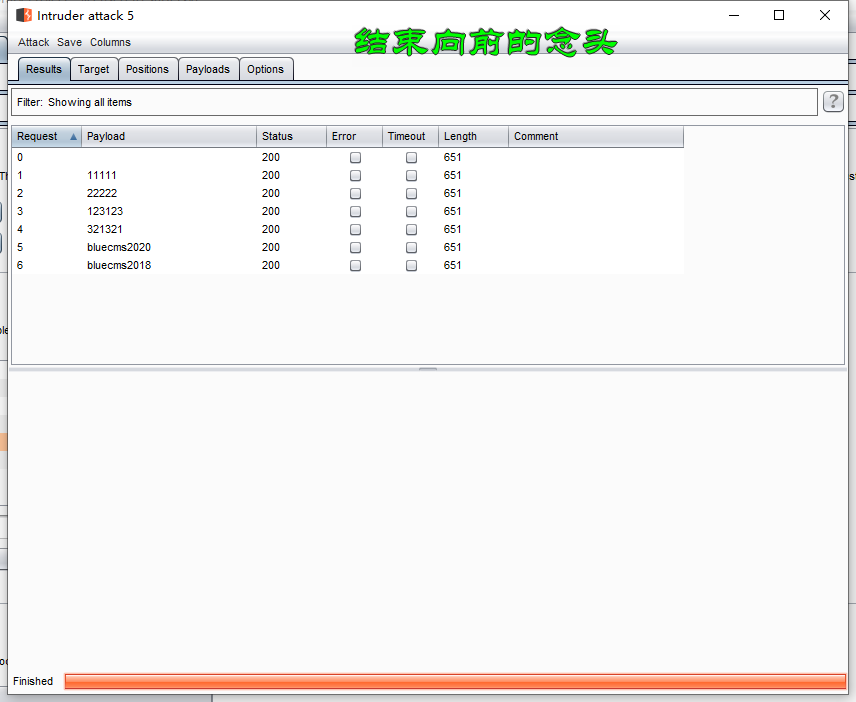
查看Target目录：

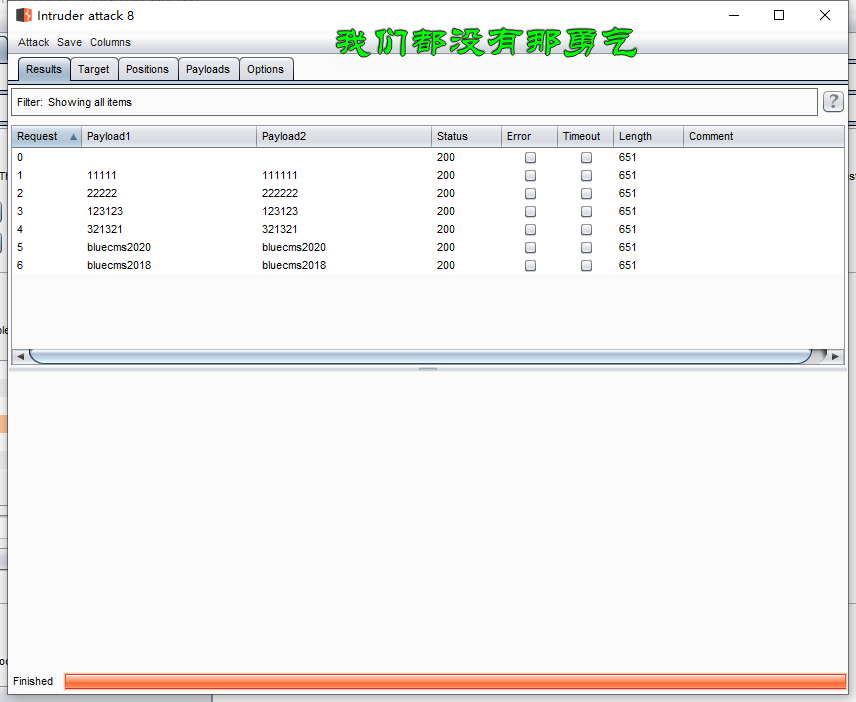


BurpSuit自动化攻击：

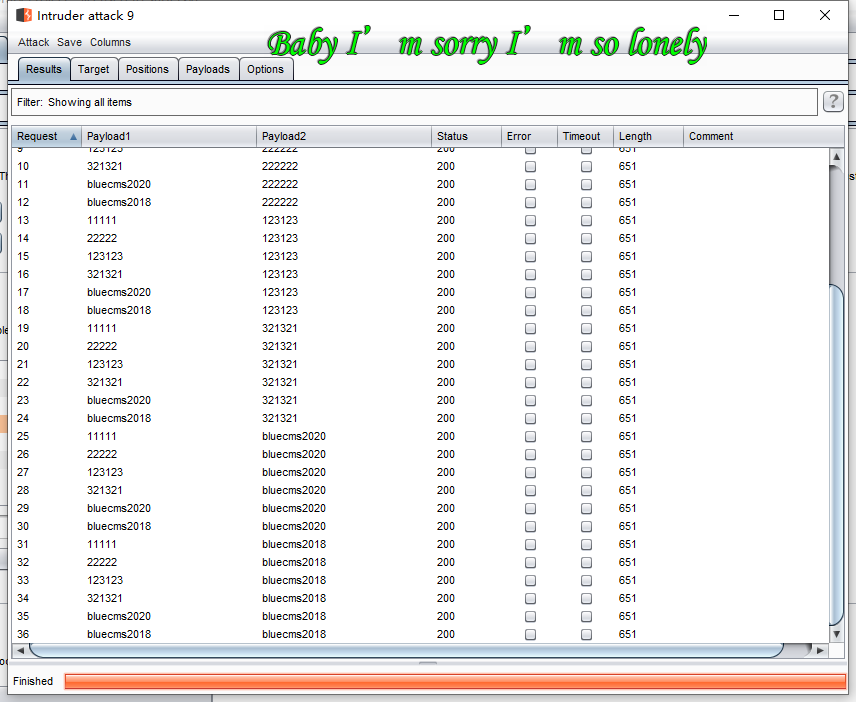
Sniper：

Battering ram：

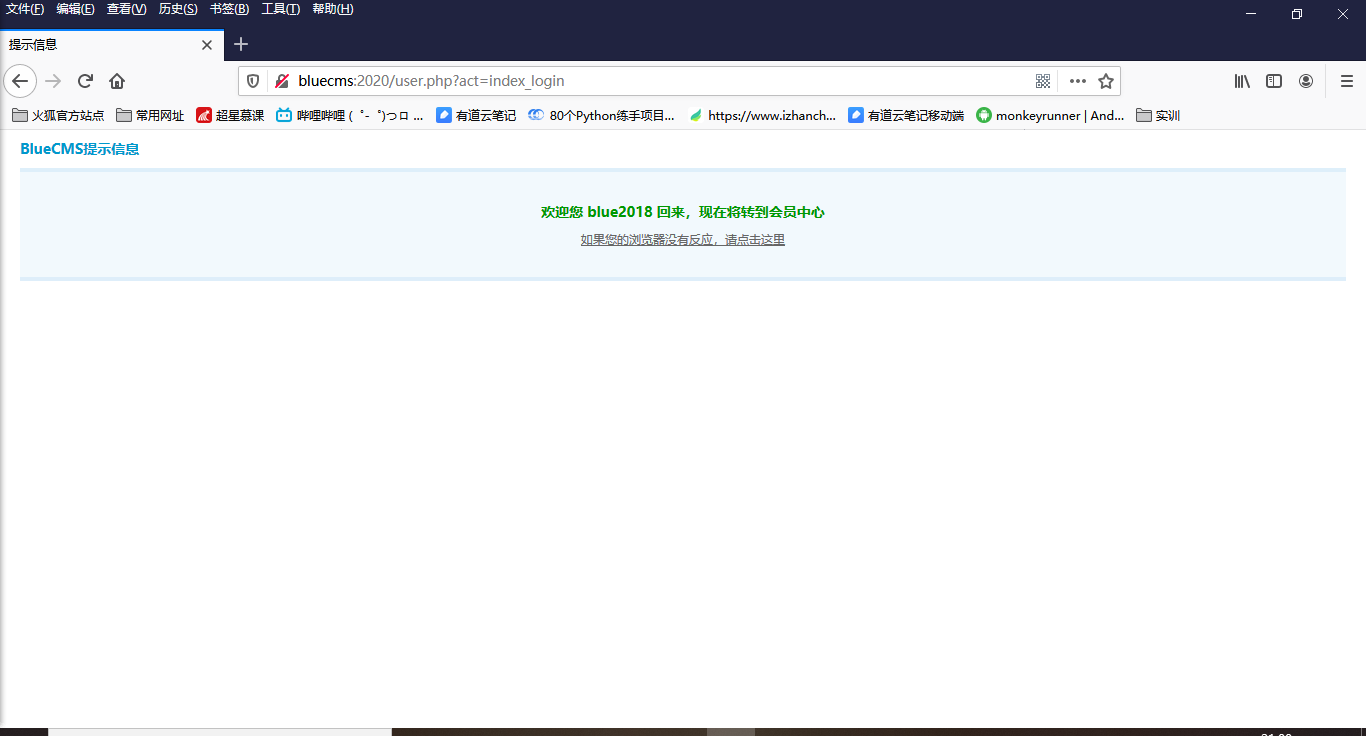


Pitch fork：

Cluster bomb：



手工测试：

1、 明文提交密码  


表单包含pwd密码字段

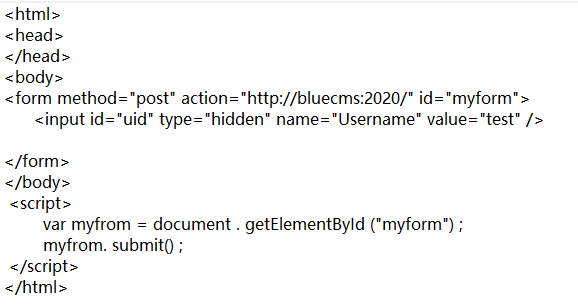
2、CSRF

操作步骤：

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

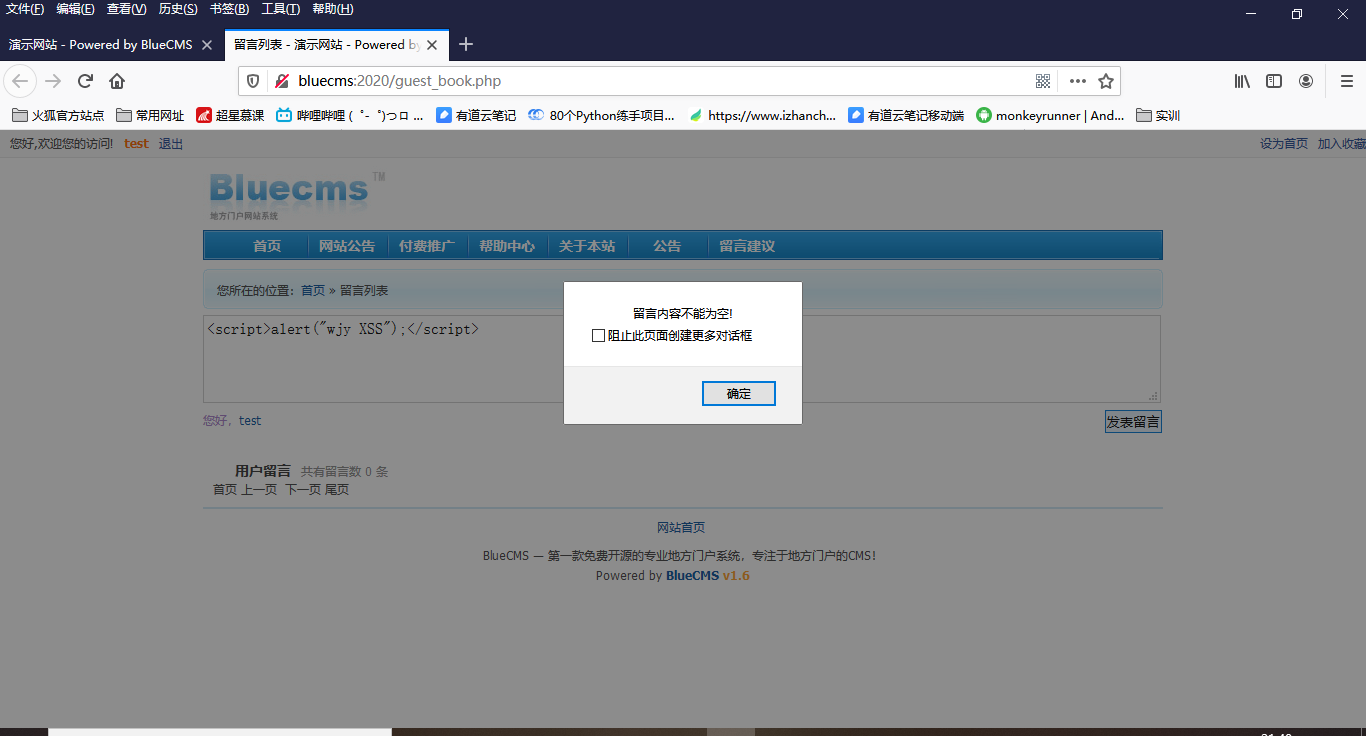
Post.html文件内容如下：



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

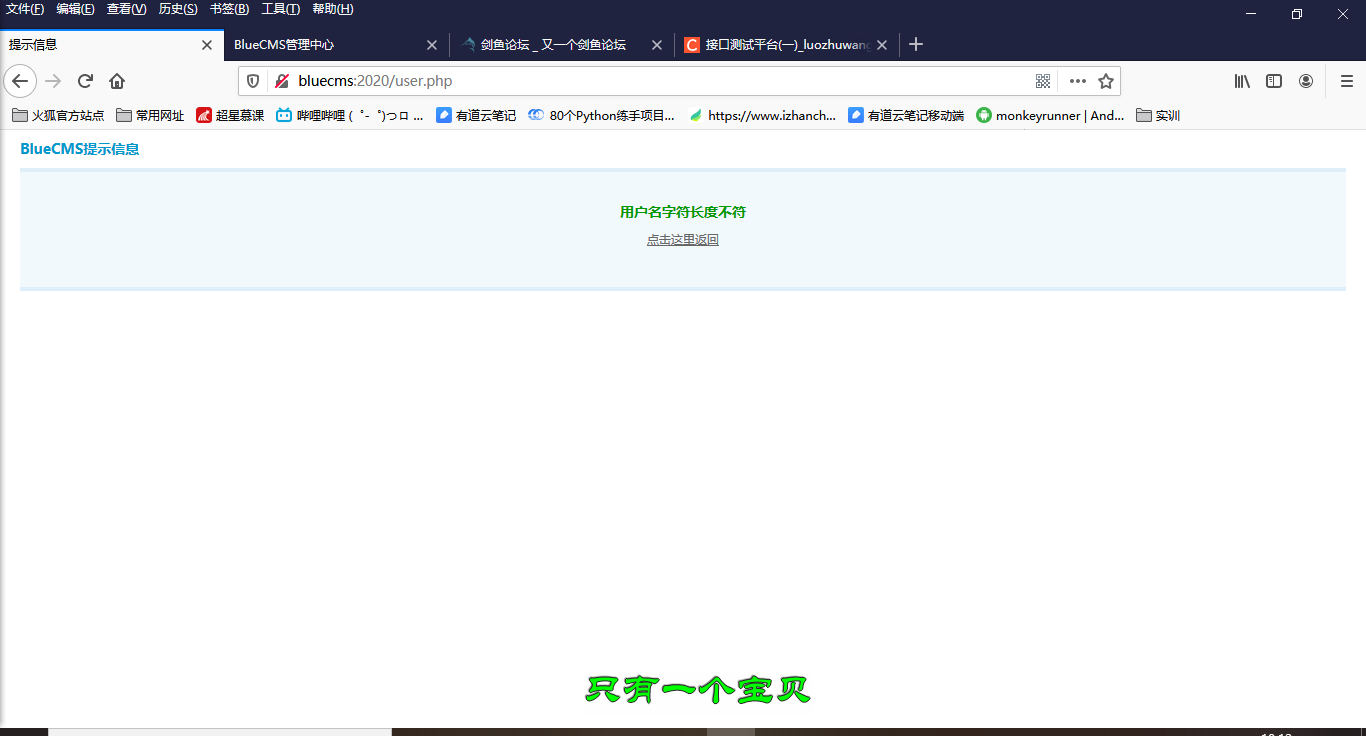
3、无法留言



4、注册时，用户名使用空格，显示用户名可以使用：



但是提交注册后提示用户名字符长度不符：



5、发布新闻中新闻内容的粘贴功能无法点击

6、首页登录不需要验证码，而登录界面需要验证码，不合理