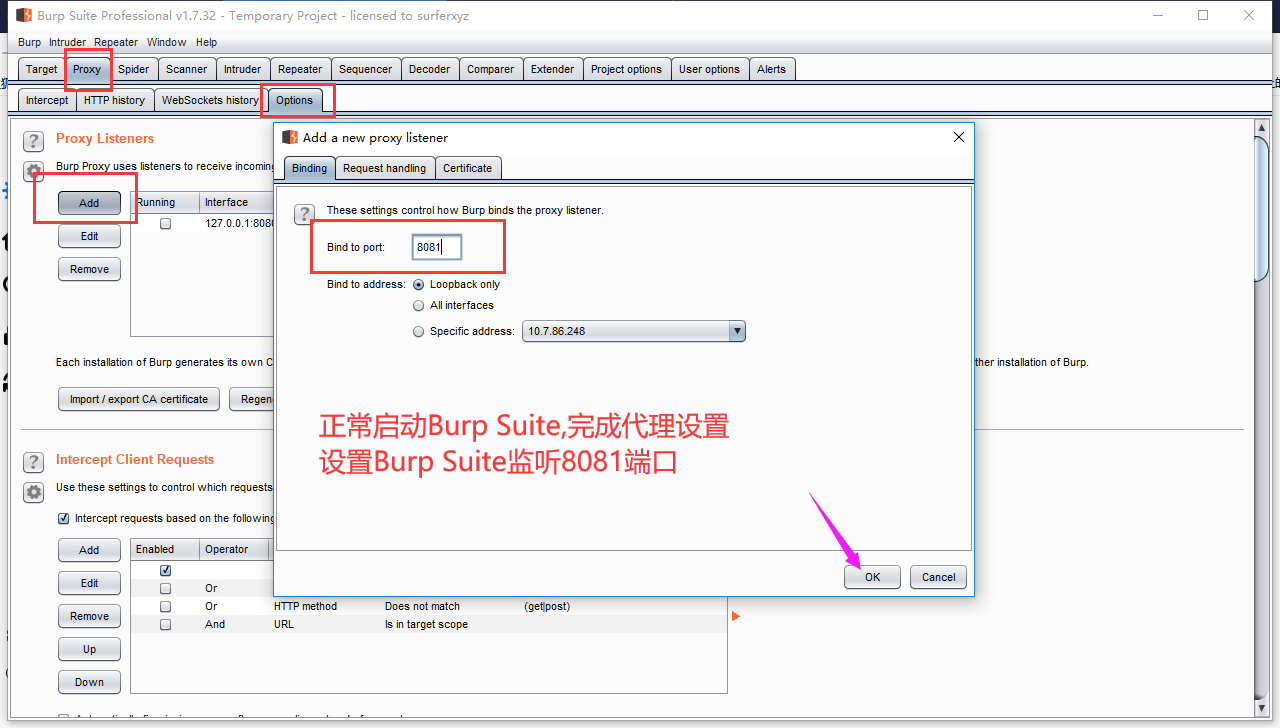
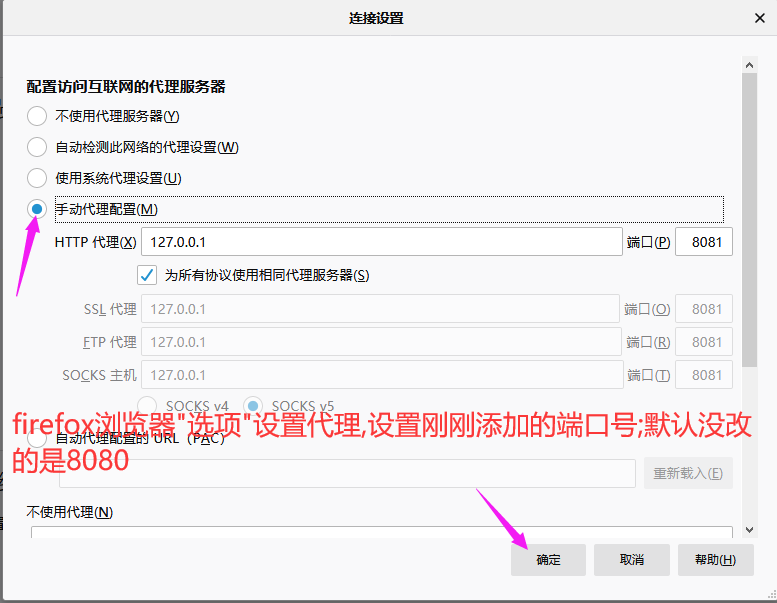
# 漏洞扫描-<http://localhost:9775/uploads/>

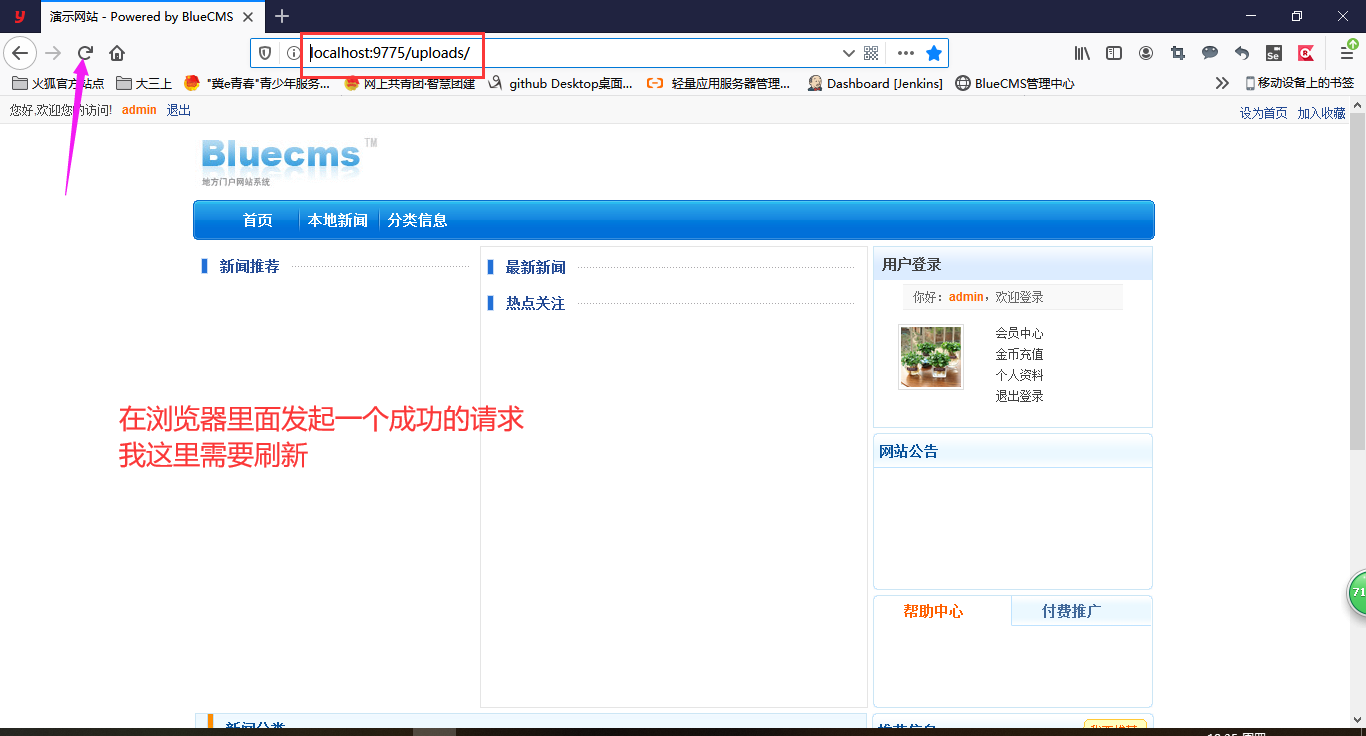
1. 工具 Burp Suite-Scanner
2. 网站 <http://localhost:9775/uploads/>
3. 过程
4. 正常启动Burp Suite,完成代理设置;设置Burp Suite监听8081端口;

如果本地没有其他应用占用默认端口8080,可以不设置



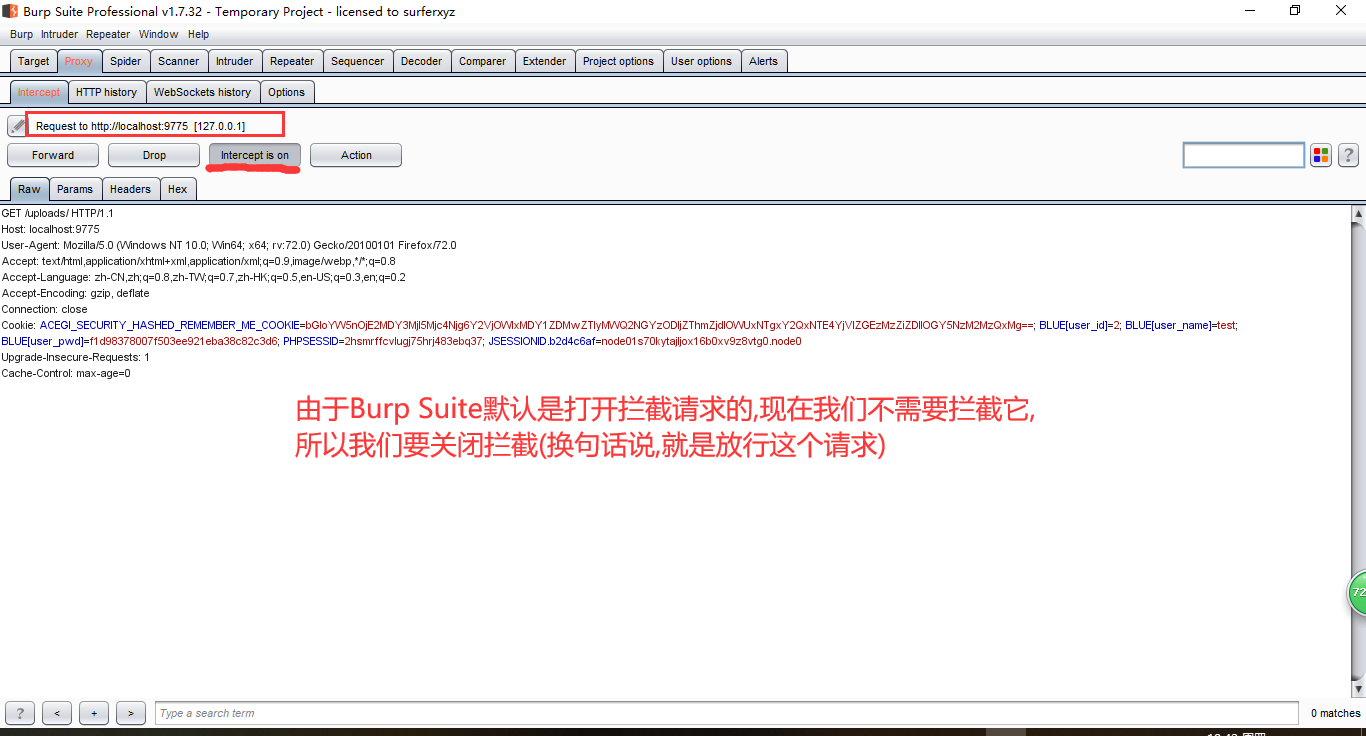


1. 在浏览器发起一个正常成功的请求,我这里需要刷新,因为我提前打开过一次网站了

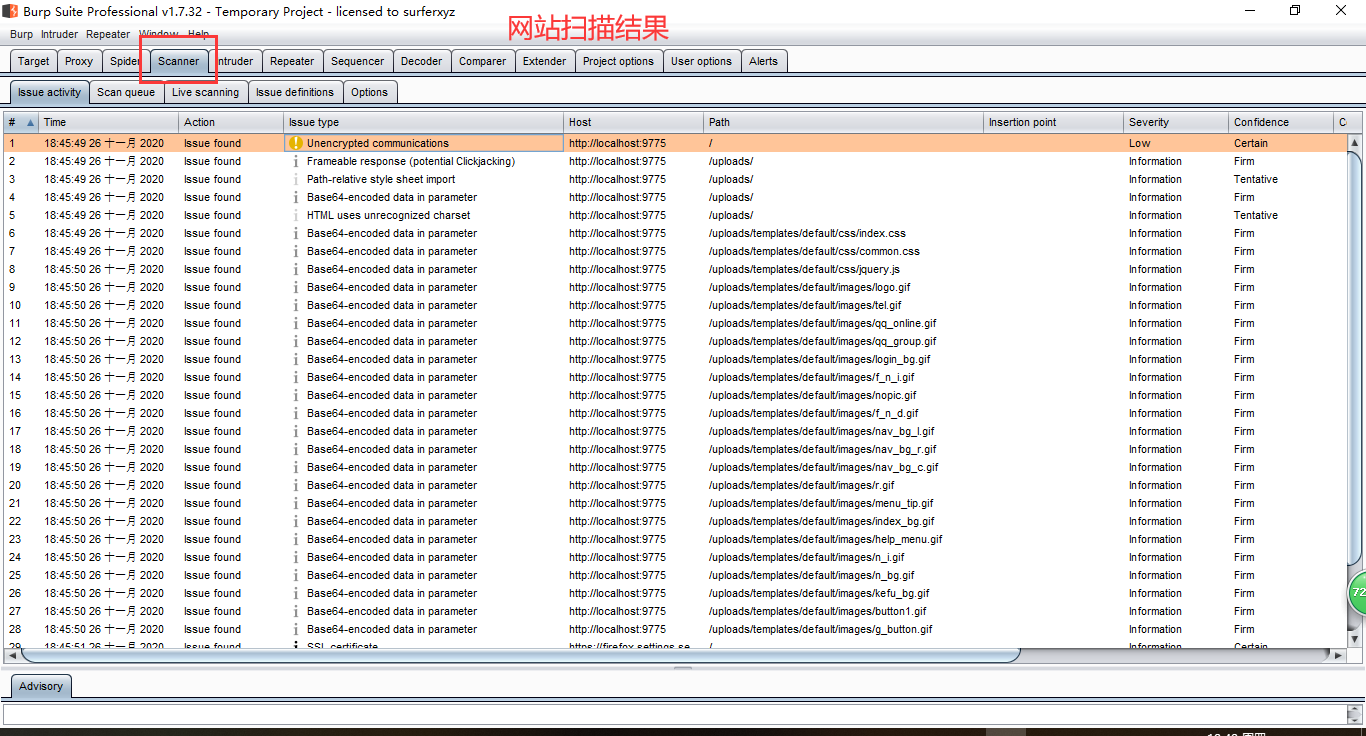


1. 刷新之后,Burp Suite亮了:拦截到一个该网站的请求,Burp Suite默认是拦截请求的,现在我们不需要拦截请求,而是要扫描网站,所以我们要关闭拦截请求





1. 点击Scanner,查看网站扫描结果



4.网站扫描结果 33

|  |  |  |  |
| --- | --- | --- | --- |
| 编号 | 严重程度 | 数量 | 备注 |
| 1 | Low | 1 | Unencrypted communications |
| 2 | Information | 32 |  |
| 结论:此网站存在的漏洞严重程度较低 | | | |

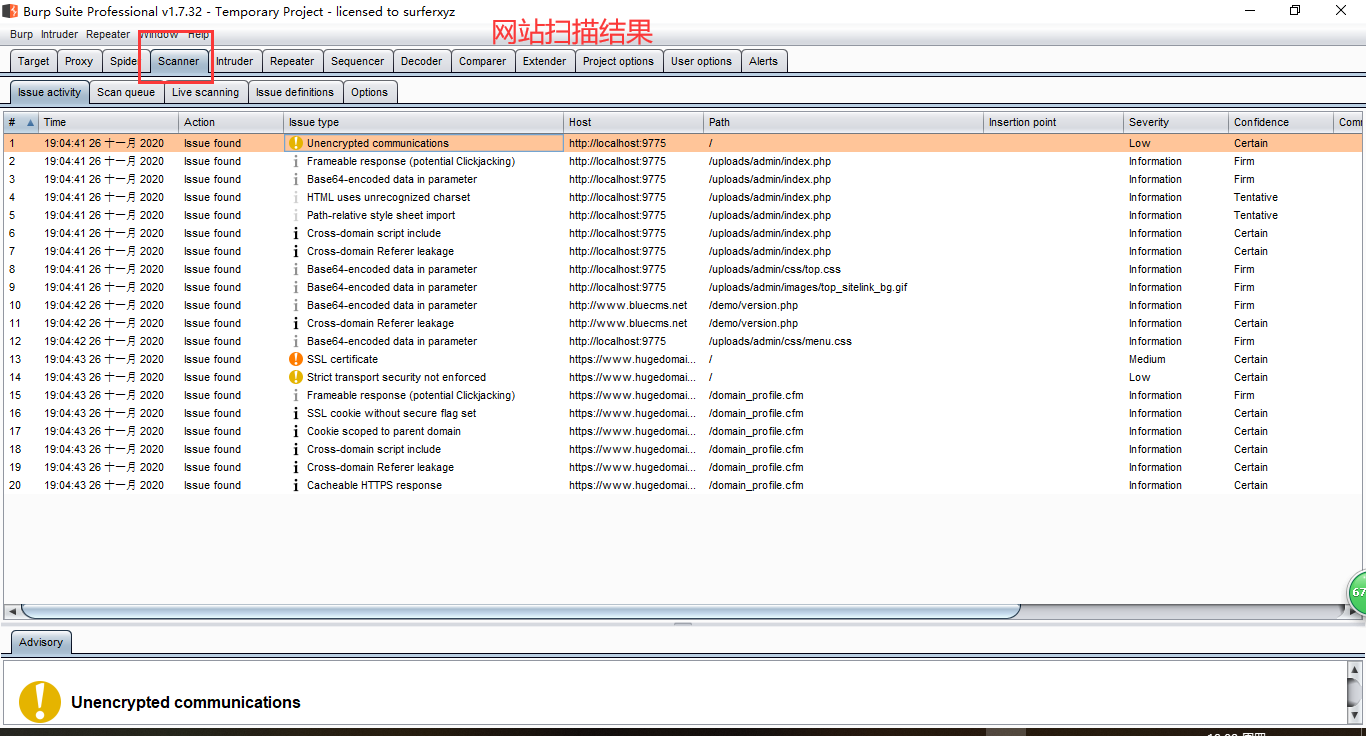
# 漏洞扫描-http://localhost:9775/uploads/admin/index.php

1. 工具 Burp Suite-Scanner
2. 网站 <http://localhost:9775/uploads/admin/index.php>
3. 过程

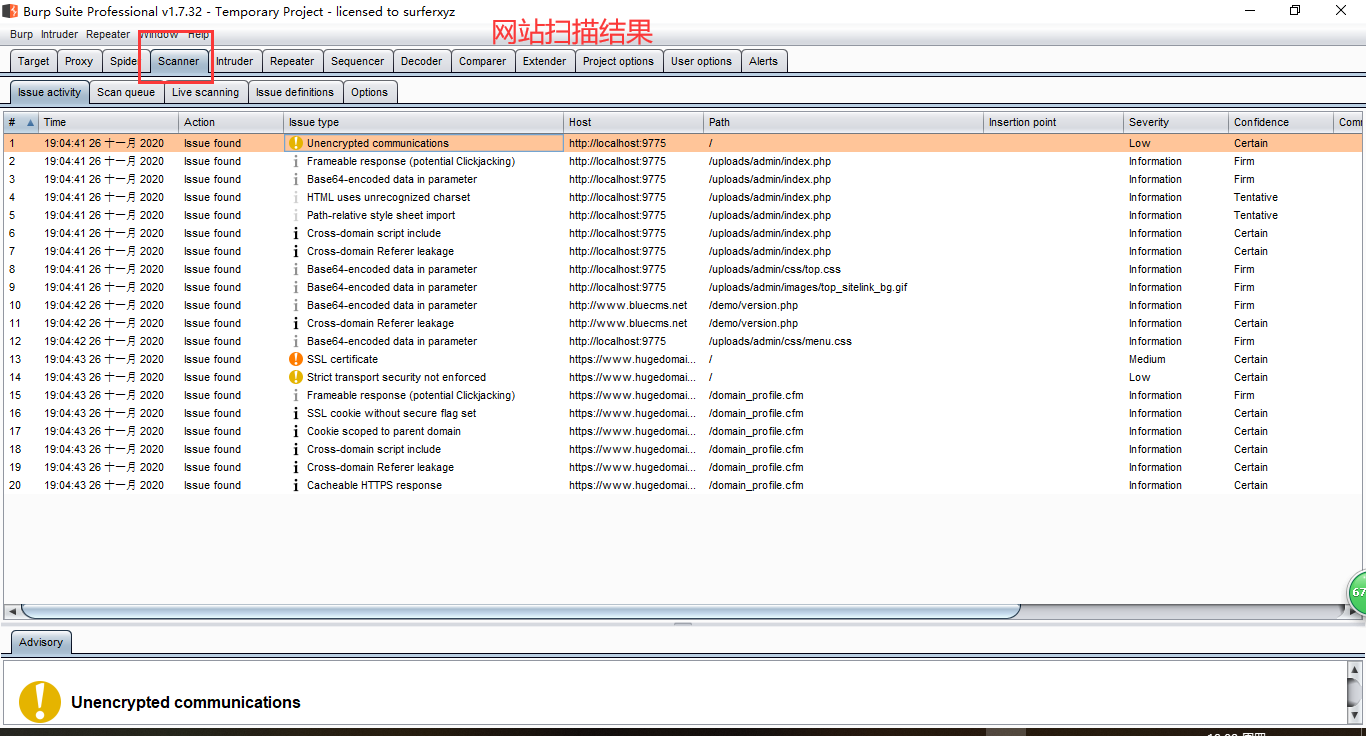
* 正常启动Burp Suite,完成代理设置
* 在浏览器发起一个正常成功的请求,我这里需要刷新,因为我提前打开过一次网站了



* 关闭拦截请求
* 点击Scanner,查看网站扫描结果



* 点击Scanner,查看网站扫描结果



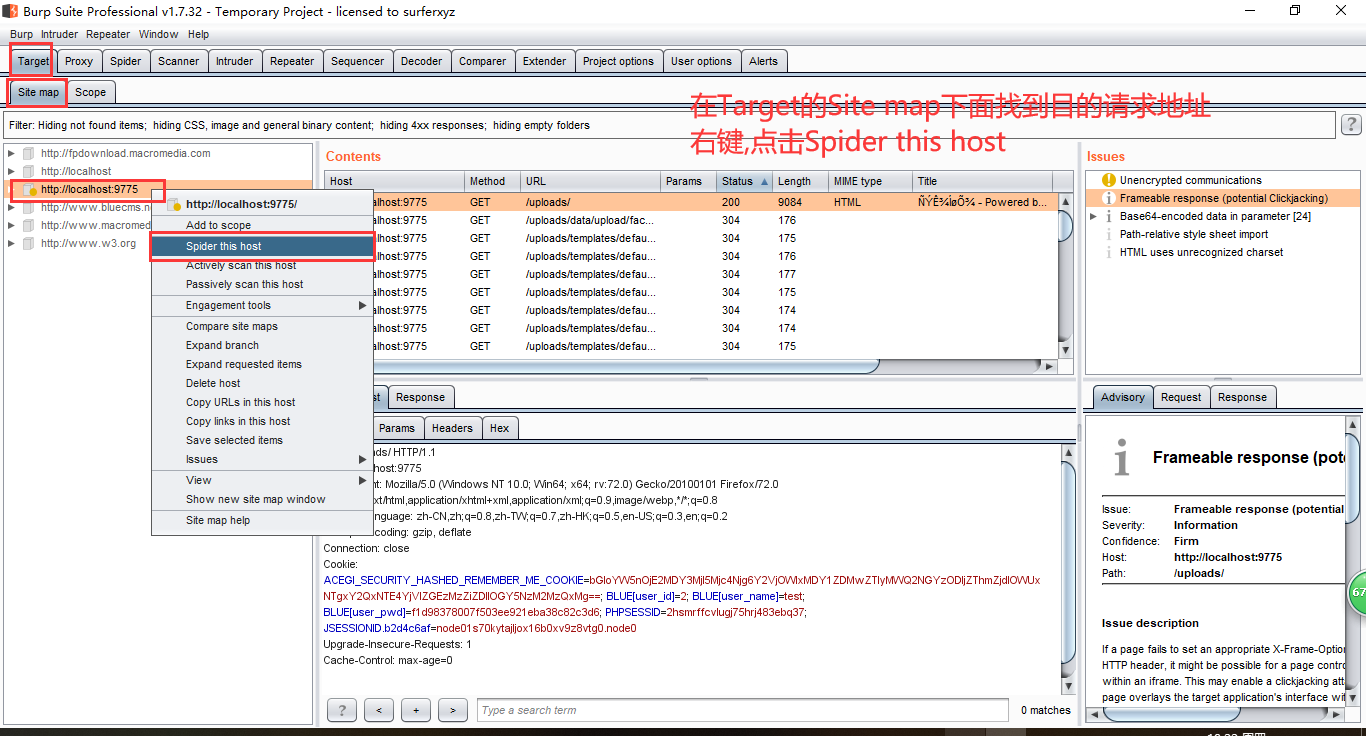
1. 网站扫描结果 20

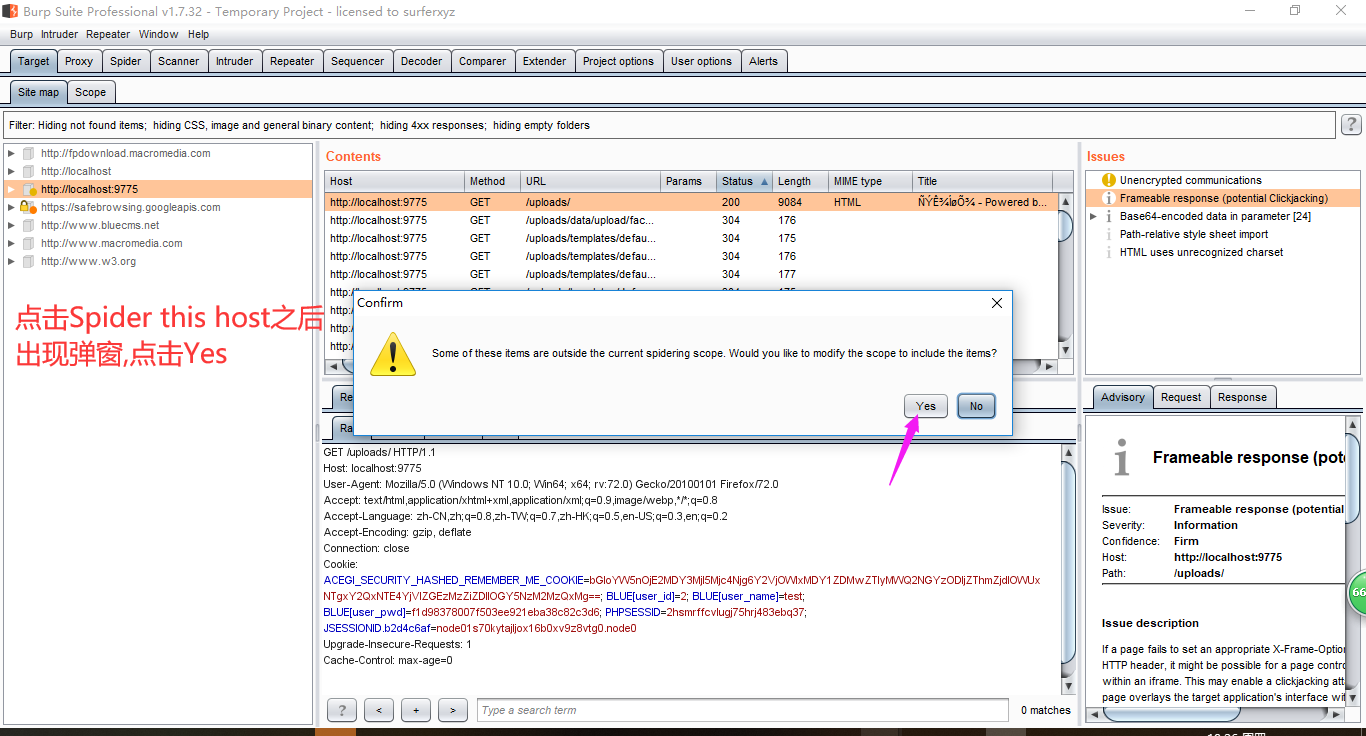
|  |  |  |  |
| --- | --- | --- | --- |
| 编号 | 严重程度 | 数量 | 备注 |
| 1 | Medium | 1 | SSL certificate |
| 2 | Low | 2 | Unencrypted communications;  Strict transport security not enforced |
| 3 | Information | 17 |  |

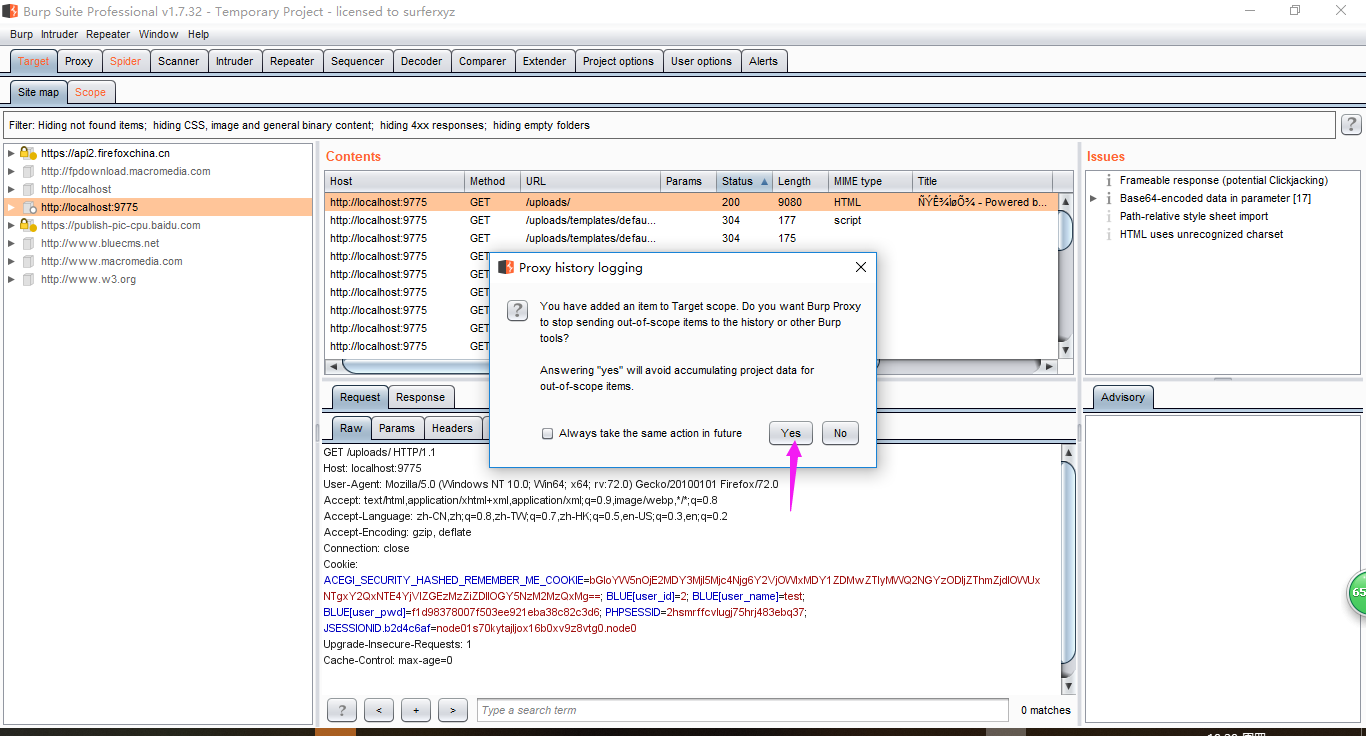
# 网站爬取- <http://localhost:9775/uploads/>

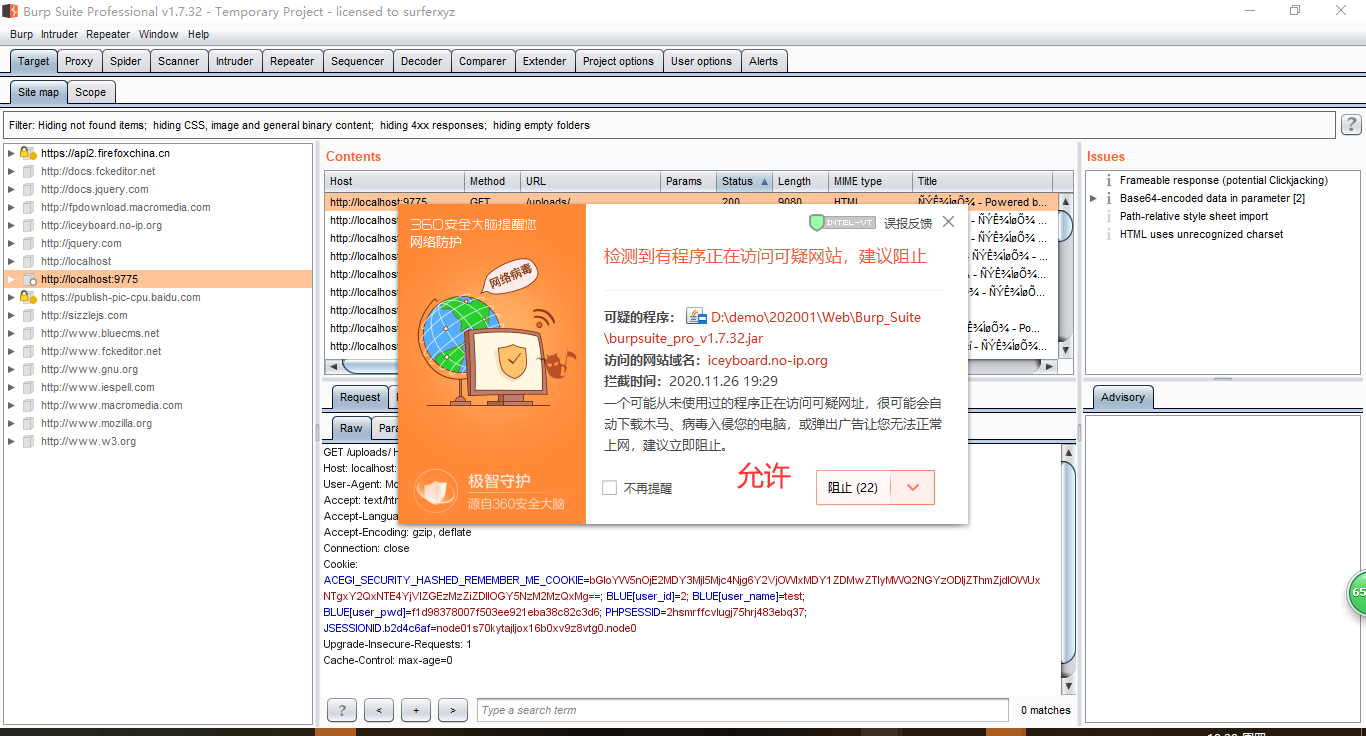
1. 工具 Burp Suite-Spider
2. 网站 <http://localhost:9775/uploads/>
3. 过程

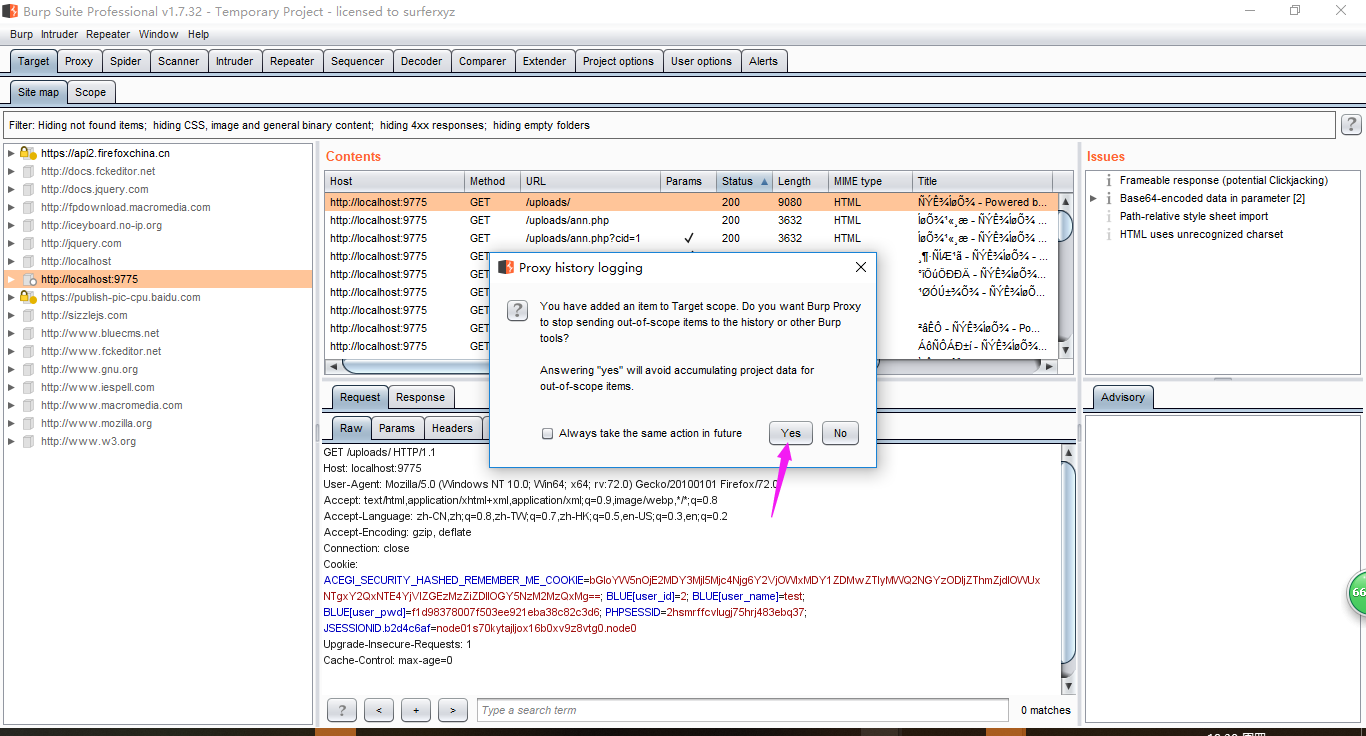
* 正常启动Burp Suite,完成代理设置
* 在浏览器发起一个正常成功的请求,我这里需要刷新,因为我提前打开过一次网站了
* 关闭拦截请求
* 在Target下面的Site map找到目的请求地址,右键点击Spider this host

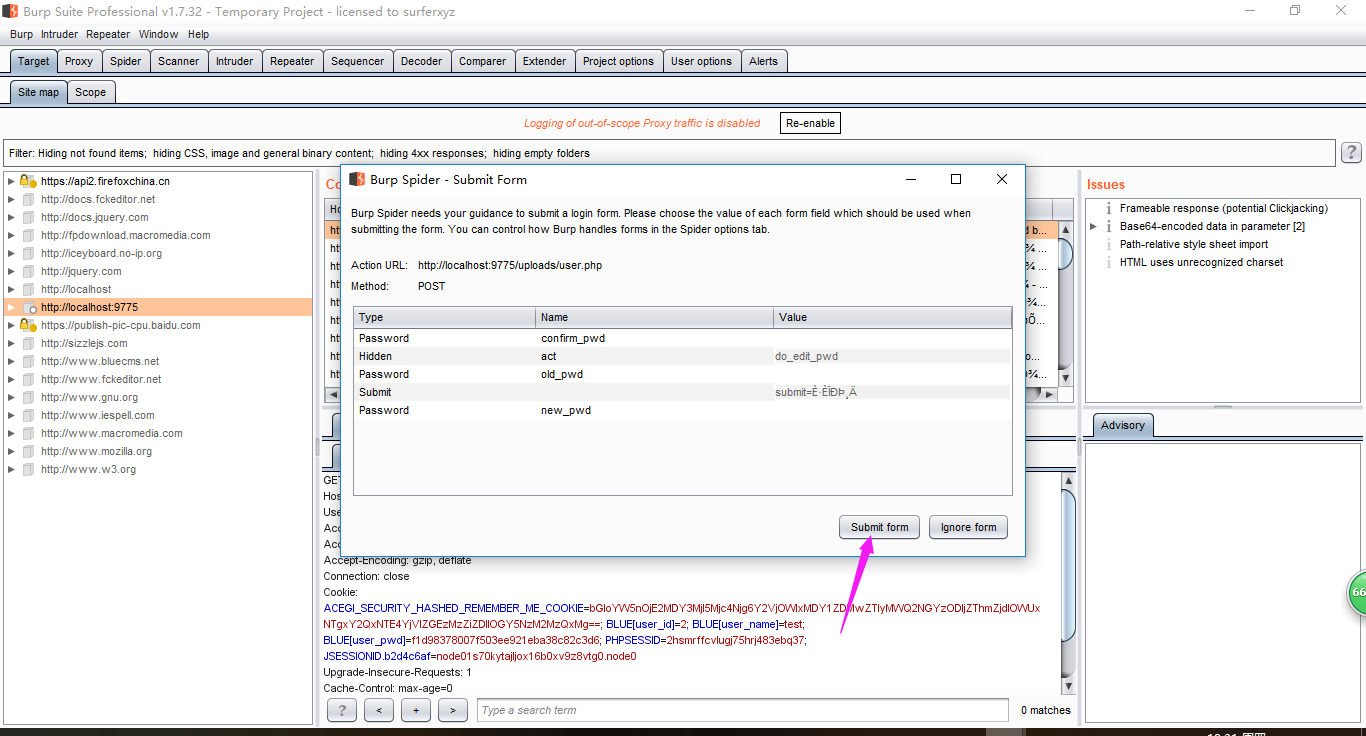


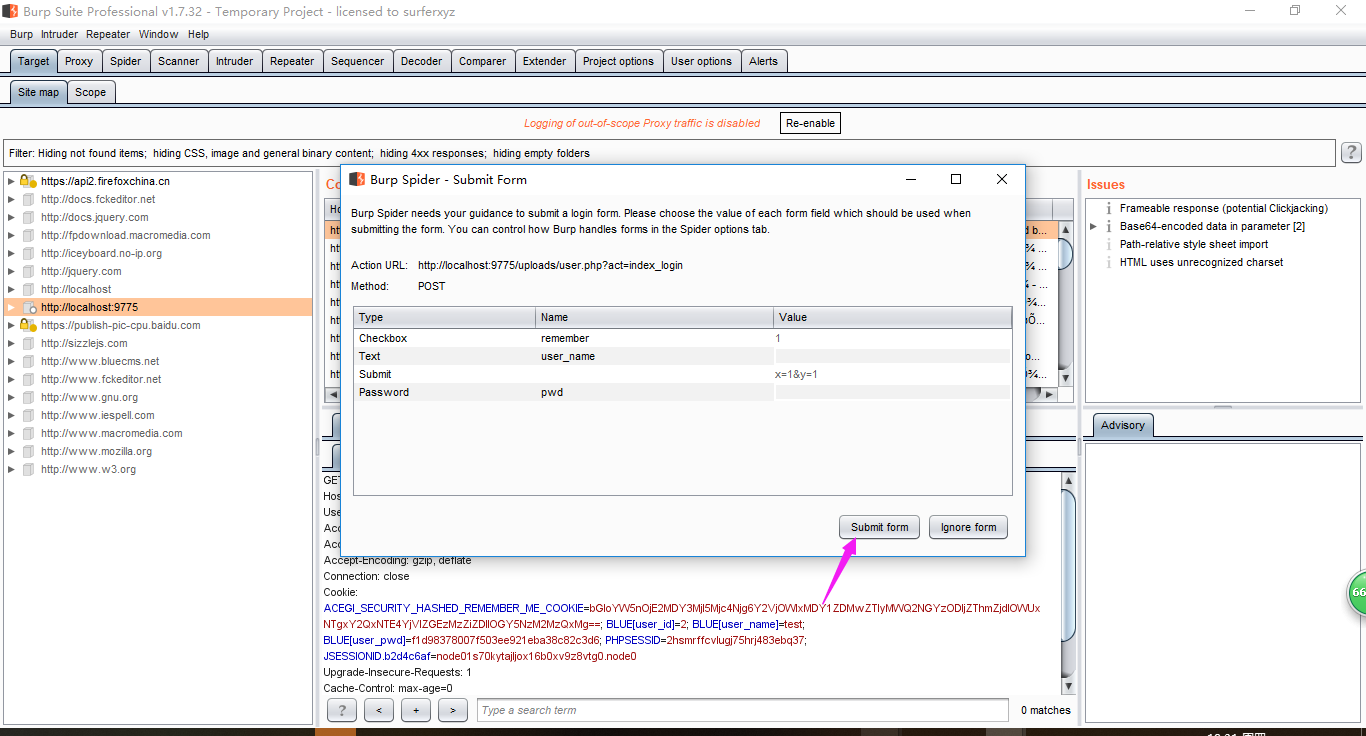




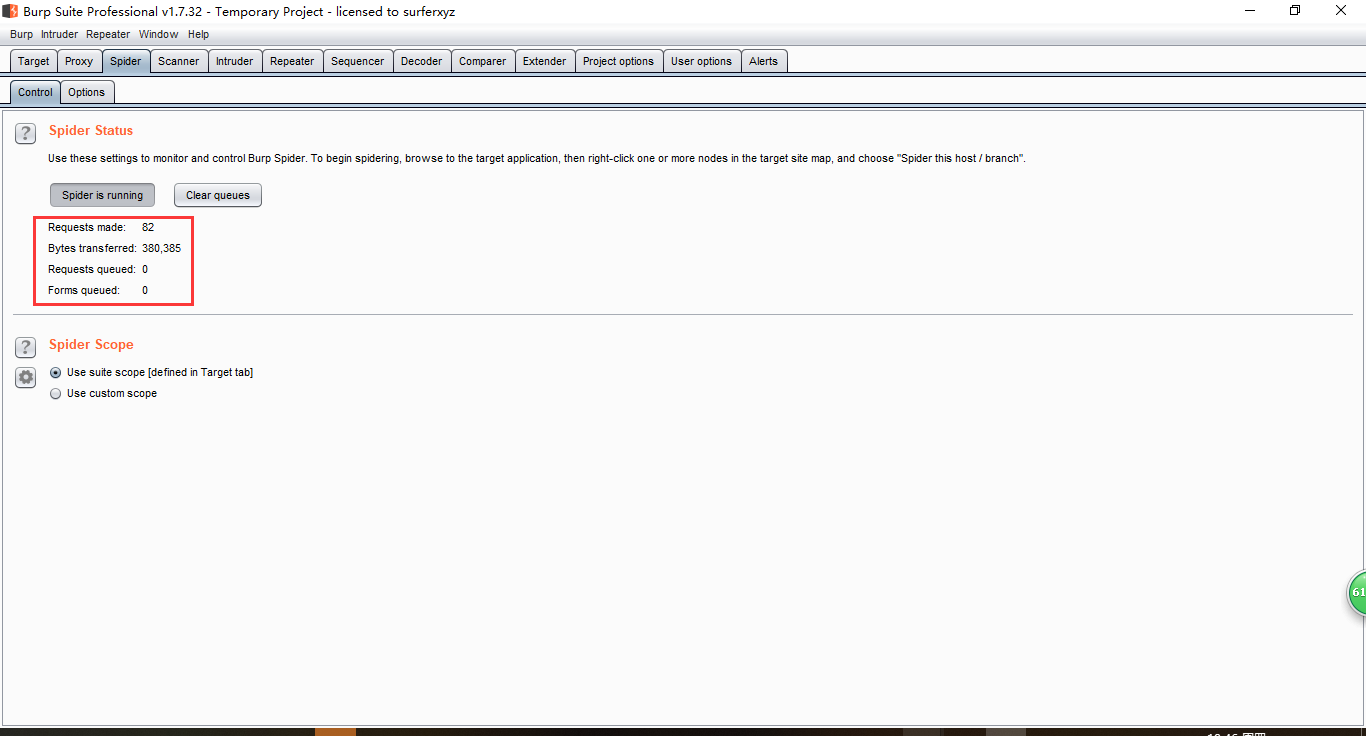








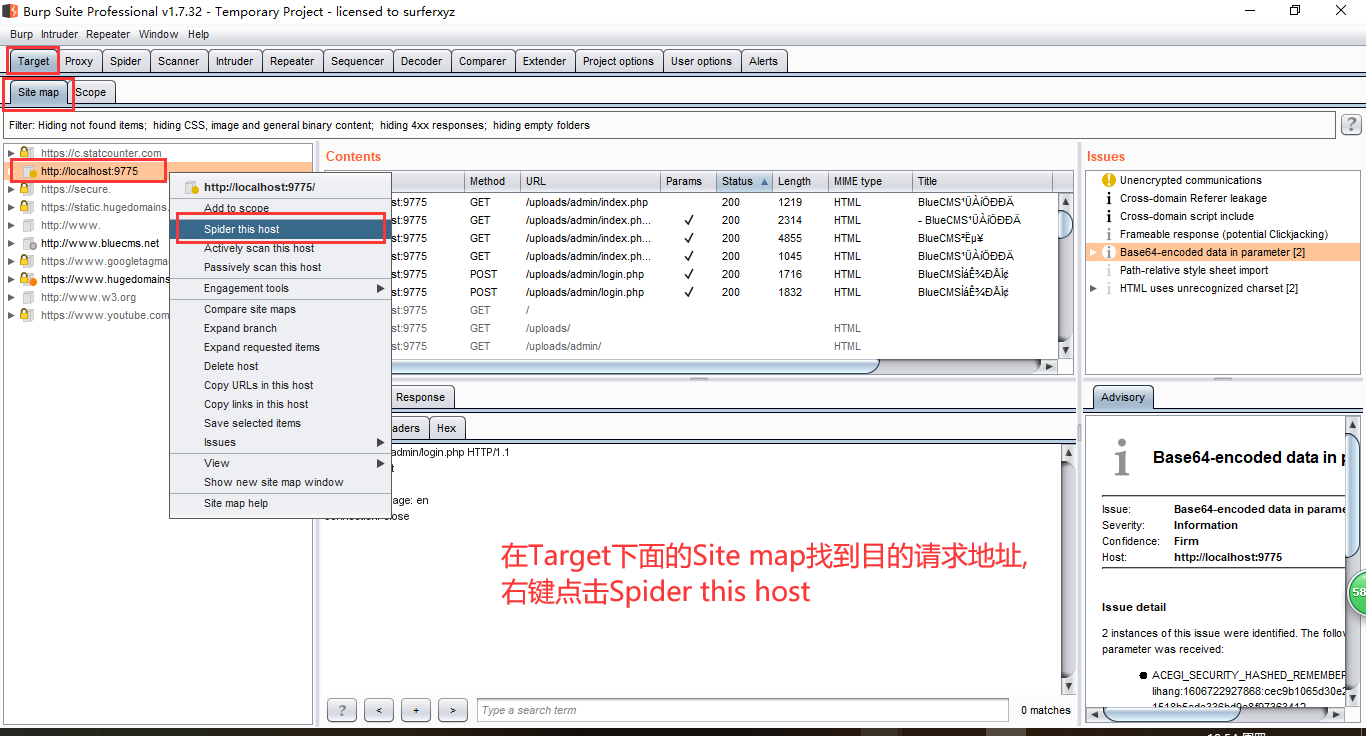
* 爬取数据

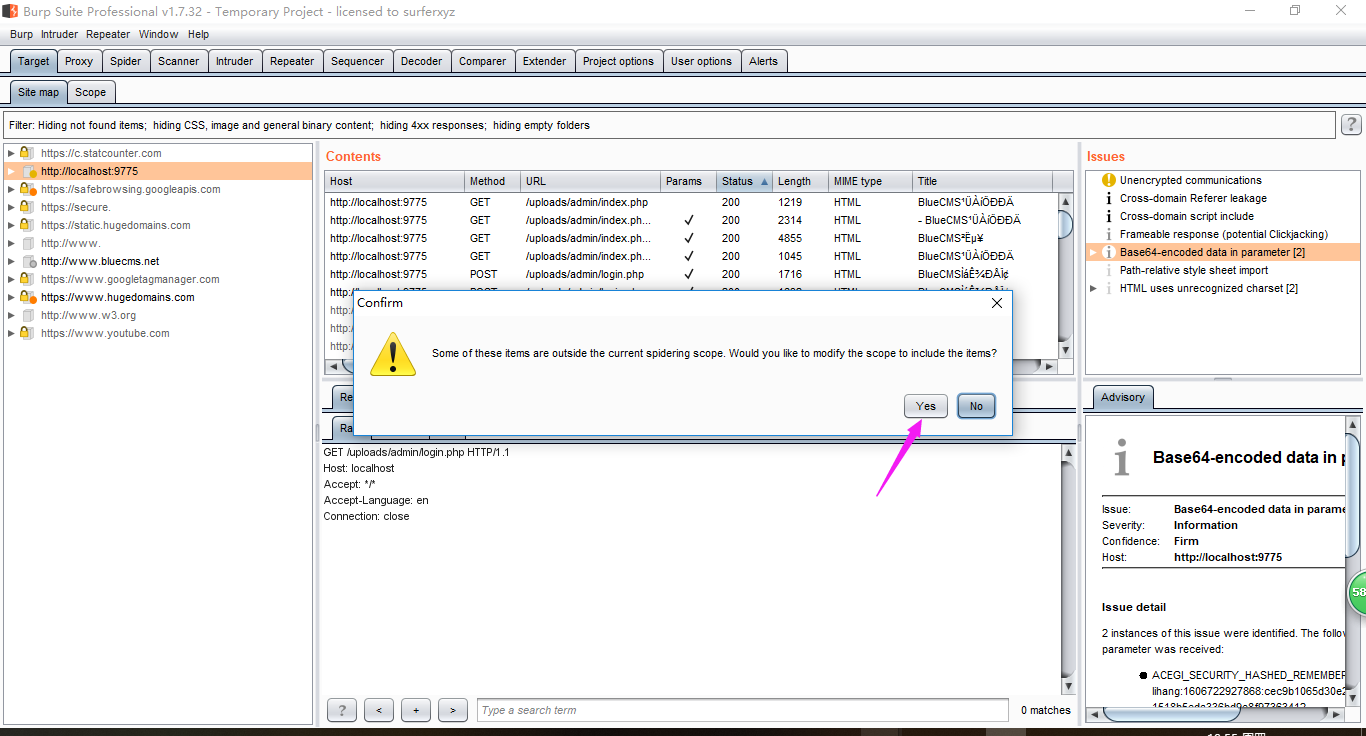


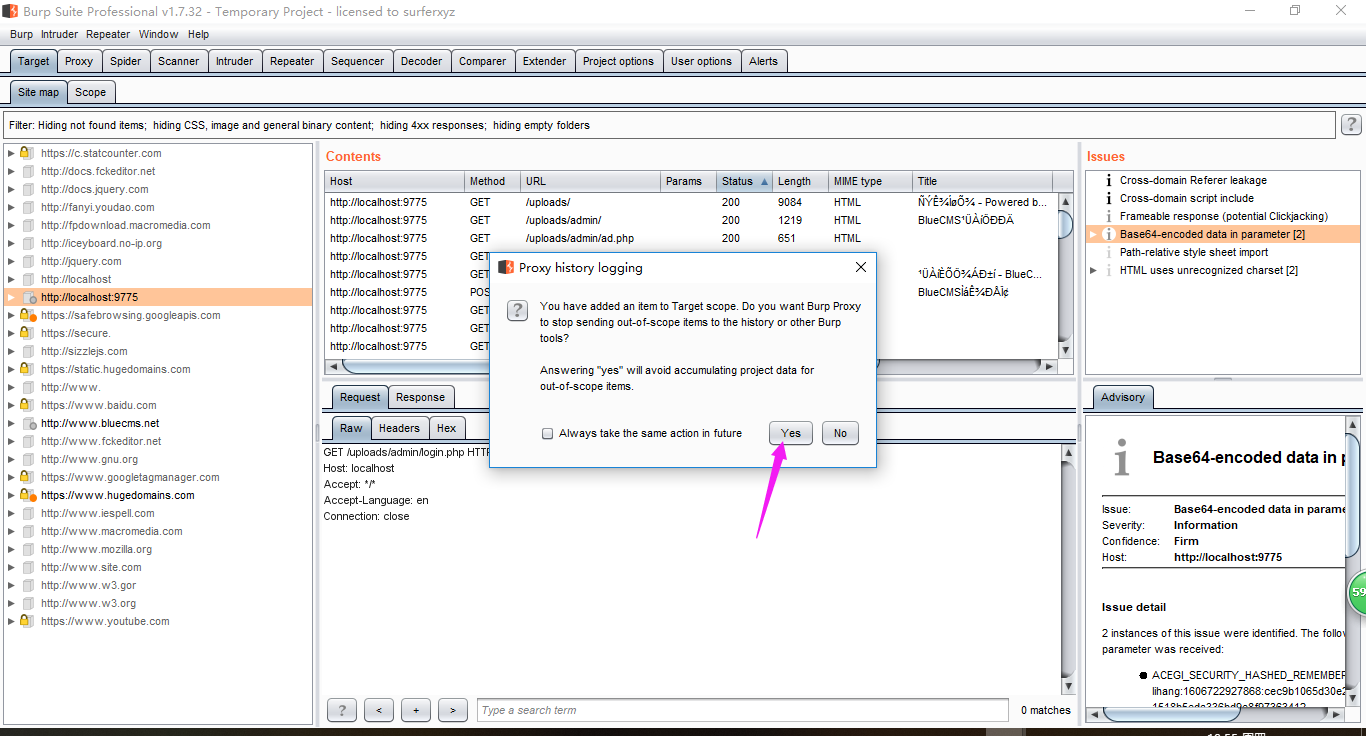
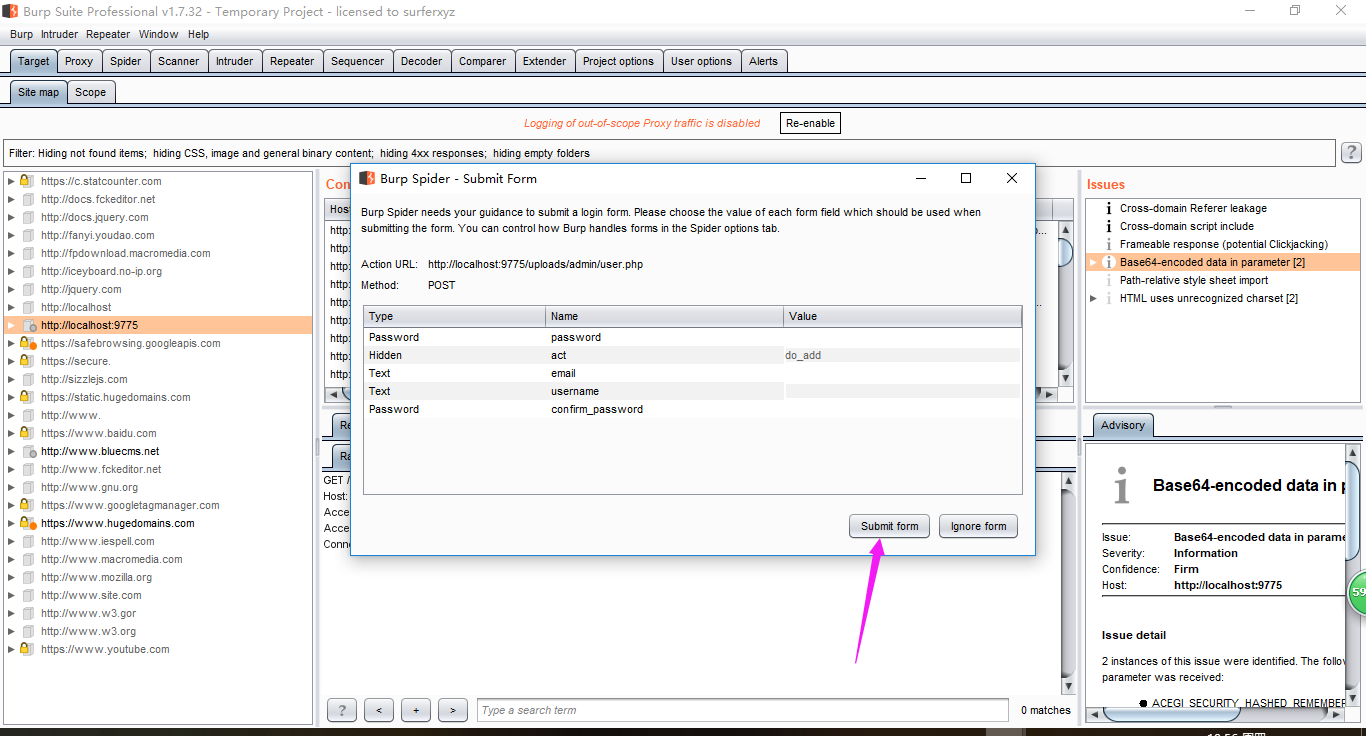
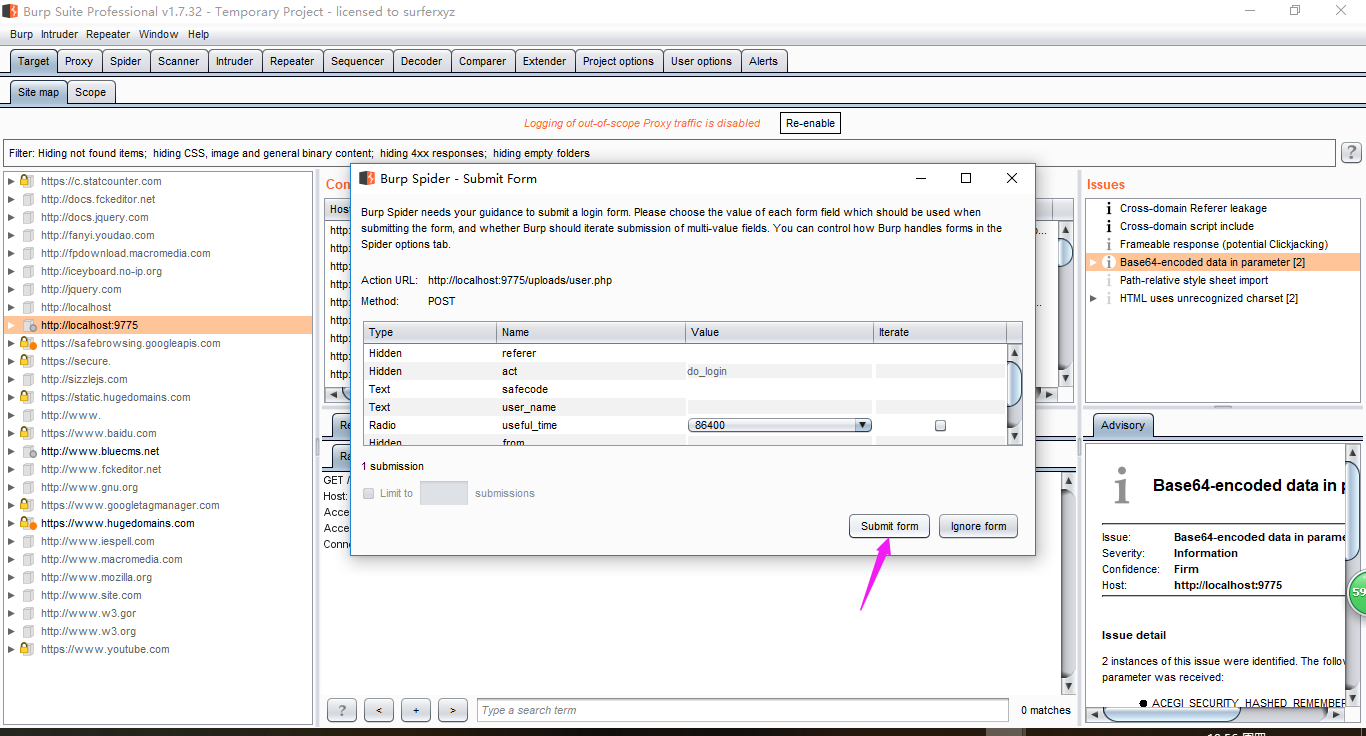
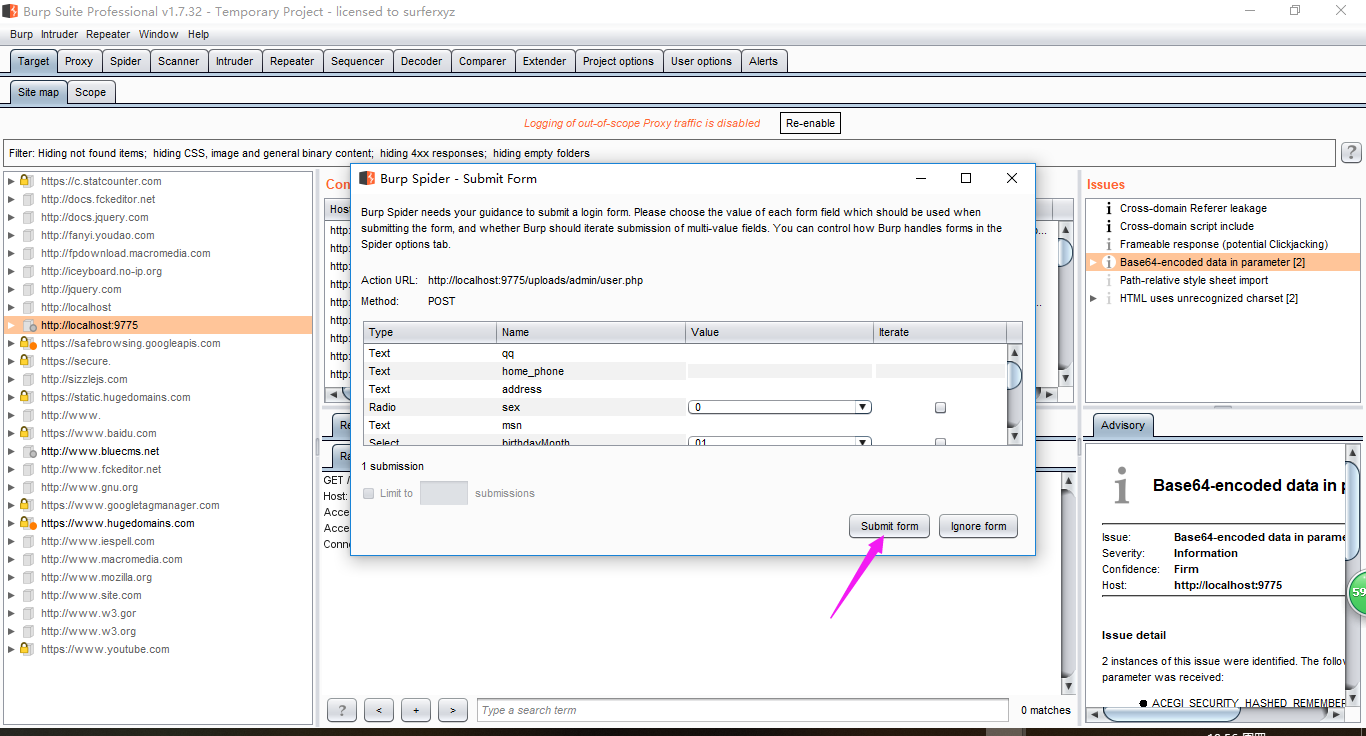
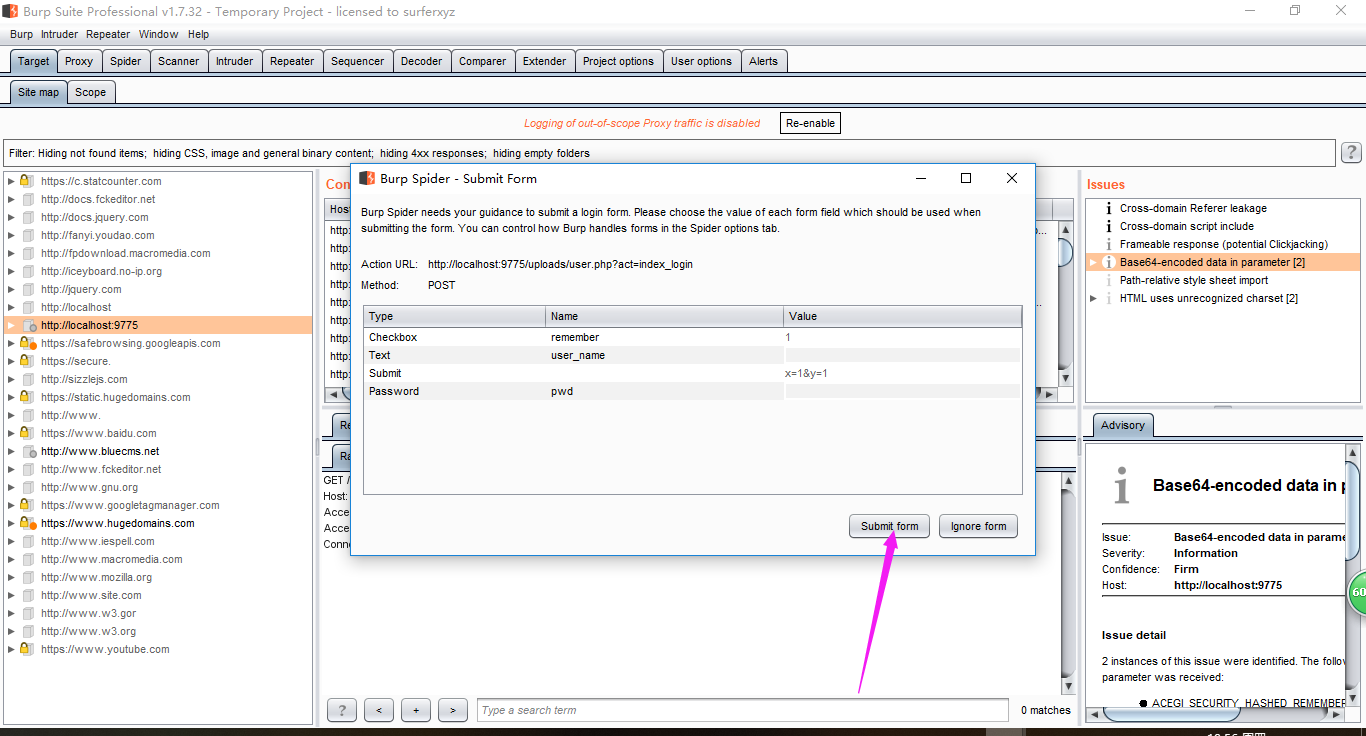
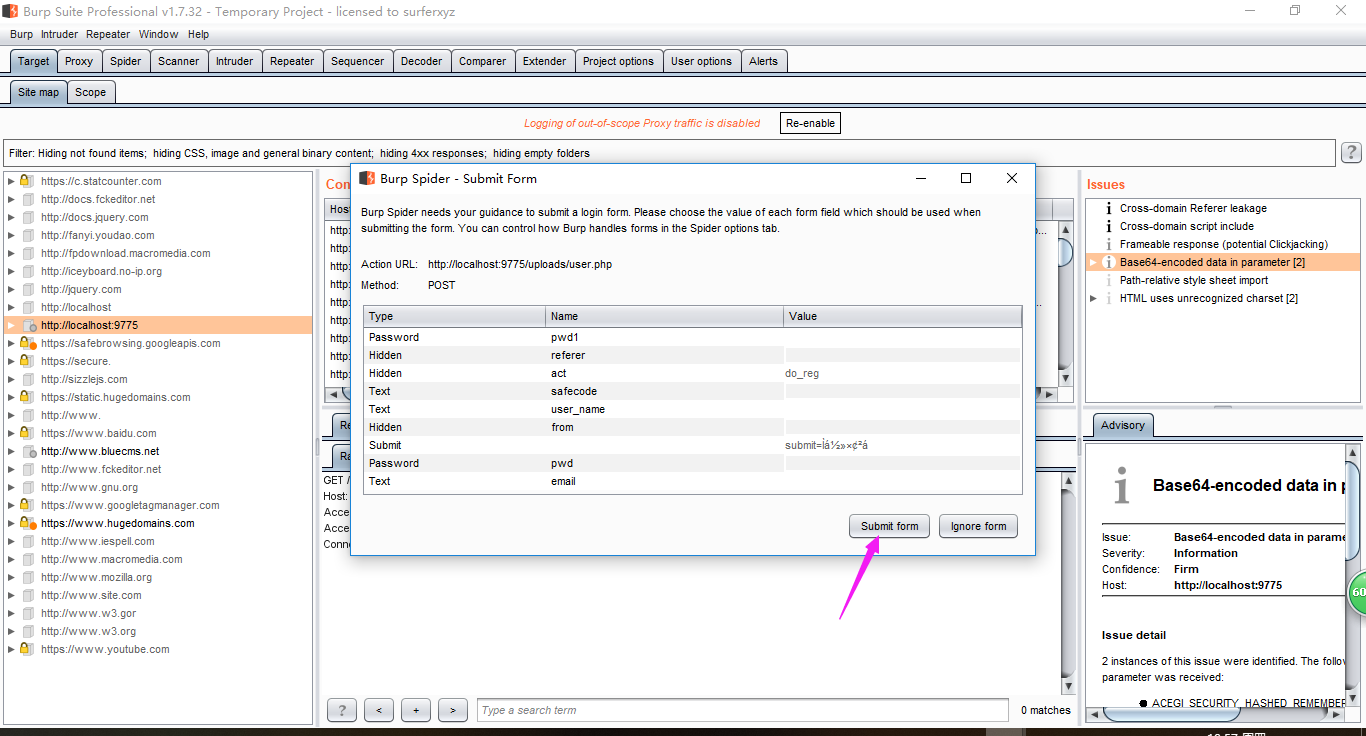
# 网站爬取- <http://localhost:9775/uploads/admin/index.php>

1. 工具 Burp Suite-Spider
2. 网站 <http://localhost:9775/uploads/admin/index.php>
3. 过程

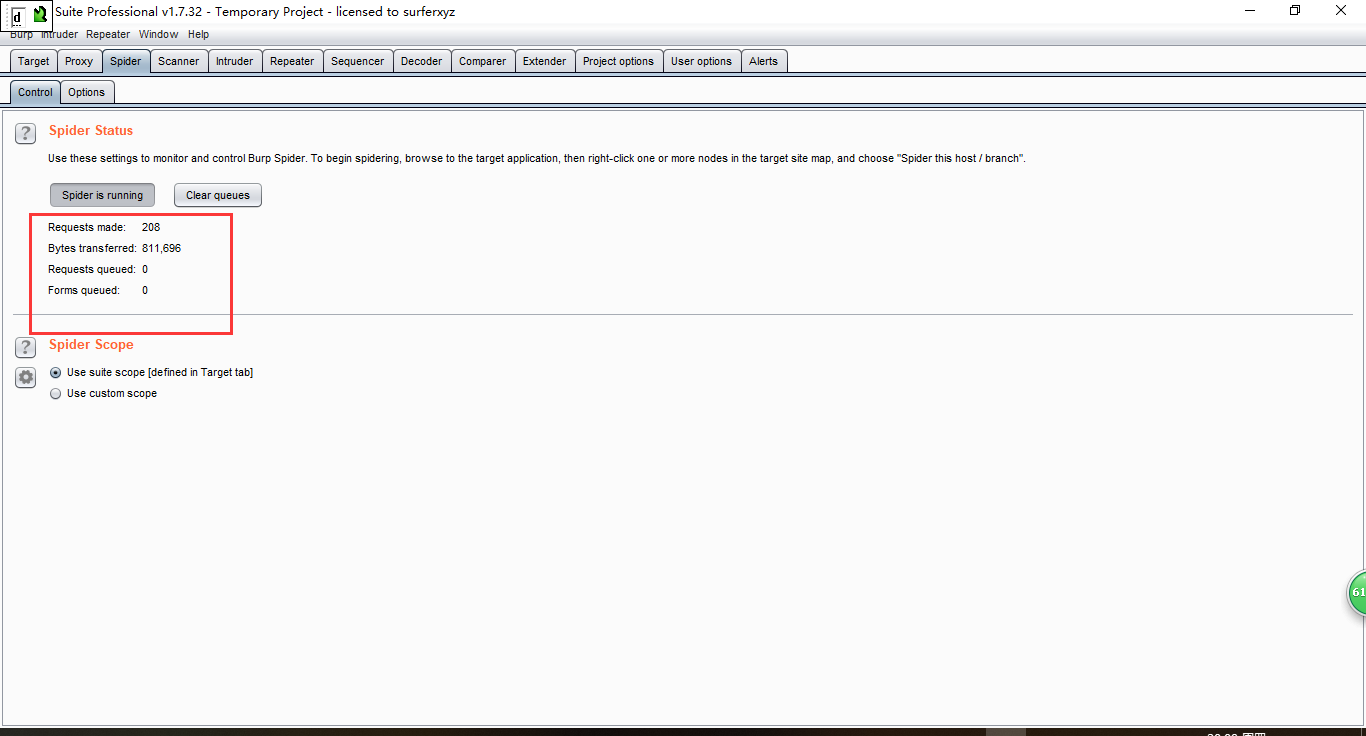
* 正常启动Burp Suite,完成代理设置
* 在浏览器发起一个正常成功的请求,我这里需要刷新,因为我提前打开过一次网站了
* 关闭拦截请求
* 在Target下面的Site map找到目的请求地址,右键点击Spider this host





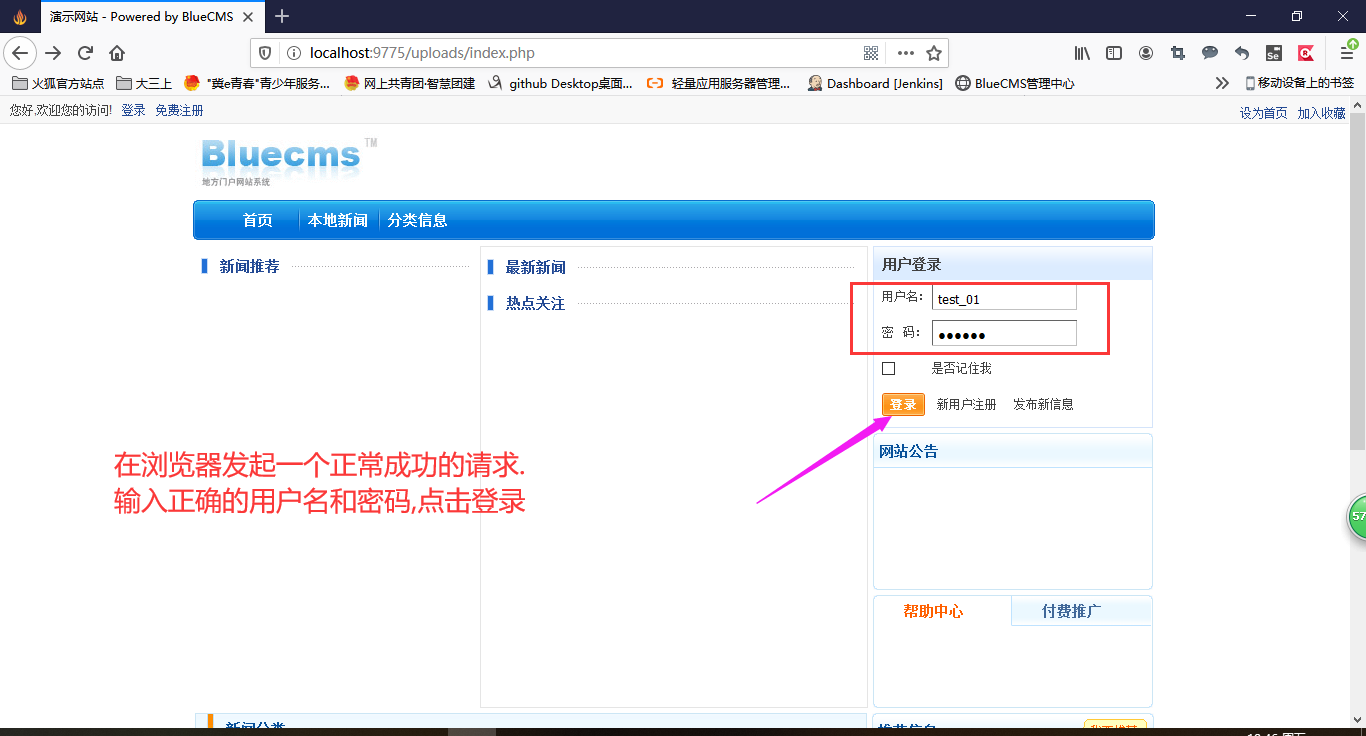
* 爬取数据



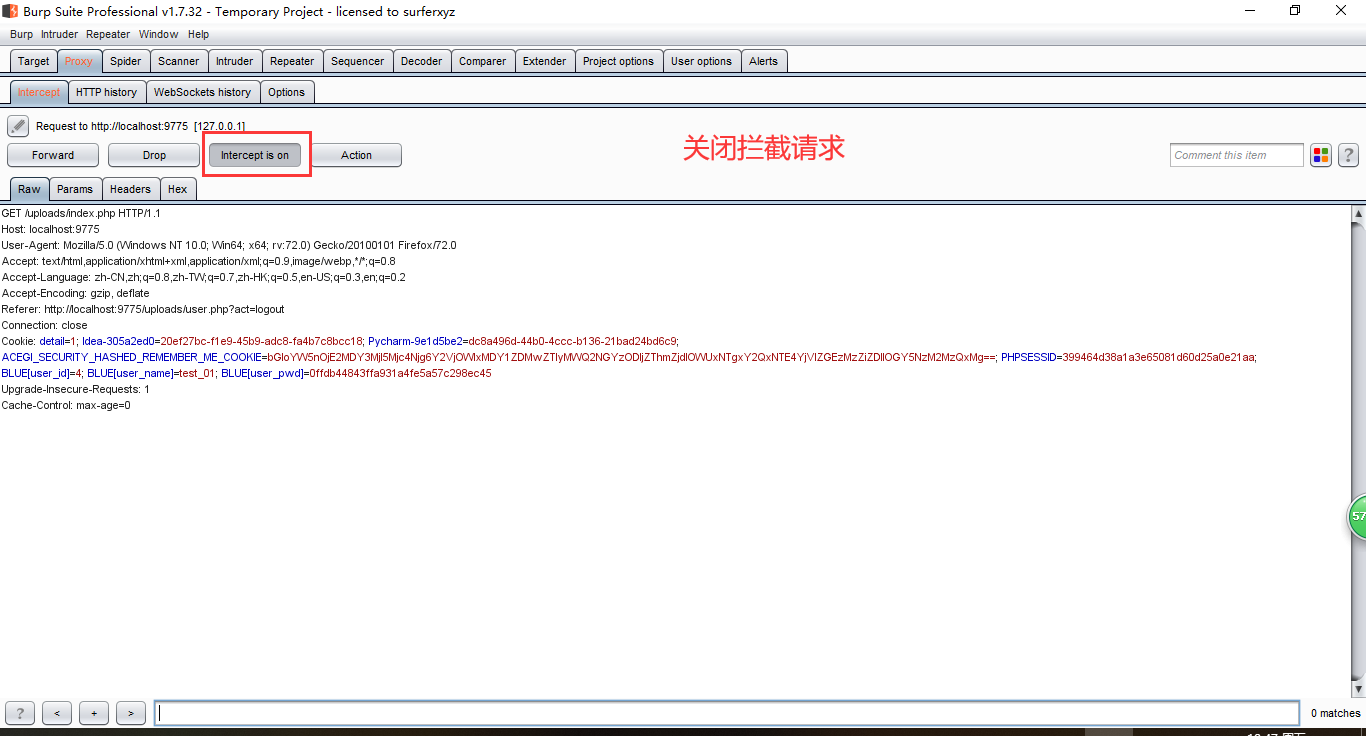
# 自动化攻击- http://localhost:9775/uploads/index.php

1. 工具 Burp Suite-Intruder
2. 网站 http://localhost:9775/uploads/index.php
3. 过程

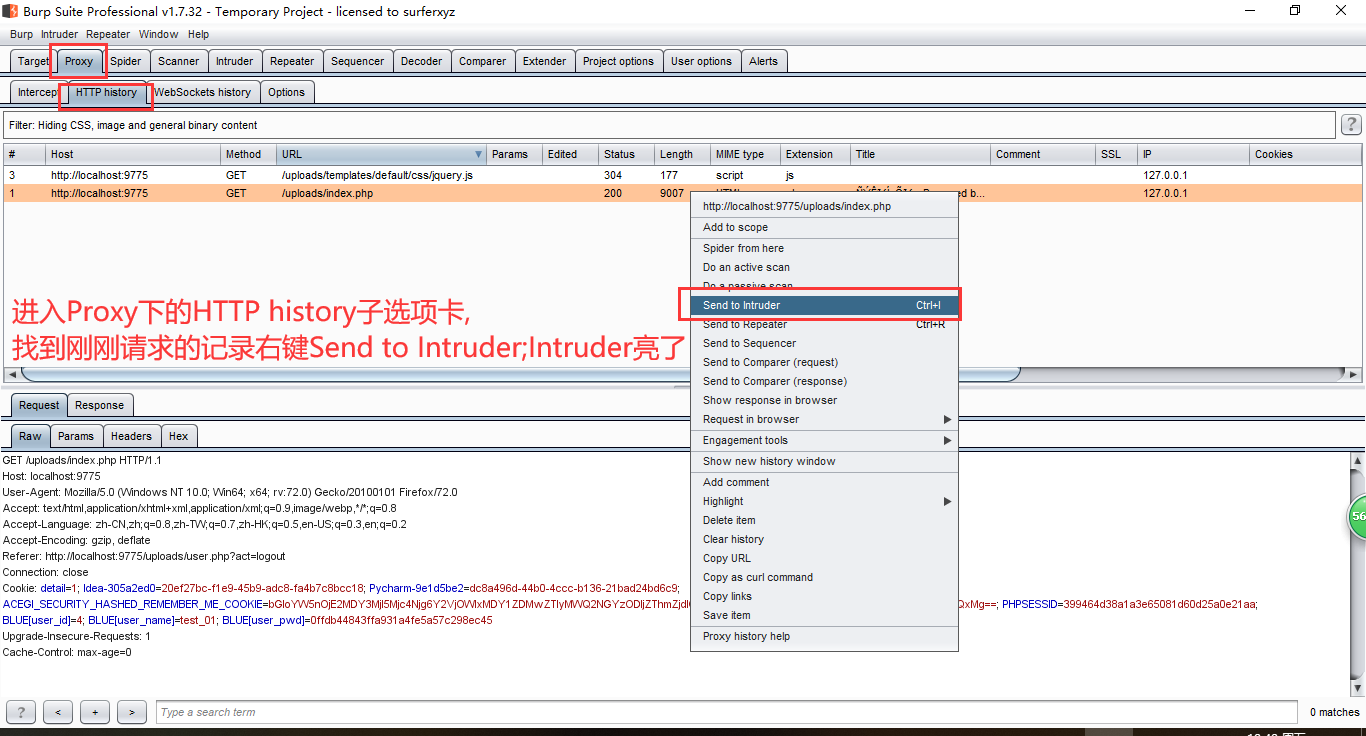
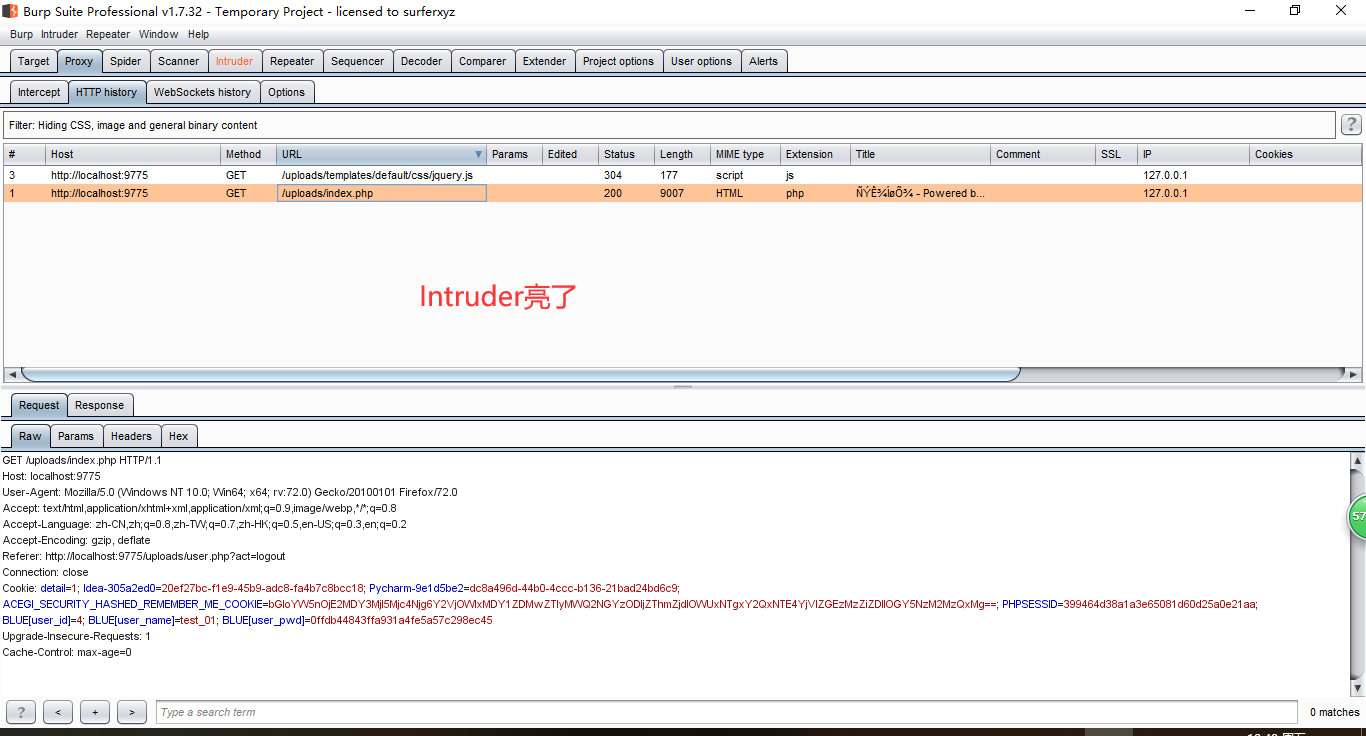
* 正常启动Burp Suite,完成代理设置
* 在浏览器发起一个正常成功的请求.输入正确的用户名和密码,点击登录;



* 关闭拦截请求

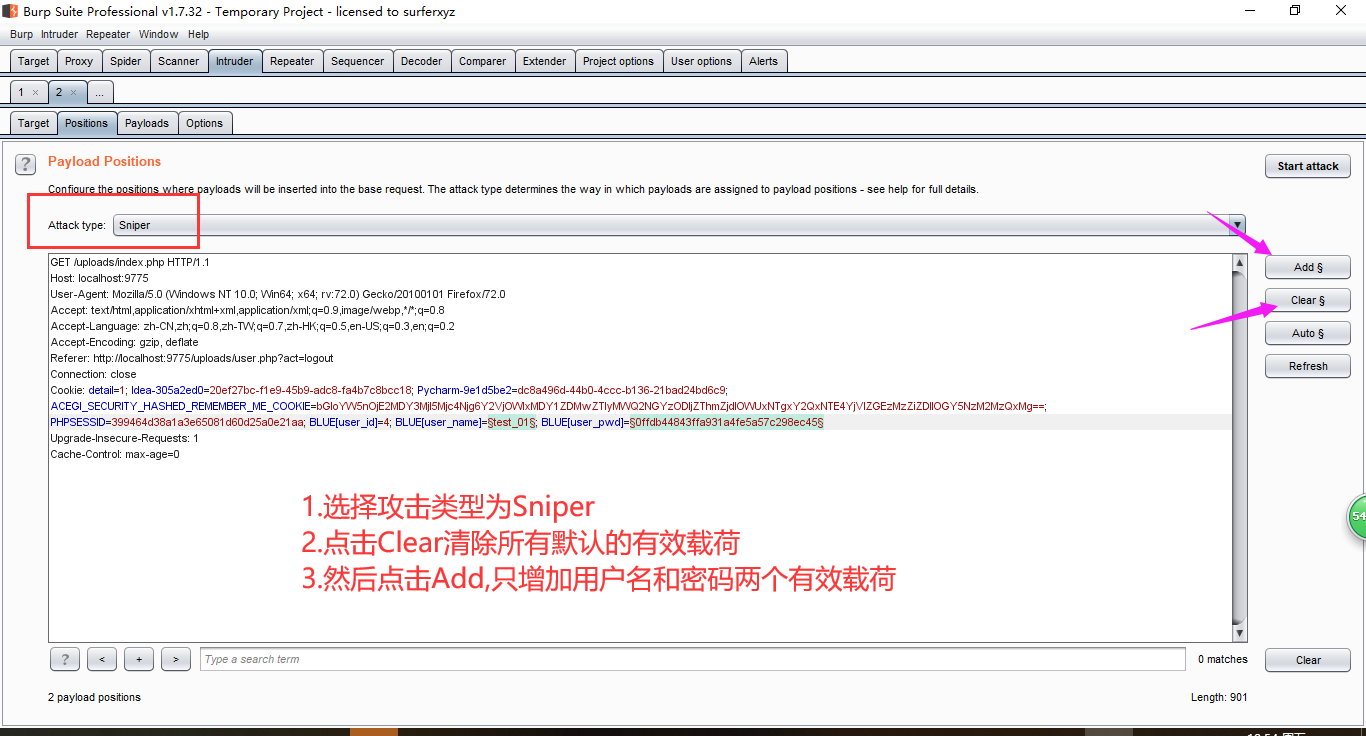


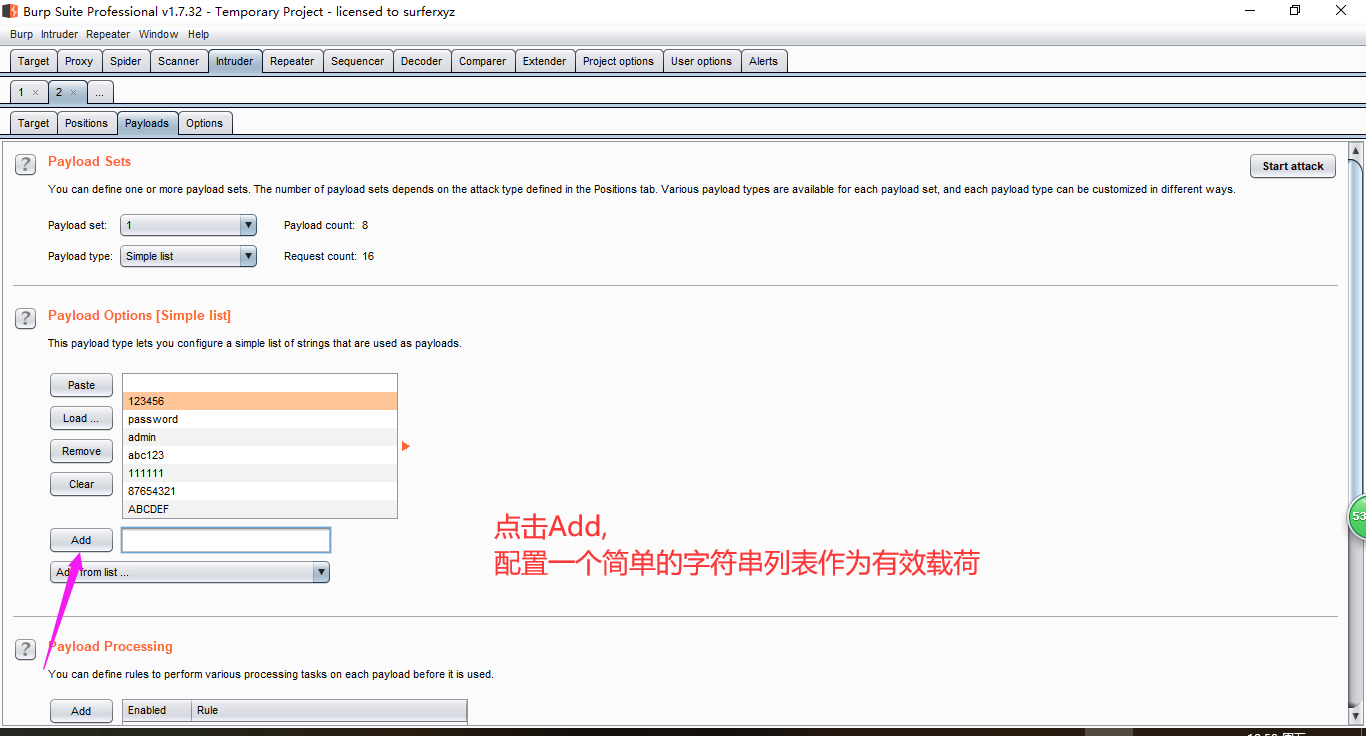
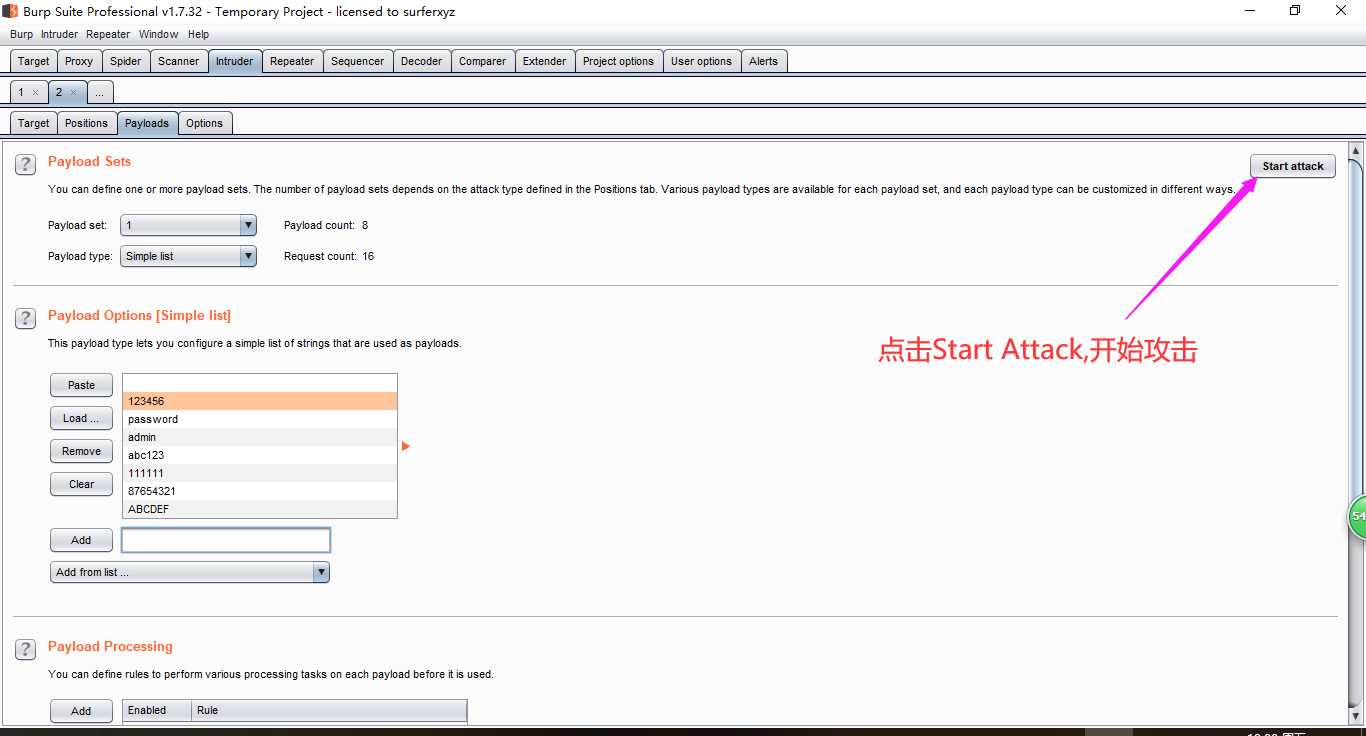
* 进入Proxy下的HTTP history子选项卡,找到刚刚请求的记录右键Send to Intruder;Intruder亮了

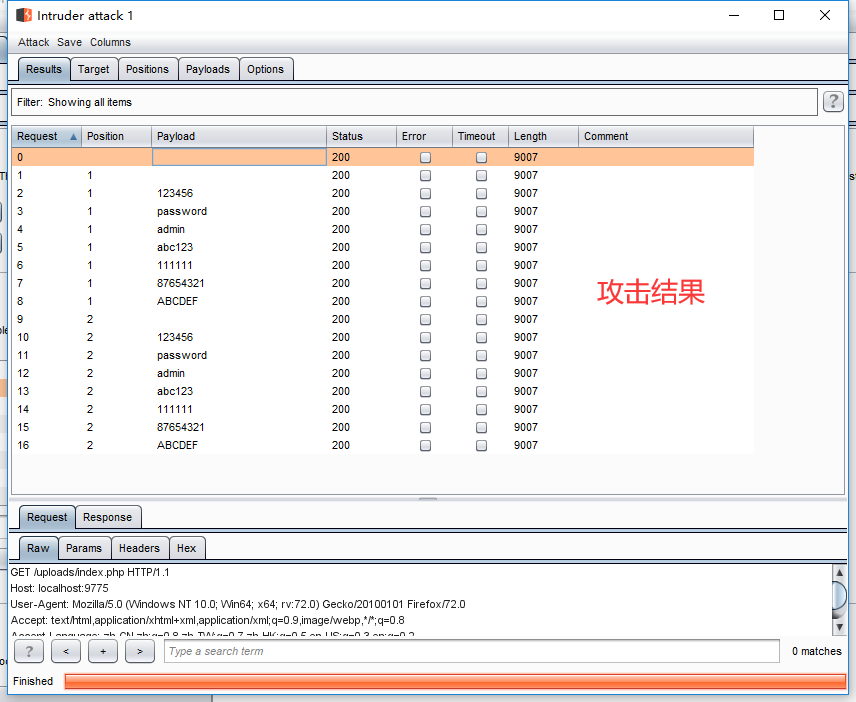
* 点击进入Intruder,

设置Target,Positions,Payloads,Options(Target和Options可以默认,不设置)



* 攻击结果



# 自动化攻击-<http://localhost:9775/uploads/admin/login.php?act=login>

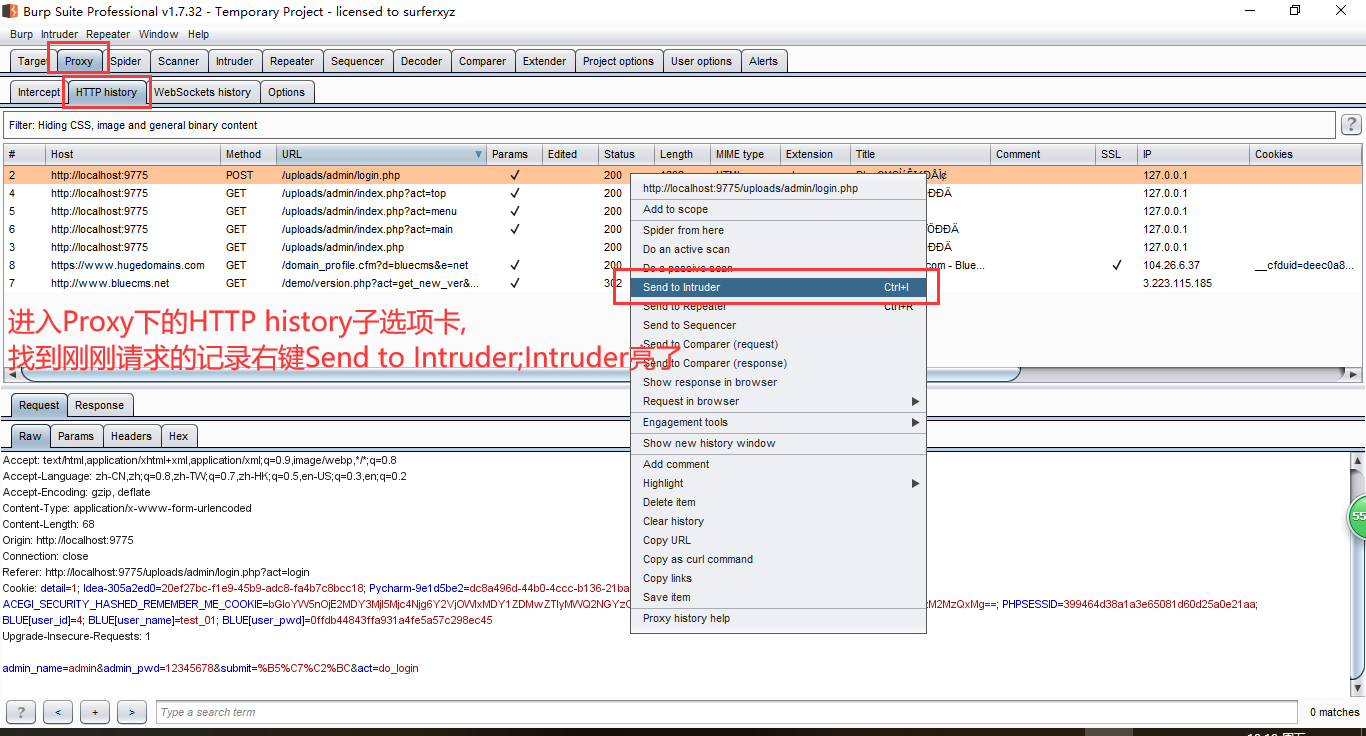
1. 工具 Burp Suite-Intruder
2. 网站 <http://localhost:9775/uploads/admin/login.php?act=login>
3. 过程
   * 正常启动Burp Suite,完成代理设置
   * 在浏览器发起一个正常成功的请求.输入正确的用户名和密码,点击登录;

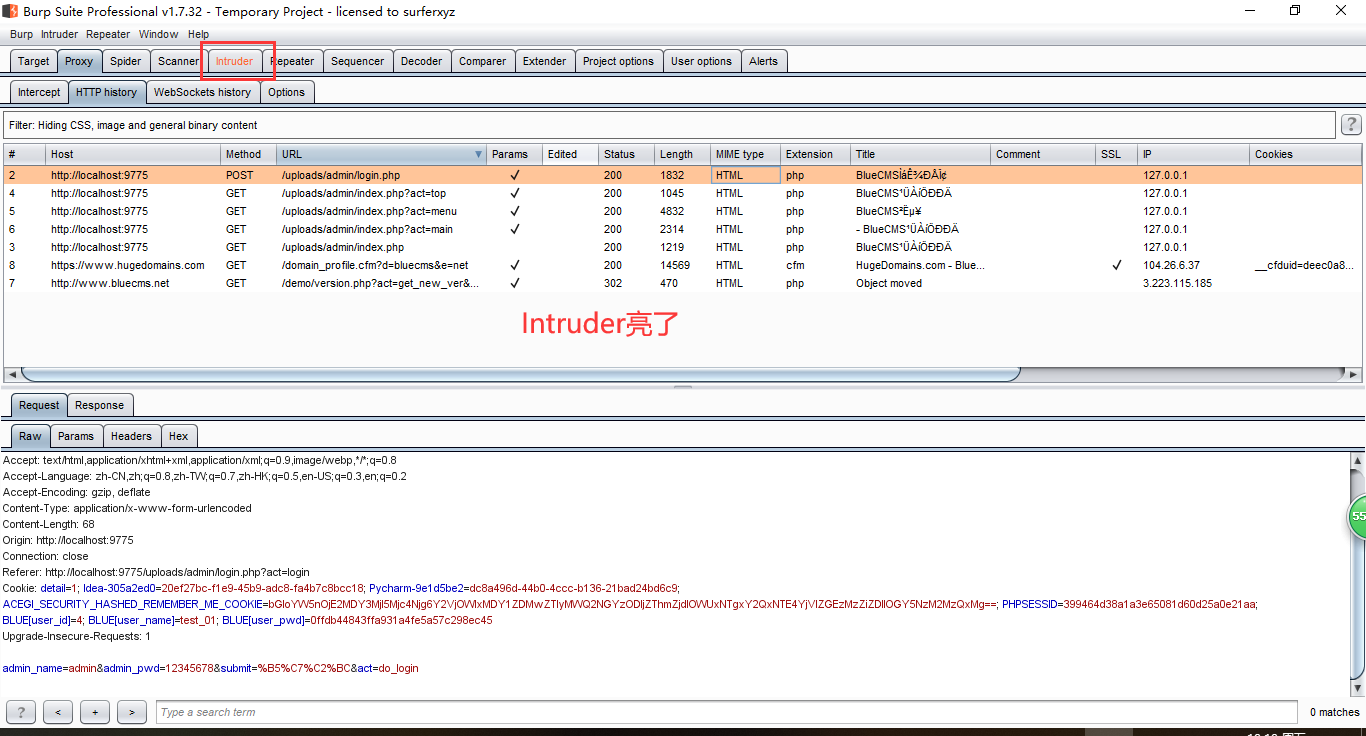


* + 关闭拦截请求



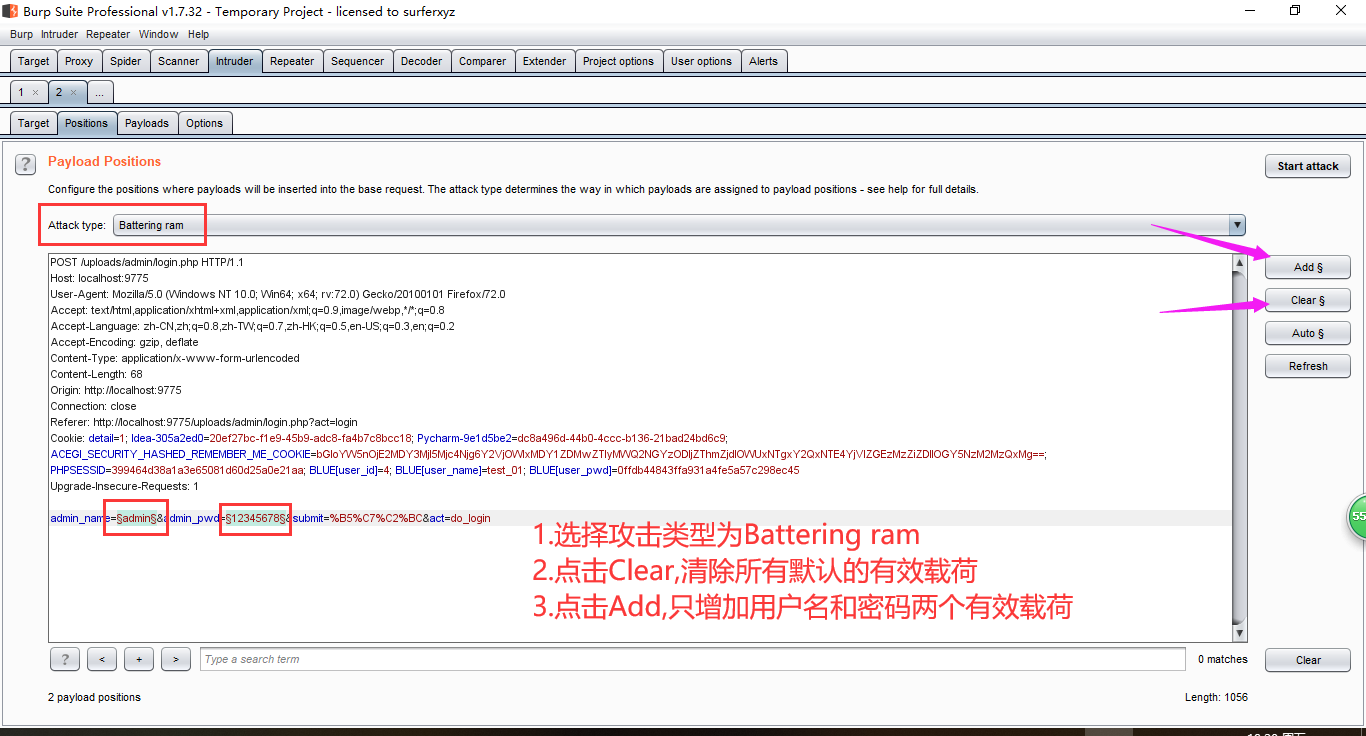
* + 进入Proxy下的HTTP history子选项卡,找到刚刚请求的记录右键Send to Intruder;Intruder亮了

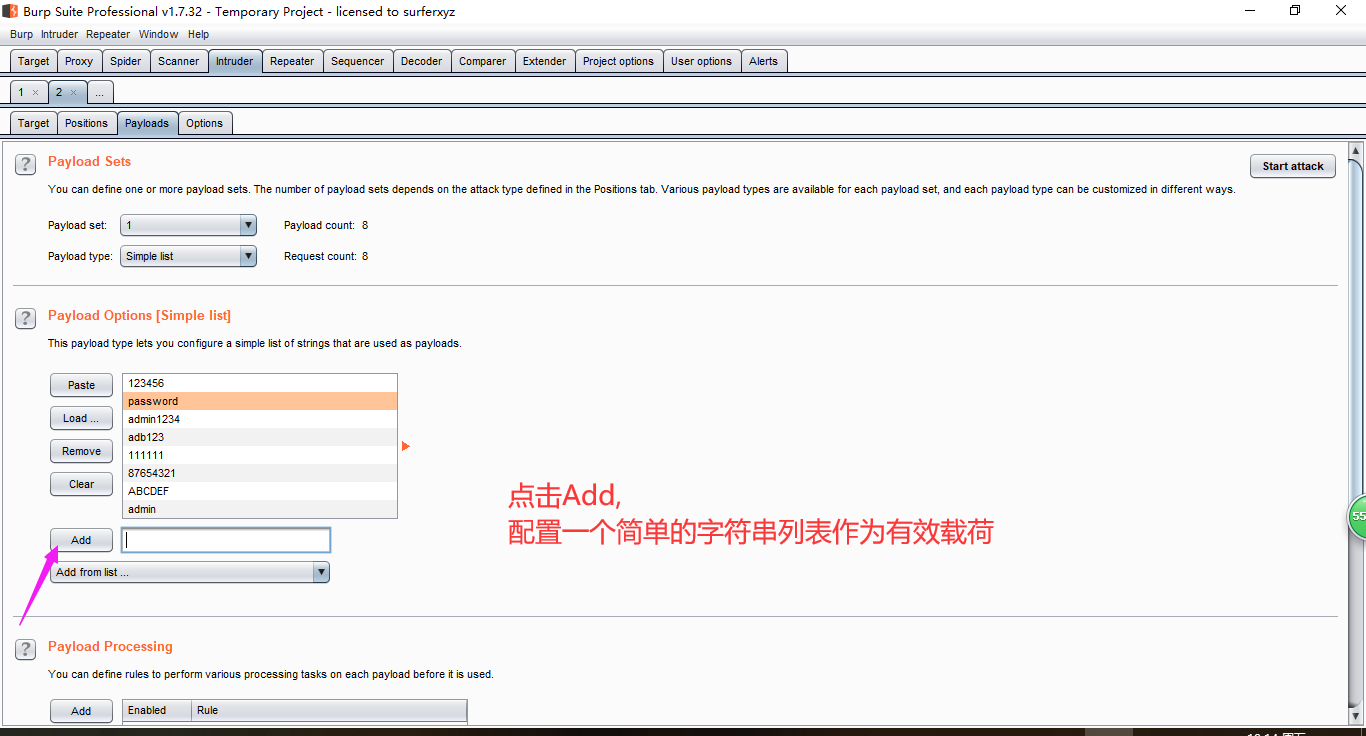
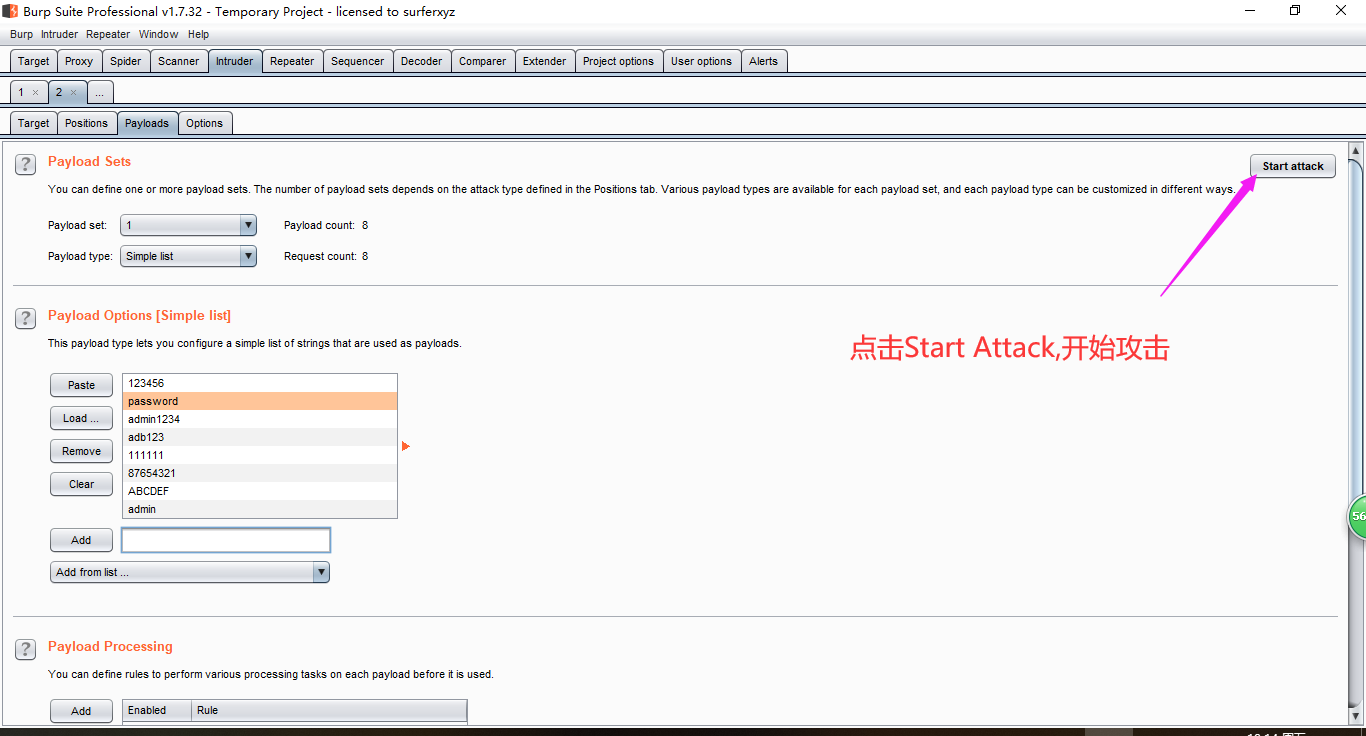




* 点击进入Intruder,

设置Target,Positions,Payloads,Options(Target和Options可以默认,不设置)



* 攻击结果

