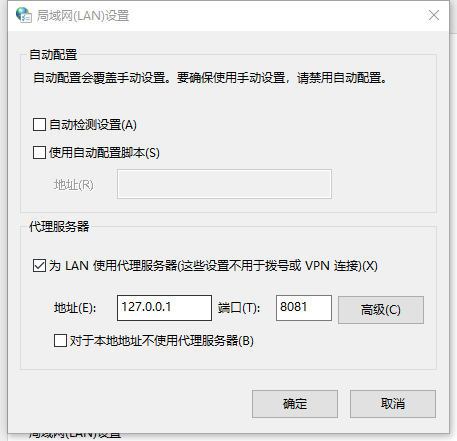
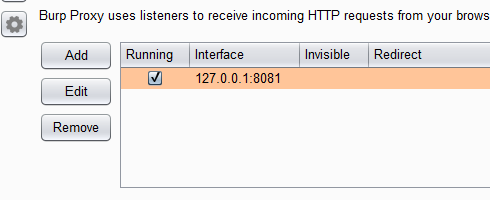
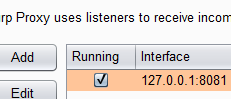
1. **设置本地代理为127.0.0.1:8081**



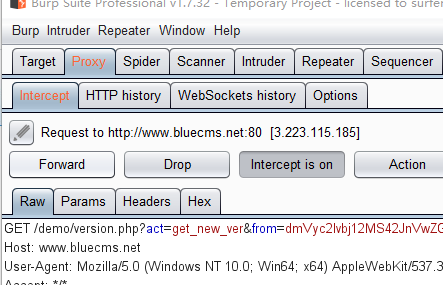
1. **burpsuite点击Options设置端口号为8081**



1. **选中刚刚设置的地址**

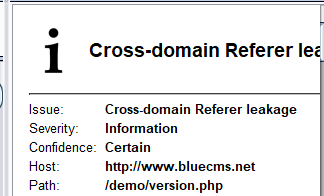


1. **intercept选择intercept is on**



1. **登录bluecms网站**

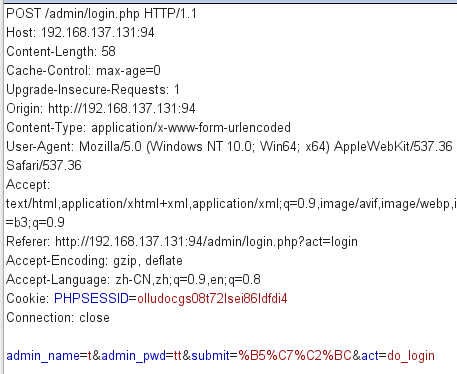
**Spider选项卡选择options自选项卡，向下滚动到application login部分，选择handle as ordinary forms；转到proxy选项卡，关闭proxy interception拦截，转到浏览器访问<http://demo.testfire.net/>;转到target选项卡，选择的sitemap自选项卡，选择url右键选择expand branch；选择使用的url选择相关的位置右键spider this host，点击yes，当spider中的control中的requests queued和form queued都显示为0时返回到target选项卡和sitemap，选择相应的位置（index.php）右键activity scan this host；**



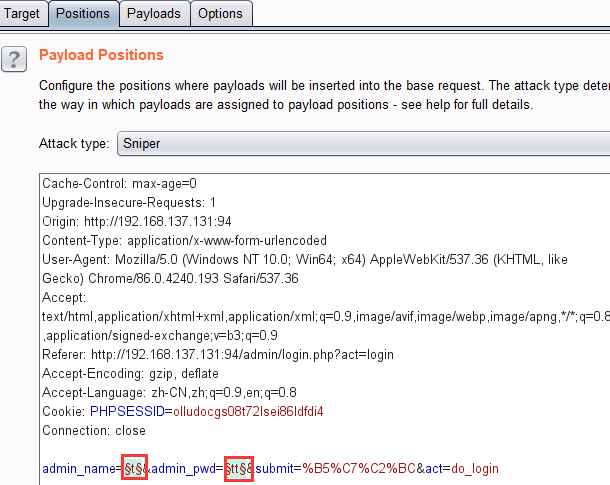
**6.攻击**

**①Sniper攻击**

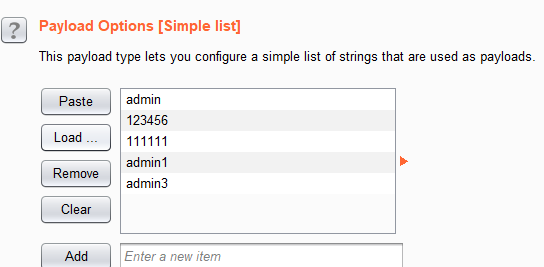
**用户名和密码输入t，tt用burpsuite打开intercept on ，进行抓包后发送到intruder模块**



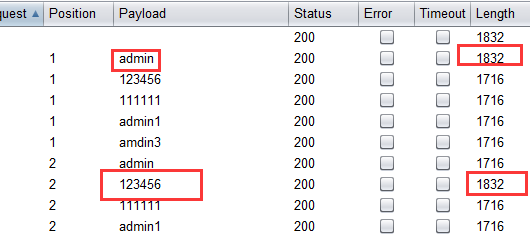
**发送到intruder模块后，选择positions attack type选择Sniper，点击clear清除变量，仅添加username和password变量**



**然后选择poyloads set 为1，type为simple list，点击select file选择准备好的用户名字典**



**返回positions模块，点击右上角的start attack**

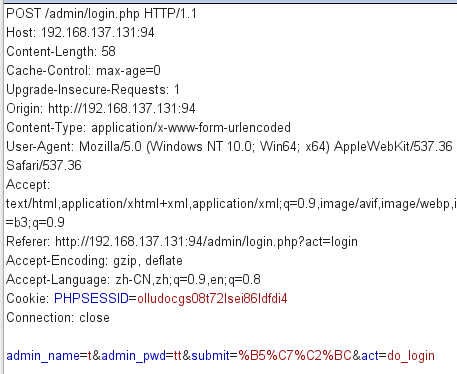


**用admin账号登录看是否成功**

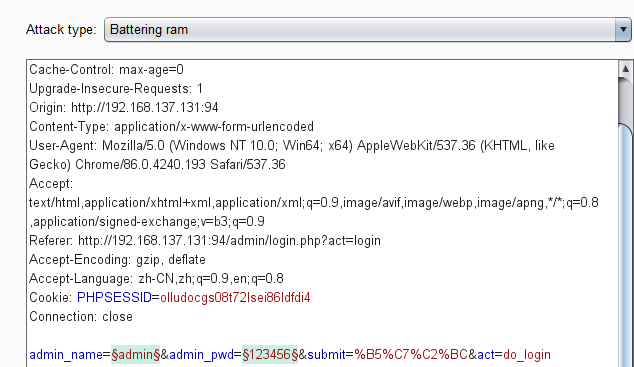


**②battering ram攻击**

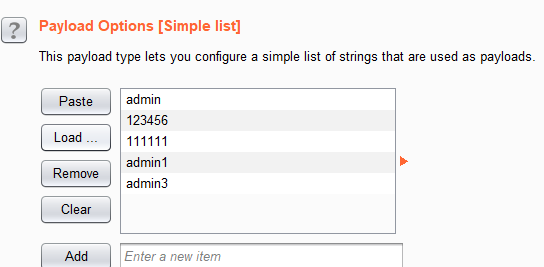
**用户名和密码随便输入t,tt,用burpsuite 打开intercept on，进行抓包后发送到intruder模块**



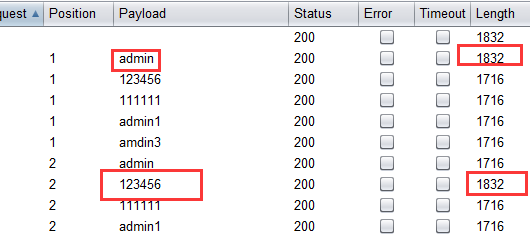
**发送到intruder模块后，选择positions attack type选择Battering ram；点击clear清除变量，仅添加username和password的变量。**



**然后选择poyloads   set为1，type为simple list，点击select file选择准备好的用户名字典**



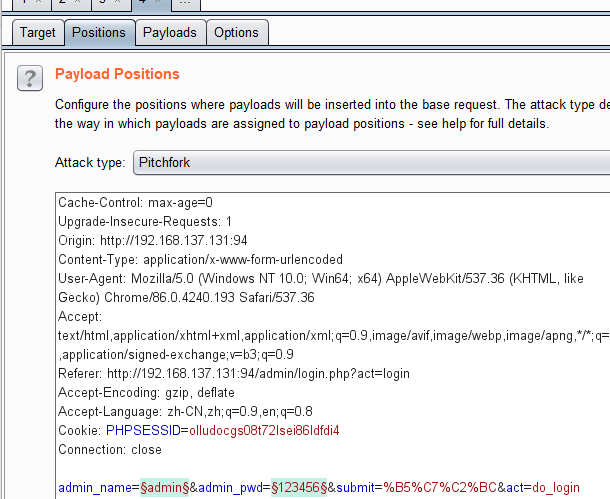
**返回positions模块，点击右上角start attack。**



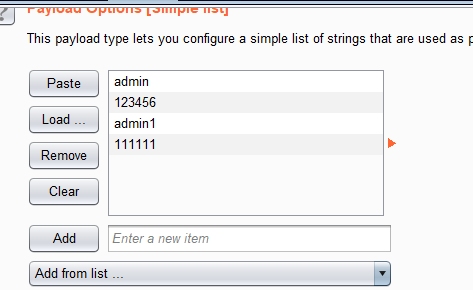
**用admin登录看是否成功**



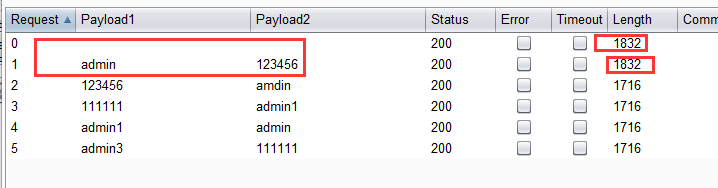
**③用pitchfork攻击**



**然后选择poyloads   set为2，type为simple list，点击select file选择准备好的用户名字典**



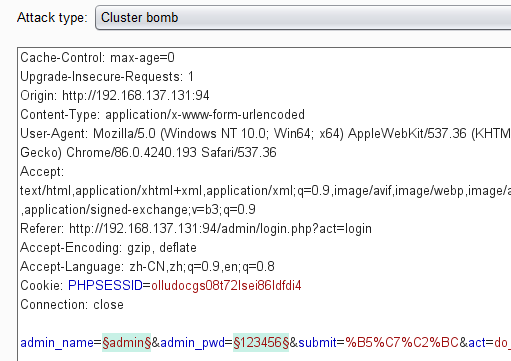
**返回positions模块，点击右上角start attack。**

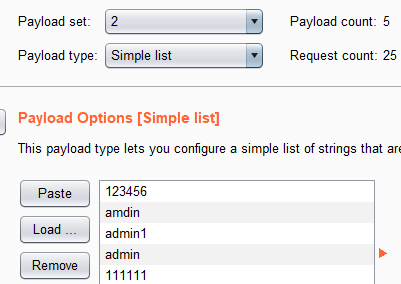


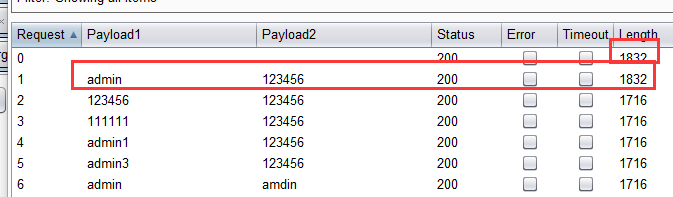
**用admin登录看是否登录成功**



**④Cluster bomb攻击**





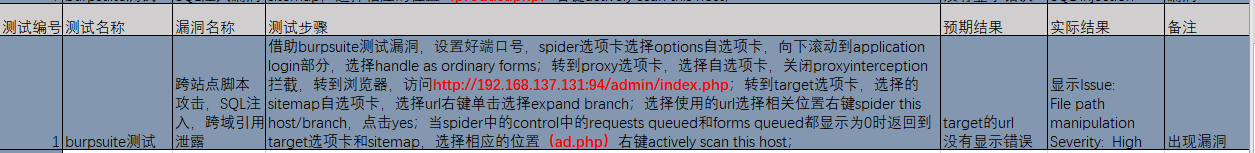


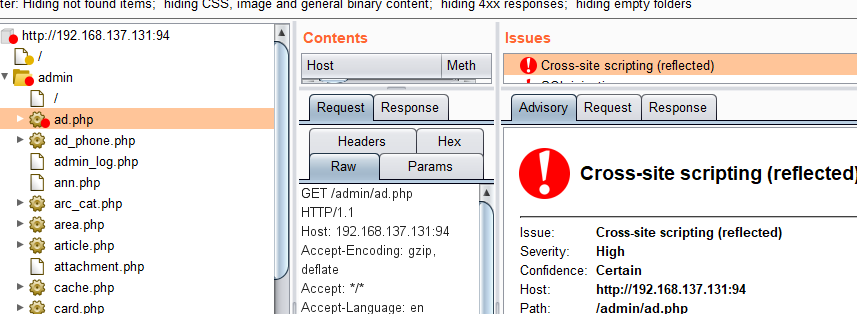
**用admin登录，看是否登录成功**

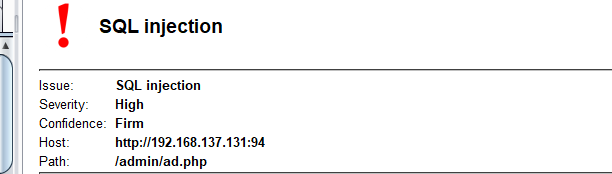


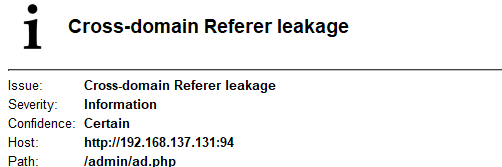
**7.渗透测试**

**①跨站点脚本攻击，SQL注入，跨域引用泄露**

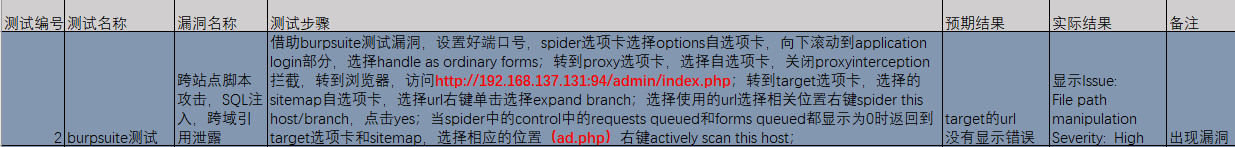


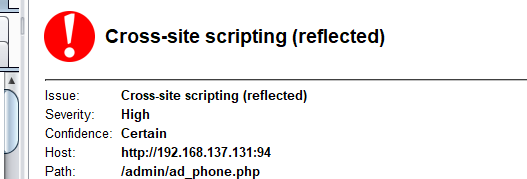


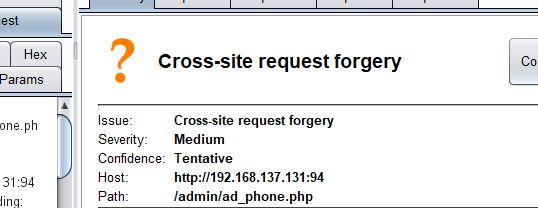


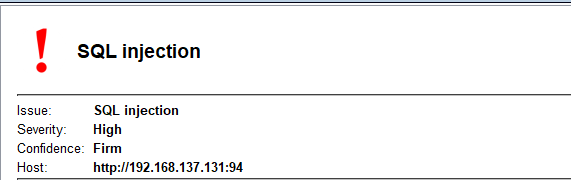


**②跨站点脚本攻击，SQL注入，跨域引用泄露**

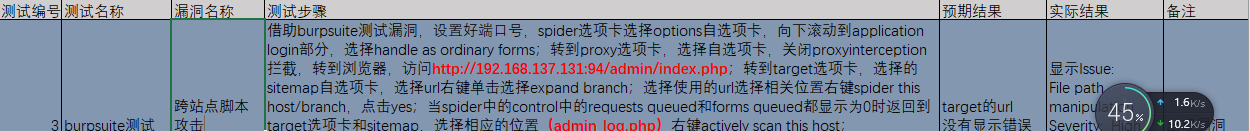


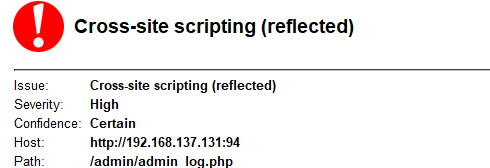




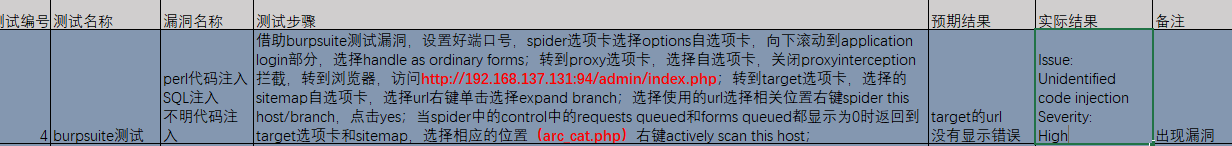


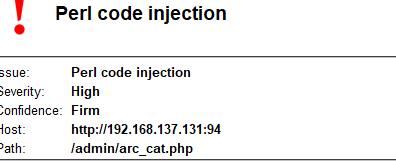
**③跨站点脚本攻击**

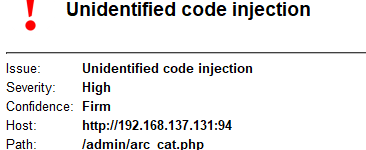


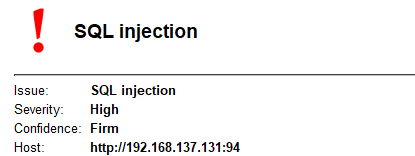


**④perl代码注入，SQL注入，不明代码注入**

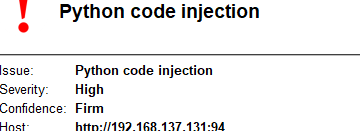


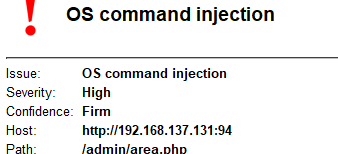


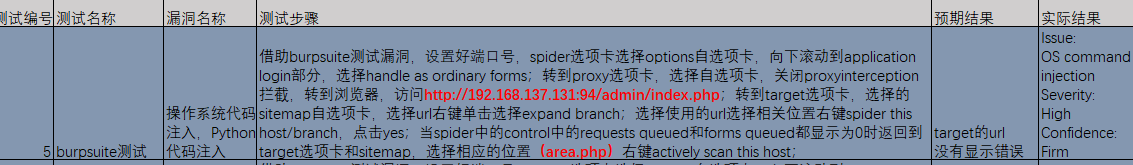




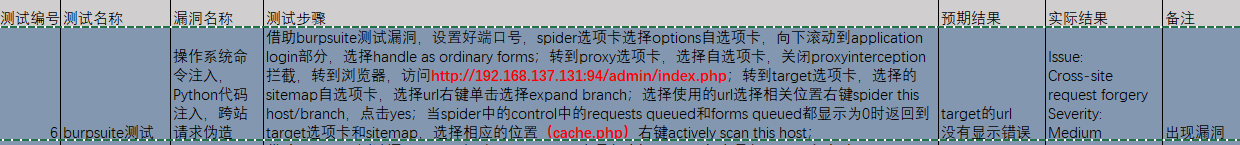
**⑤操作系统代码注入，Python代码注入**





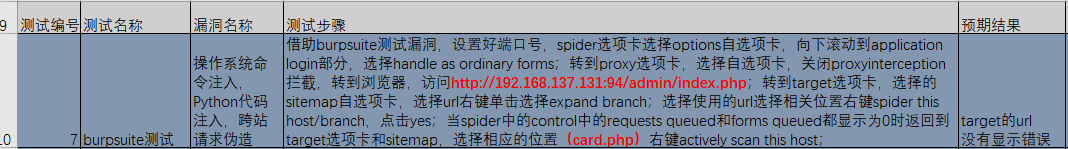


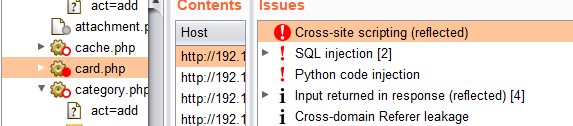
**⑥跨站请求伪造，操作系统命令注入**



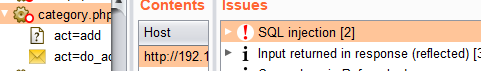


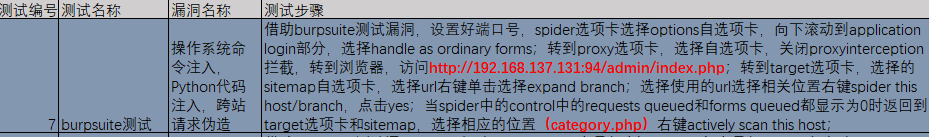
**⑦跨站点脚本反射，SQL注入，python代码注入**



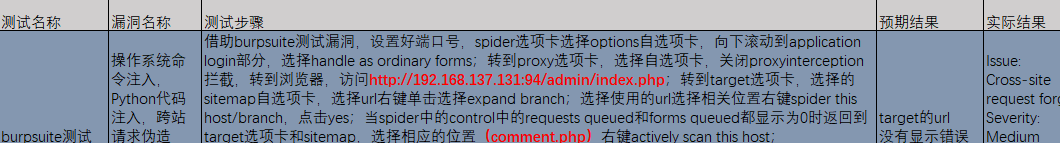


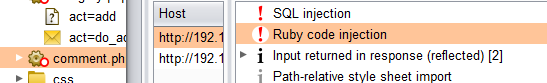
**⑧ SQL注入**





**⑨Ruby代码注入，SQL注入**





**⑩明文提交密码**

