# 用Burpsuite破解网站密码

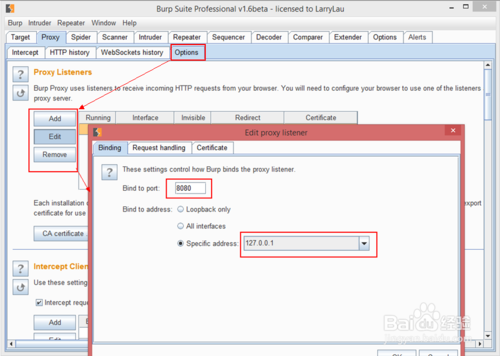
工具/原料

* burpsuite专业版
* 一个网站

方法/步骤

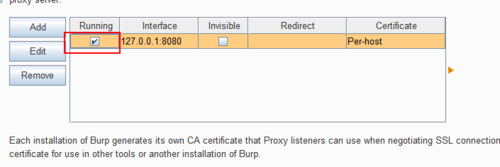
1. 1

切换至proxy选项卡的Option选项下，设置代理地址和端口：127.0.0.1:8080。

[](http://jingyan.baidu.com/album/200957619c8739cb0721b4ff.html?picindex=1)

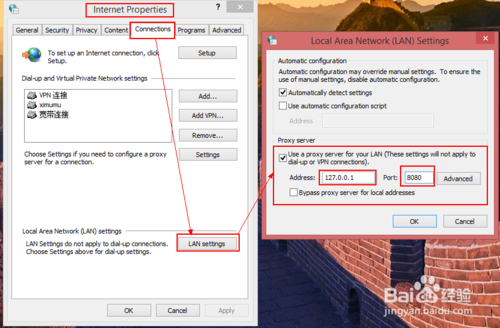
1. 2

启动刚刚设置的代理

[](http://jingyan.baidu.com/album/200957619c8739cb0721b4ff.html?picindex=2)

1. 3

打开Internet Properties，依次选择：Connections ->LAN Settings ->Proxy Server.分别输入127.0.0.1和8080。如图所示。

[](http://jingyan.baidu.com/album/200957619c8739cb0721b4ff.html?picindex=3)

1. 4

找一个目标网址为

[](http://jingyan.baidu.com/album/200957619c8739cb0721b4ff.html?picindex=4)

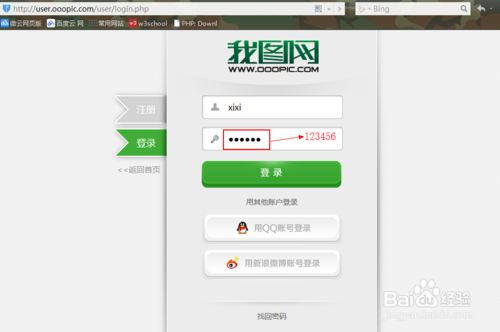
1. 5

点击“登录”时，出现的是一个弹出窗口，为了找到真正的登录网址，我们点击“免费注册”。

[](http://jingyan.baidu.com/album/200957619c8739cb0721b4ff.html?picindex=5)

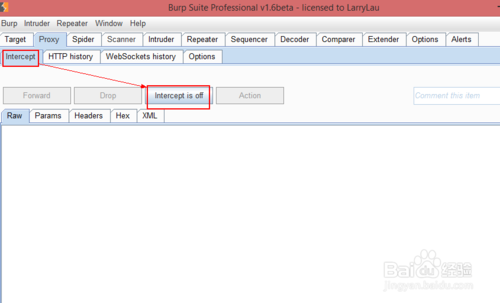
1. 6

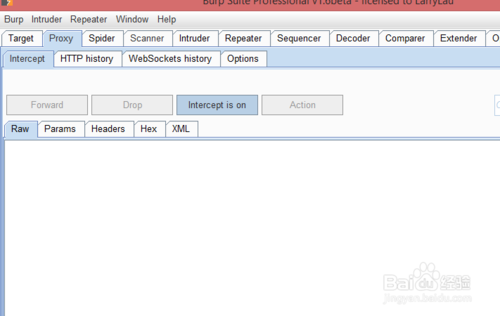
点击旁边的“登录”，随便输入一个账号，密码输入“123456”。（先不点击登录按钮）

[](http://jingyan.baidu.com/album/200957619c8739cb0721b4ff.html?picindex=6)

1. 7

选择Proxy选项卡下的“Intercept”选项，点击“Intercept is off”按钮，按钮会变成“Intercept is on”

[](http://jingyan.baidu.com/album/200957619c8739cb0721b4ff.html?picindex=7)

[](http://jingyan.baidu.com/album/200957619c8739cb0721b4ff.html?picindex=8)

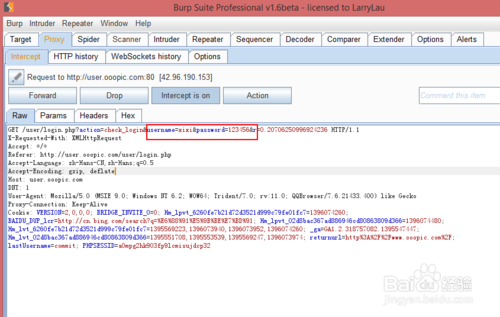
1. 8

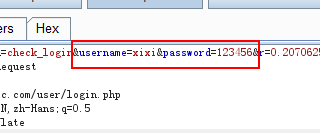
打开前面的登陆页面，点击“登录”按钮。

[](http://jingyan.baidu.com/album/200957619c8739cb0721b4ff.html?picindex=9)

1. 9

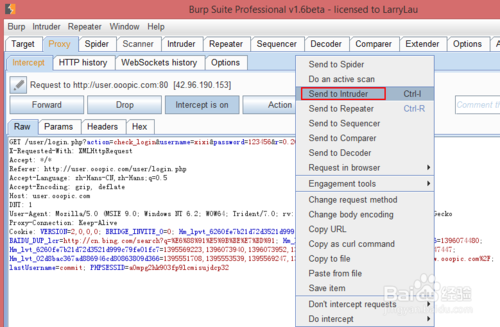
此时我们会在Burpsuite下看见刚刚截取到的数据包。可以看到我们刚刚输入的用户名和关键字。

[](http://jingyan.baidu.com/album/200957619c8739cb0721b4ff.html?picindex=10)

[](http://jingyan.baidu.com/album/200957619c8739cb0721b4ff.html?picindex=11)

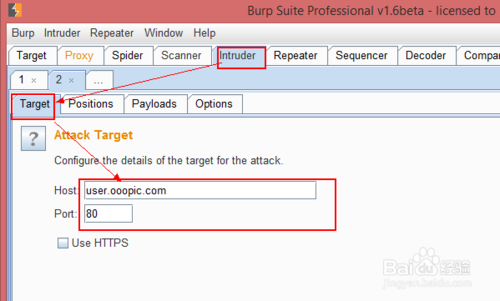
1. 10

在文字区域内单击右键，选择“Send to Intrder”

[](http://jingyan.baidu.com/album/200957619c8739cb0721b4ff.html?picindex=12)

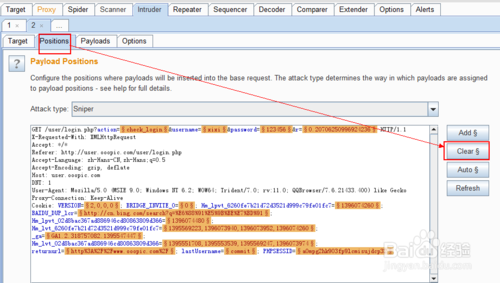
1. 11

切换到Intruder选项卡下，选择“Target”，设置主机地址以及端口号，端口号默认是80，假如网站使用的是HTTPS协议的话就勾选下方的“Use HTTPS”切换到443端口（SSL）

[](http://jingyan.baidu.com/album/200957619c8739cb0721b4ff.html?picindex=13)

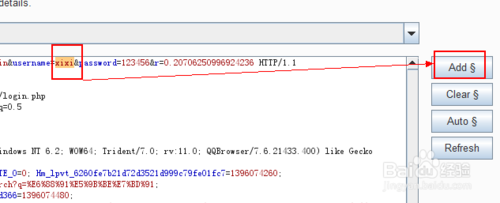
1. 12

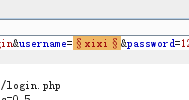
切换到Positions选项，点击右边的“Clear $”按钮，清除所有默认参数。

[](http://jingyan.baidu.com/album/200957619c8739cb0721b4ff.html?picindex=14)

1. 13

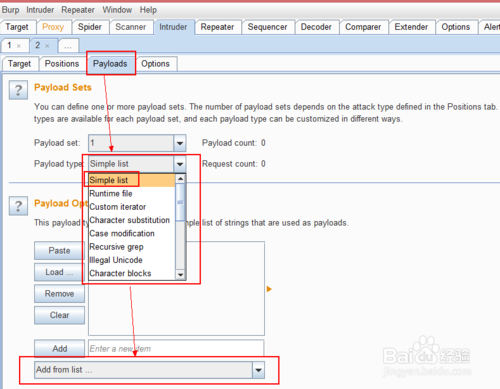
鼠标选中username后边的文字（我们输入的用户名），点击“Add $”按钮。

[](http://jingyan.baidu.com/album/200957619c8739cb0721b4ff.html?picindex=15)

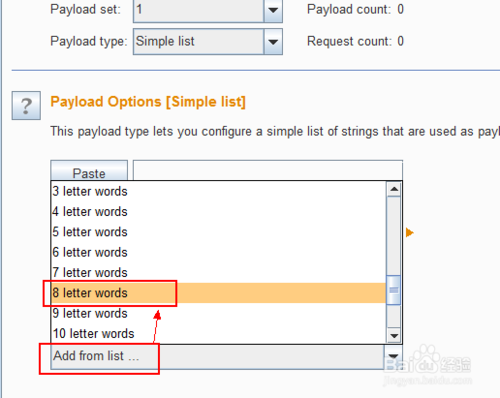
[](http://jingyan.baidu.com/album/200957619c8739cb0721b4ff.html?picindex=16)

1. 14

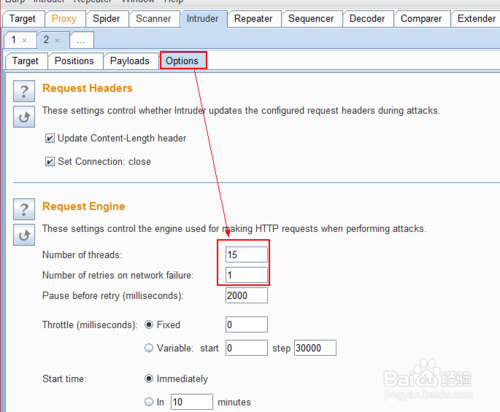
切换到“Payloads”选项，选择要使用的“Payload type”，这里我们选择“Simple list”。

[](http://jingyan.baidu.com/album/200957619c8739cb0721b4ff.html?picindex=17)

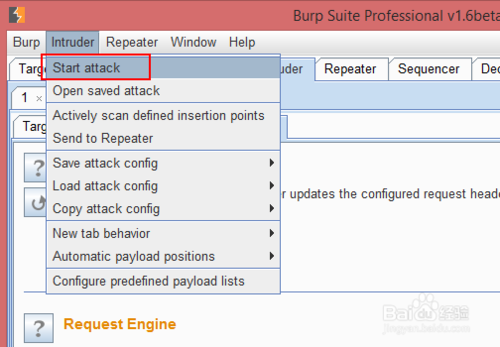
1. 在下方的“Add from list”中选择一种密码，这里我们选择“8 letter words”。

[](http://jingyan.baidu.com/album/200957619c8739cb0721b4ff.html?picindex=18)

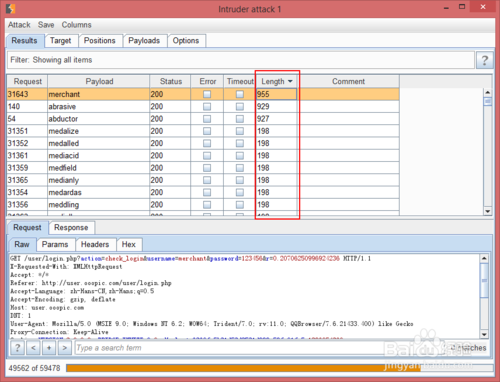
1. 切换到“Options”选项卡下，设置线程数和其他参数，如下图所示。

[](http://jingyan.baidu.com/album/200957619c8739cb0721b4ff.html?picindex=19)

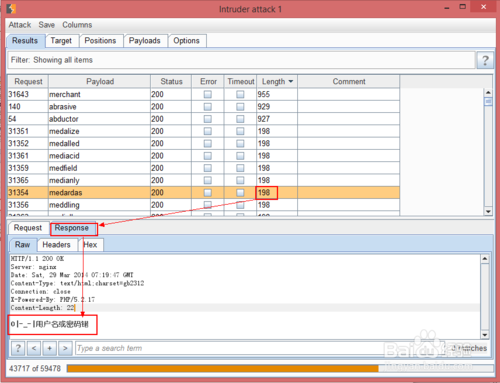
1. 点击菜单栏的“Intruder”，选择“Start attack”

[](http://jingyan.baidu.com/album/200957619c8739cb0721b4ff.html?picindex=20)

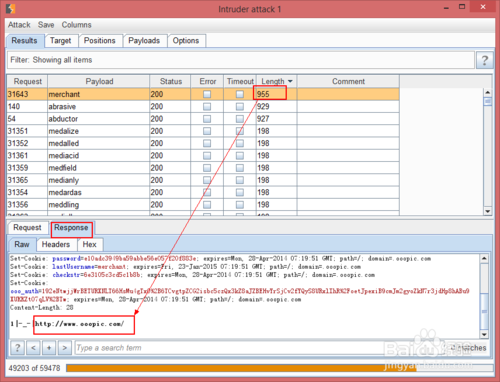
1. 扫描到差不多的时候，我们按Length（长度）大小排序。这是我们会看到几种不同的数据包，许多一样的，还有几个数据包很大的基本就是正确的了。

[](http://jingyan.baidu.com/album/200957619c8739cb0721b4ff.html?picindex=21)

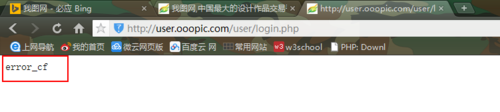
1. 选择其中一个较小的数据包，点击下方的“Response”，会看见有提示“用户名或密码错”

[](http://jingyan.baidu.com/album/200957619c8739cb0721b4ff.html?picindex=22)

1. 同理，我们再选择一个较大的数据包，这是，我们会看见下方并没有提示“用户名或密码错误”，

[](http://jingyan.baidu.com/album/200957619c8739cb0721b4ff.html?picindex=23)

1. 当我再重新打开登录页面时发现已经进不去了

[](http://jingyan.baidu.com/album/200957619c8739cb0721b4ff.html?picindex=24)

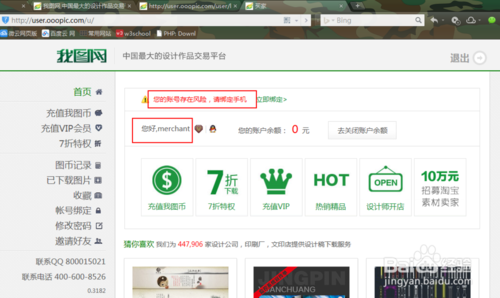
1. 初步猜测应该是IP被网站封了，所以我们换一个IP登录试试。我用手机流量开热点链接电脑，这时再去打开网页时果然显示出来了。

[](http://jingyan.baidu.com/album/200957619c8739cb0721b4ff.html?picindex=25)

1. 输入我们刚刚获得的用户名（这里以merchant为例）以及密码123456。然后点击登录。

[](http://jingyan.baidu.com/album/200957619c8739cb0721b4ff.html?picindex=26)

1. 成功登录

[](http://jingyan.baidu.com/album/200957619c8739cb0721b4ff.html?picindex=27)

END

注意事项

* .网络安全确实是个很大的问题，所以我们在上网时尽量不要泄露太多个人的信息。
* 3.在网站注册账号时密码不要设置得太简单。因为一些网站对于暴力破解并没有进行特别的防御。