Bluecms\_1.6渗透测试报告

1.信息收集

（1）域名信息



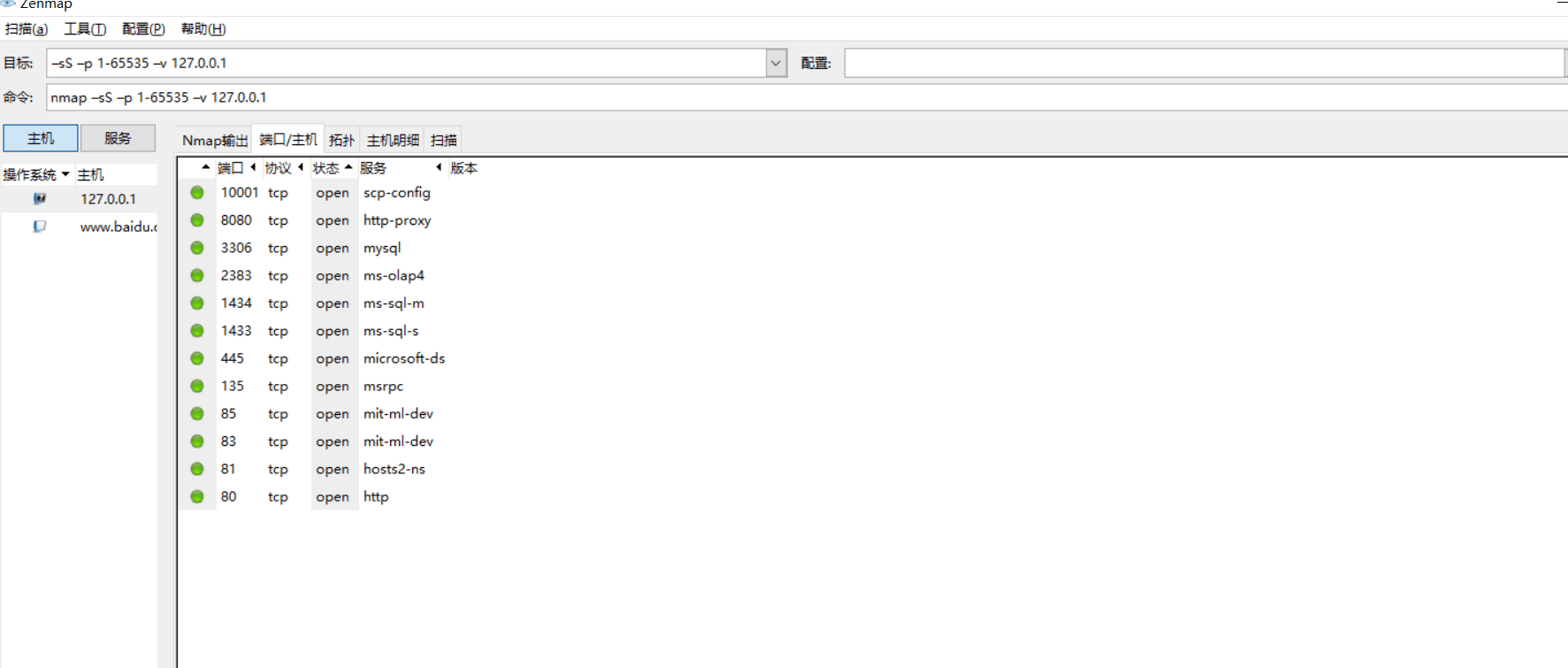
（2）查询注册人信息

在<http://whois.chinaz.com/>里输入bluecms.com，然后点击查询。

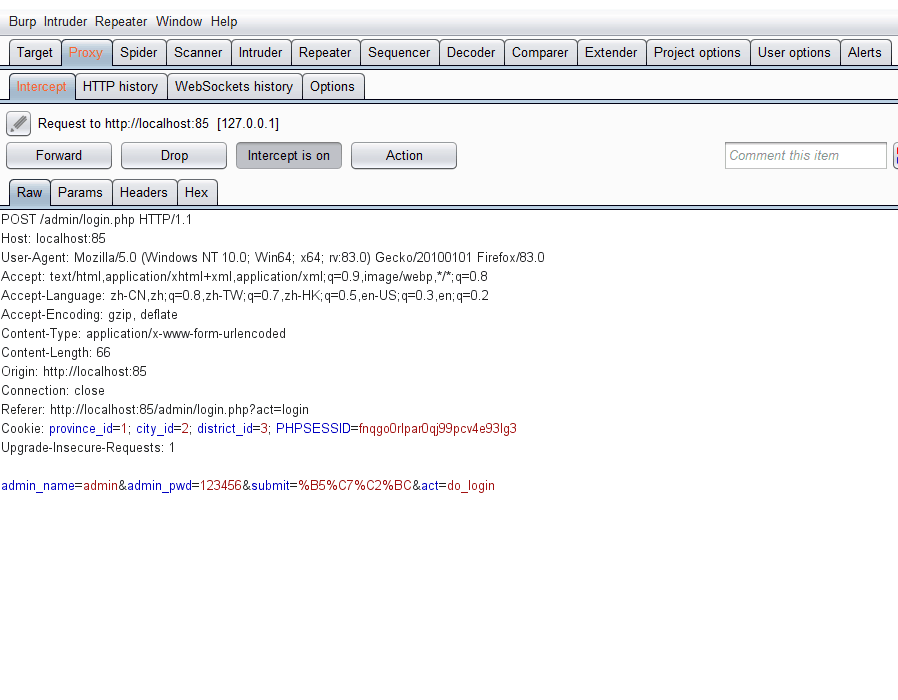


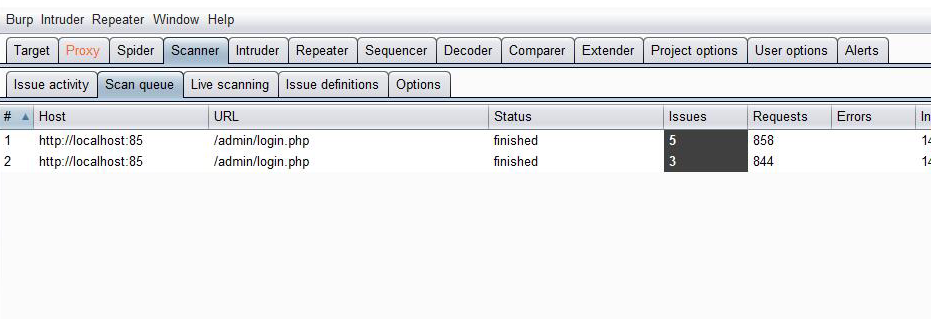


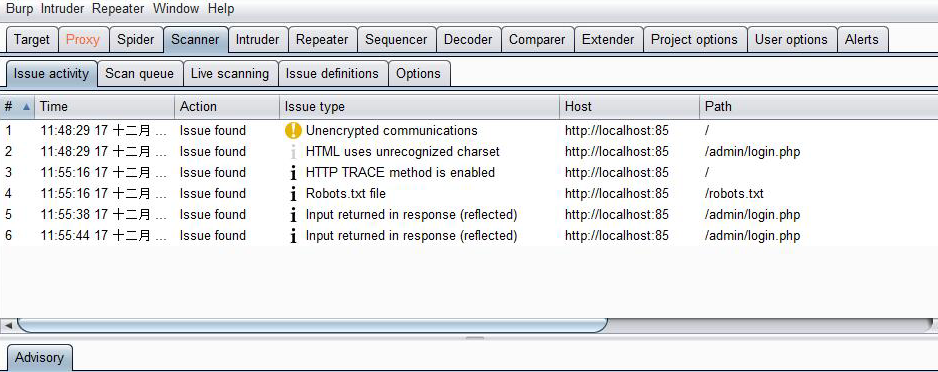
（3）端口扫描



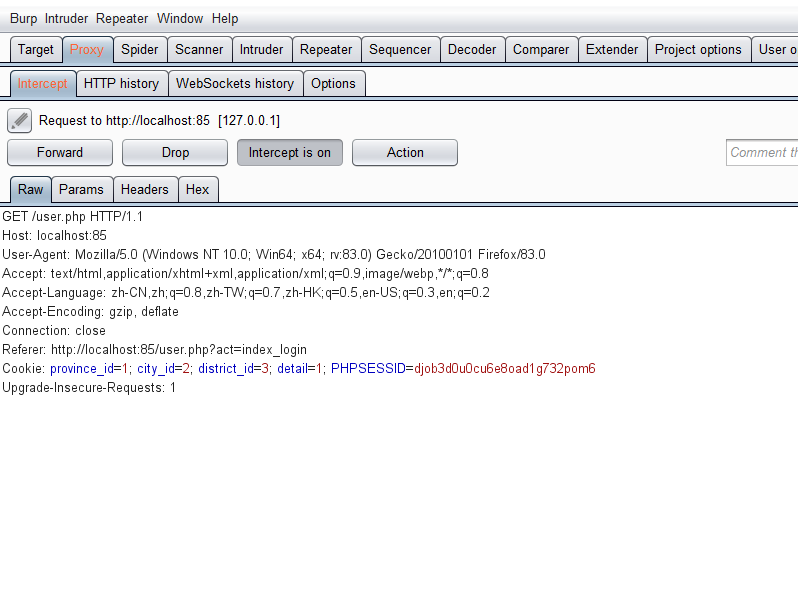
2.漏洞扫描

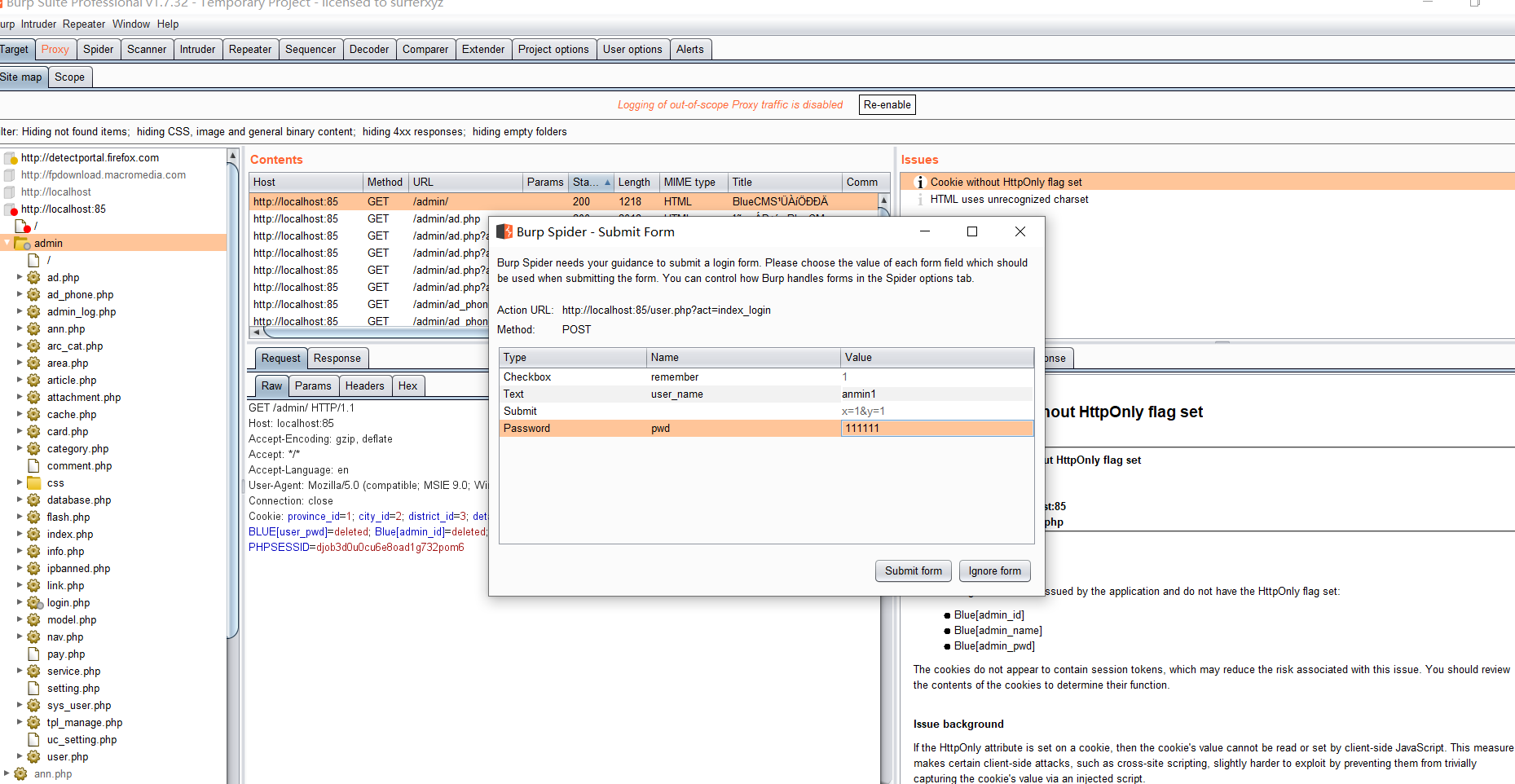
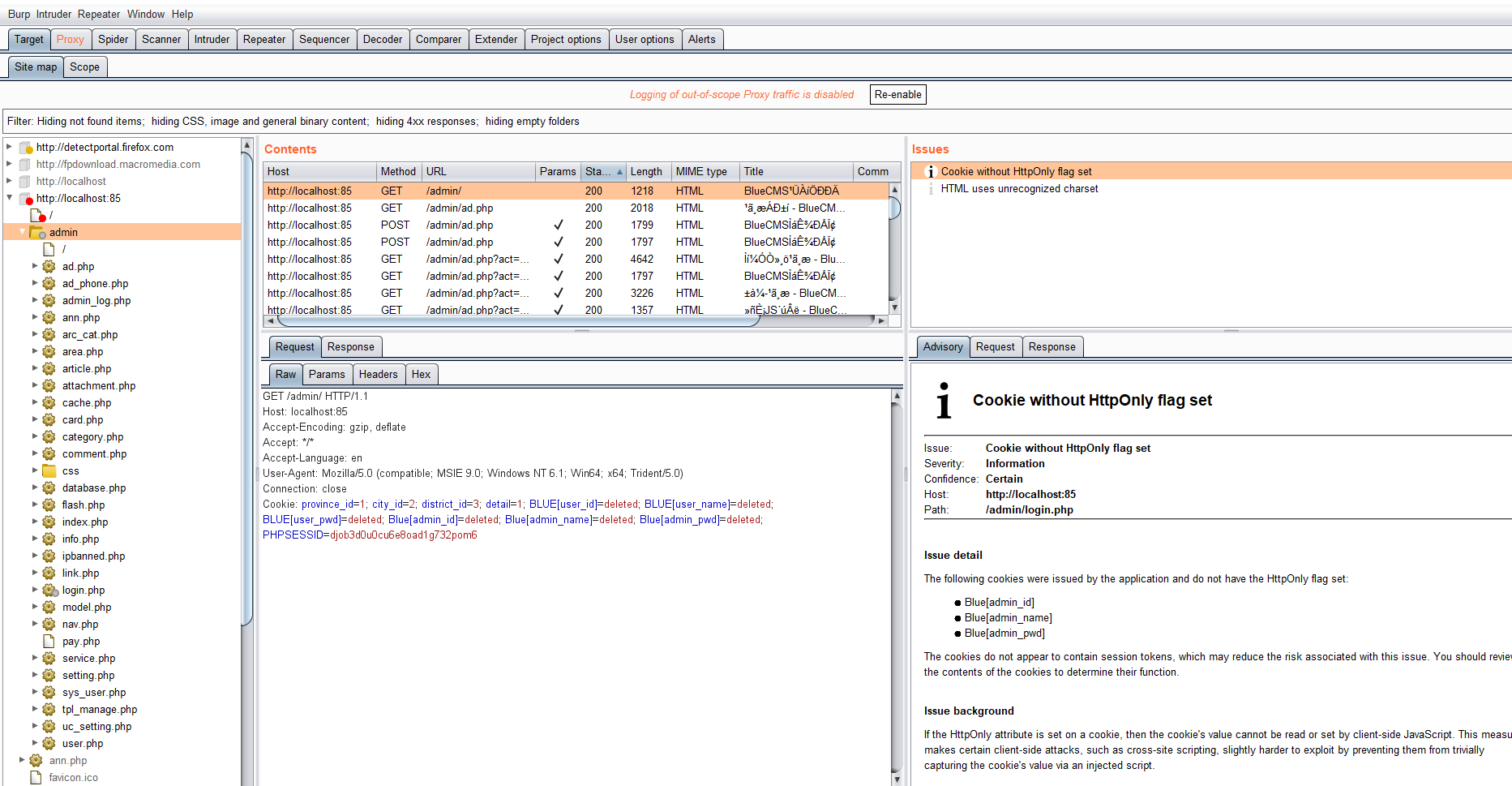


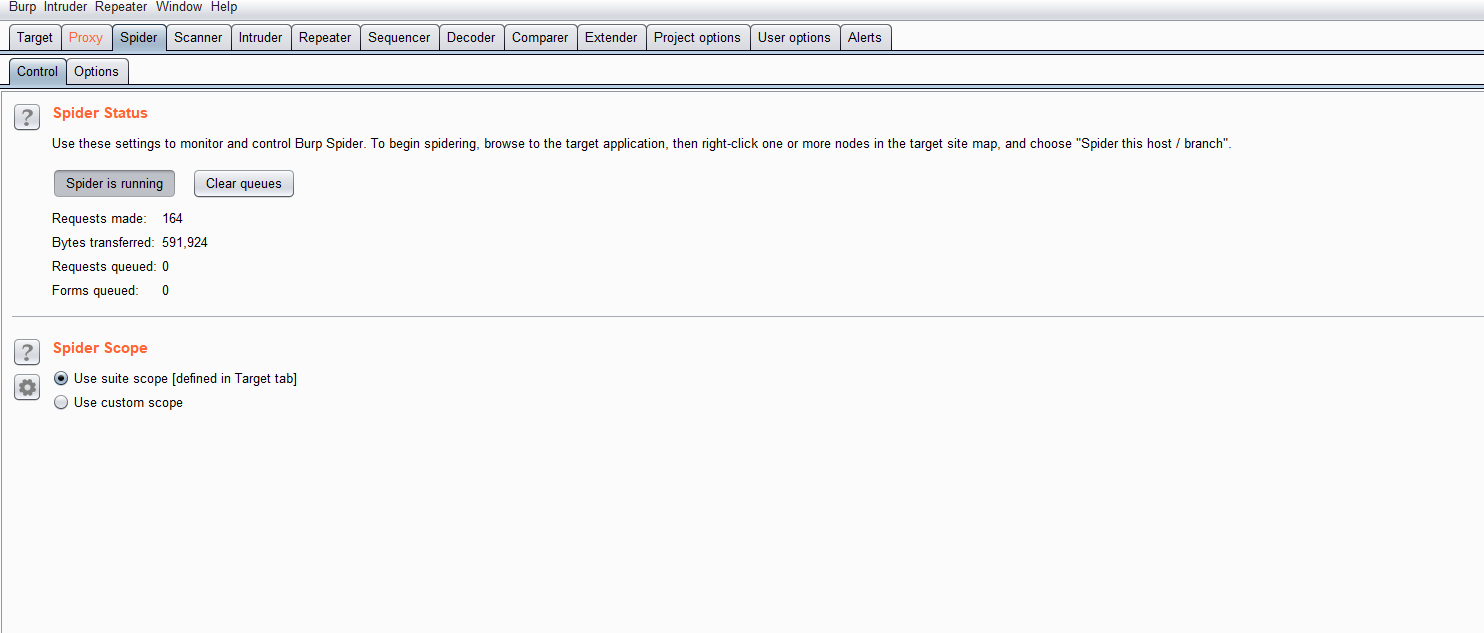




3爬取网站



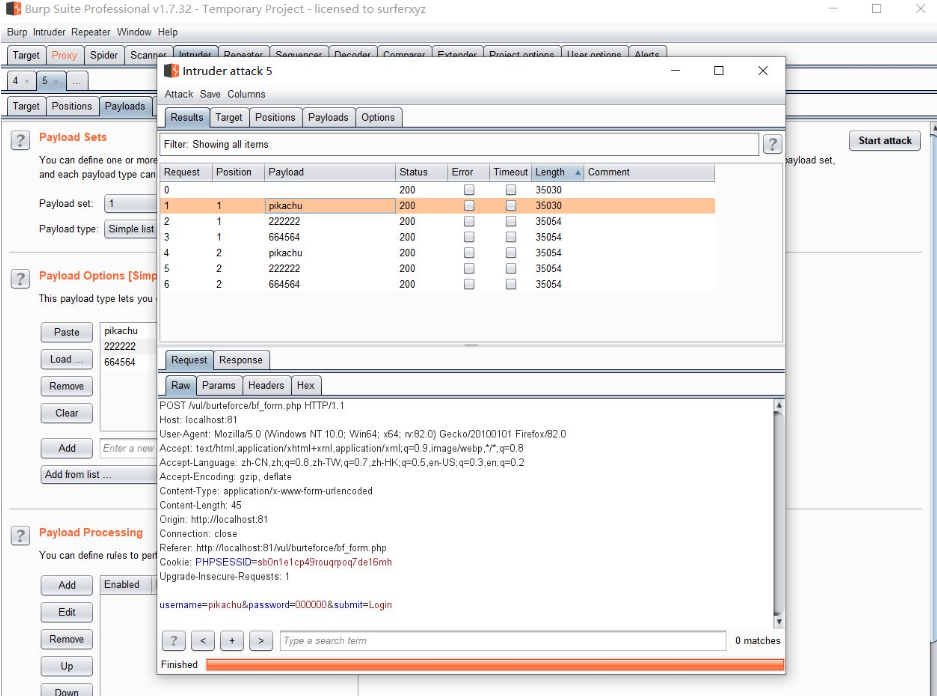




4.自动化攻击

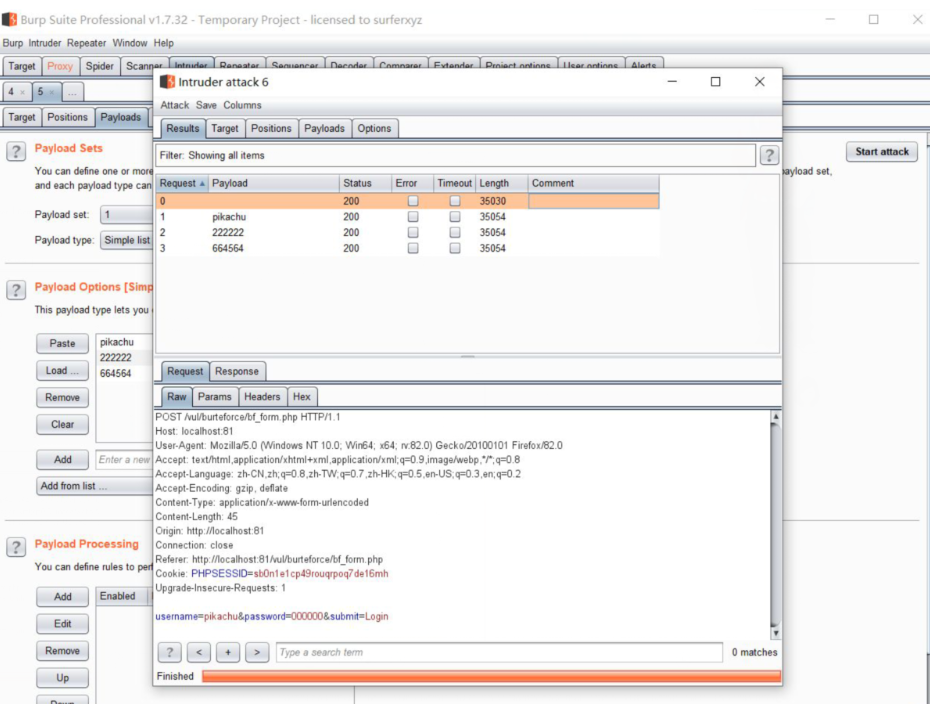
Sniper

如果添加了一个参数，且假设payload有200个的话，那就会执行200次。如果添加了两个参数的话，就会挨着来，第一个参数开始爆破时，第二个不变，然后会进行200+200次总共400次的爆破。



Battering ram

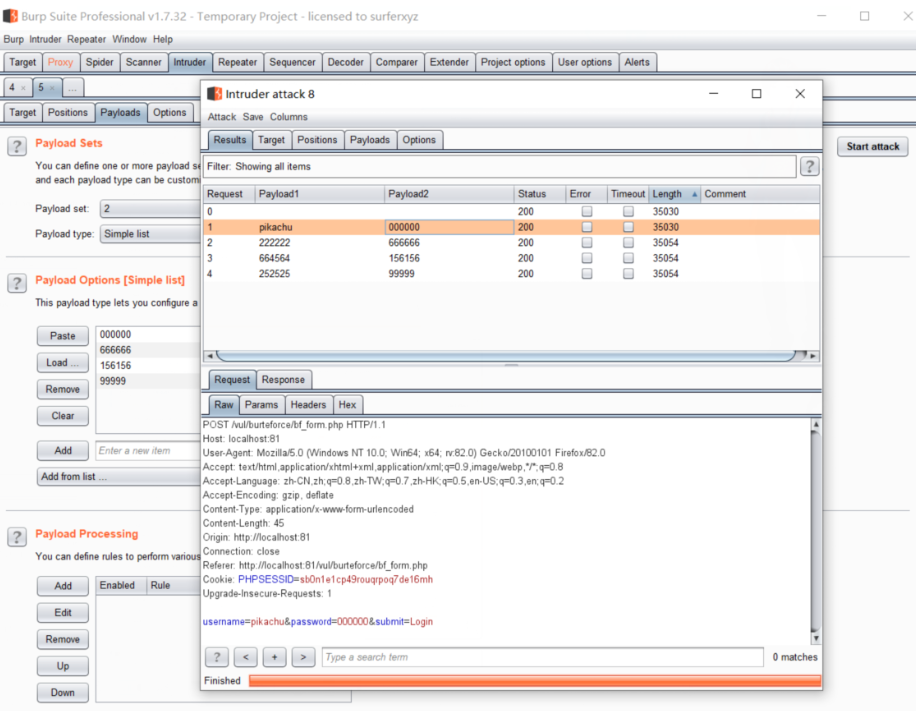
如果一个参数的话都一样，如果添加了两个参数的话，就一起进行爆破。两个参数爆破时候的值是一样的，然后会进行200次爆破



Pitchfork

此模式下如果只添加了一个参数的话，就会报错

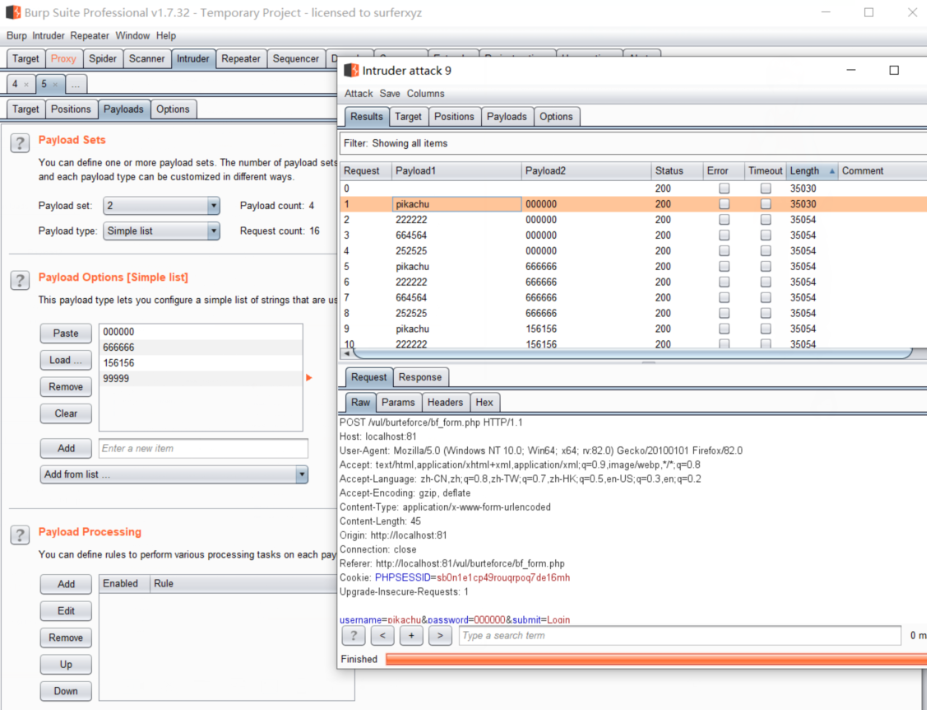
添加了两个参数的话 ，要求添加两个payload   
pl1：1，2  
pl2：3，4  
那么第一次爆破为 1，3  
而第二次爆破为2，4  
如果两个payload行数不一致的话，取最小值进行测试，爆破的次数取两个中最小的为准。



Cluster bomb

同pitchfork，起码要有两个参数，但此操作会计算两个的payload 的笛卡儿积。  
比如pl1：1，2，3  
pl2：4，5，6  
那么第一次爆破为 1，4  
第二次为1，5  
以此类推 第三次为1，6  
2，4  
2，5

......



5.手工测试

（1）我的个人资料处存在存储型XSS

在修改资料处，在电子邮件地址中输入<script>alert('xss')</script>语句，点击确认修改后。

结果：代码被执行，出现弹窗，当再次访问该页面，代码会再次执行，出现弹窗。

后台

(1)添加新会员处存在存储型XSS

在电子邮件中输入<script>alert('1111')</script>语句，点击提交。

结果：代码被执行，出现弹窗，显示1111，当再次访问该页面，代码会再次执行，出现弹窗。

(2)在广告管理的添加新广告处存在存储型XSS

在广告名称中输入<script>alert('8')</script>语句，点击提交

结果：代码被执行，出现弹窗，显示8，当再次访问该页面，代码会再次执行，出现弹窗。

（3）在友情链接的添加新链接处存在存储型XSS

在链接名称中输入<script>alert('xsssll')</script>语句，点击提交

结果：代码被执行，出现弹窗，显示xsssll，当再次访问该页面，代码会再次执行，出现弹窗。

（4）在电话广告位的添加新电话广告中存在存储型XSS

在显示名称中输入<script>alert('xssss')</script>语句，点击提交

结果：代码被执行，出现弹窗，显示xssss，当再次访问该页面，代码会再次执行，出现弹窗。

（5）发布本地新闻处存在存储型XSS漏洞，

在新闻标题中填写<script>alert('1')</script>，然后选择分类，输入新闻内容，点击提交。

结果：代码被执行，出现弹窗，显示1，当再次访问该页面，代码会再次执行，出现弹窗。

（6）在首页flash的添加新flash中存在存储型型XSS

浏览并插入图片，在图片链接中填写<script>alert('11')</script>，然后点击提交。

结果：代码被执行，出现弹窗，显示11，当再次访问该页面，代码会再次执行，出现弹窗。

（7）在导航管理的添加新连接处存在存储型XSS

在导航名称中输入<script>alert('1233')</script>，输入导航链接，点击提交。

结果：代码被执行，出现弹窗，显示1233，当再次访问该页面，代码会再次执行，出现弹窗。

输入导航名称，在导航链接中输入<script>alert('1233')</script>，点击提交。

结果：代码被执行，出现弹窗，显示1233，当再次访问该页面，代码会再次执行，出现弹窗。

（8）在新闻分类的添加栏目中存在存储型XSS

在分类名称中输入<script>alert('1233')</script>，点击提交。

结果：代码被执行，出现弹窗，显示1233，当再次访问该页面，代码会再次执行，出现弹窗。

(9) 在系统组用户中存在存储型XSS

进入系统组用户，点击编辑，在电子邮件中输入<script>alert('123456')</script>，输入密码，点击提交。

结果：代码被执行，出现弹窗，显示123456，当再次访问该页面，代码会再次执行，出现弹窗。

（10）输入正确的用户名和错误的密码也会提示用户名和密码不正确

