Web密码爆破实验

原创

烟雨天青色 于 2019-07-19 20:30:55 发布 5331 收藏 45
分类专栏： CTF 文章标签： 密码爆破 CTF

本文链接：https://blog.csdn.net/qq_38603541/article/details/96494194

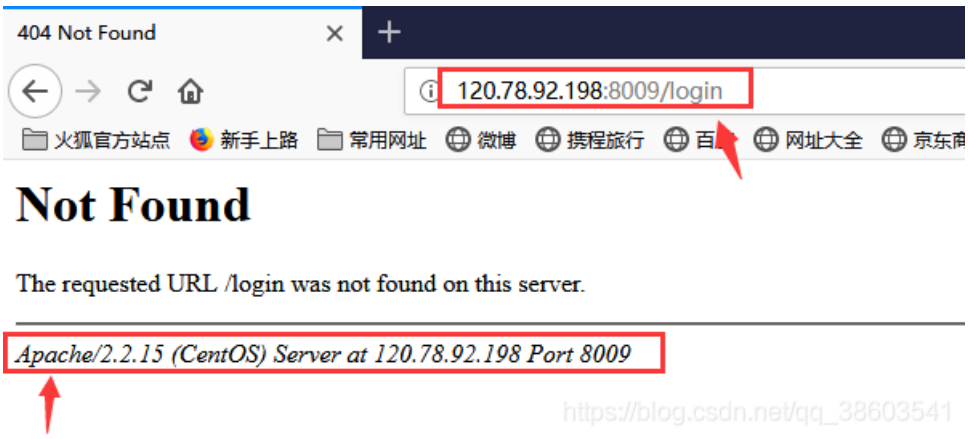
前言：由于爆破其他正常网站密码属于违法行为，因此本次实验是使用自行搭建web环境进行密码爆破实验。

这个实验是今天老师给留的附加作业，虽然心很累，但这种实验确实挺好玩。

咱们看一下实验环境吧……

实验环境是老师自己搭建的，只给了我们一个IP地址和端口号，不过这就够用了，哈哈哈哈

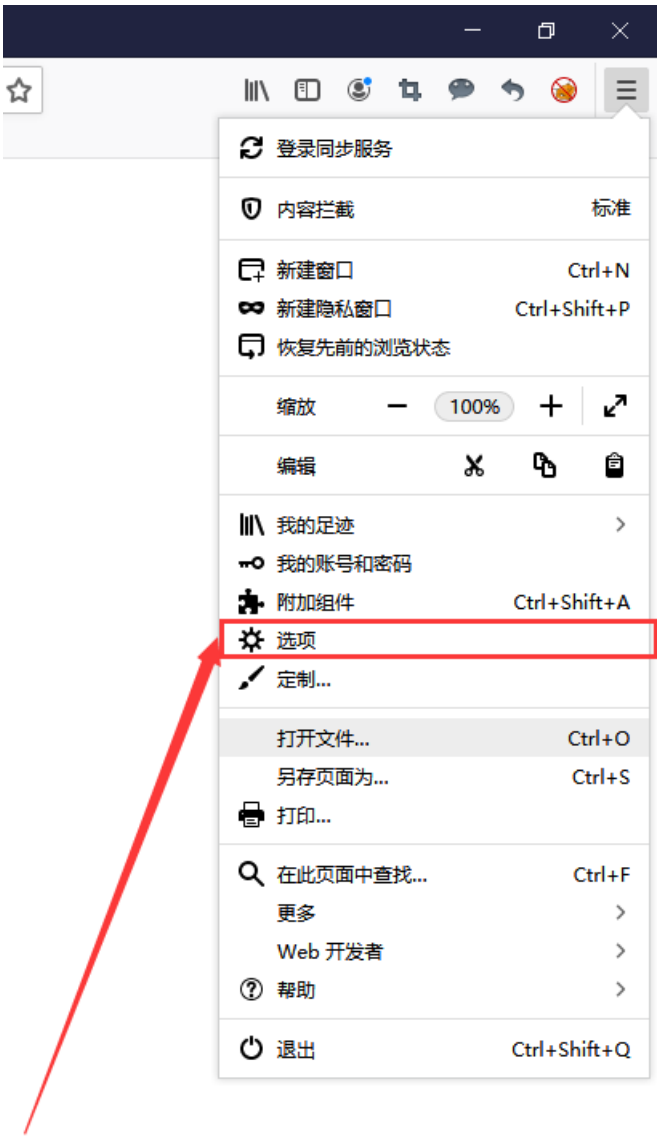
可是这个地址访问出来，提示：“Pelease find the login page ^_^”。嗯？？？什么鬼，登录页面还要自己找？？行吧行吧，这种网络后台找登录界面就单纯靠经验了……要找到登录页面就需要知道网站后台是使用什么语言写的，这个很重要，因为涉及到后缀名的，现在管它呢，随便输一个字符串看看，到底是个什么情况……

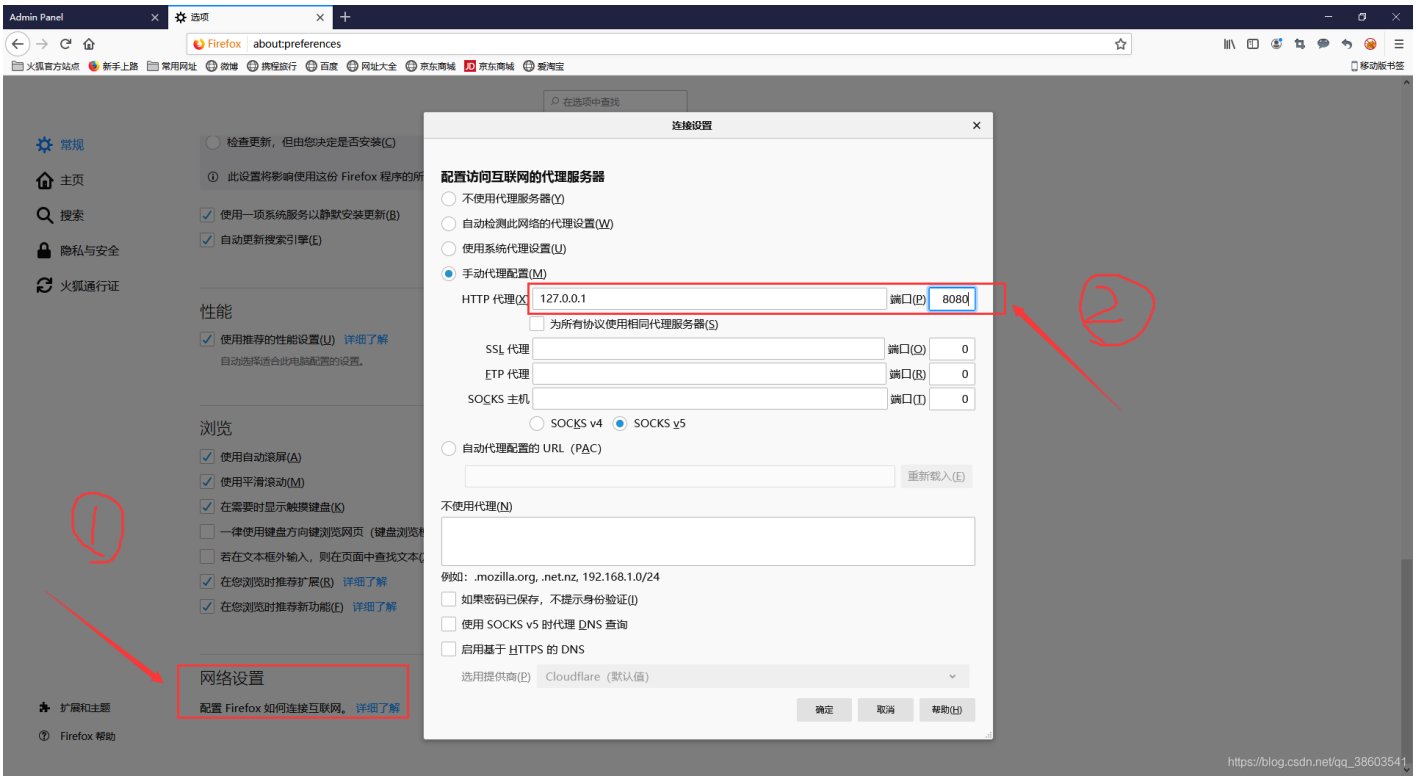


我先构造了一个login的字符串，回车之后，页面提示：Apache……巴拉巴拉的，看到Apache我们就知道，网站后台肯定是使用php写的，知道这个就好办了，我们在IP地址后面加上一个/login.php试试……不行！！昂？？想想网站后台还有啥常用的登录名：admin、manage……经过尝试，/manage.php可以访问到我们需要的登录页面。

一般遇到这样的情况，我下意识的回去查看一下网页源代码，可是……这个网页穷的什么都没有……那能咋办？上工具抓包呗……接下来，小杨开始了漫长的抓包过程……

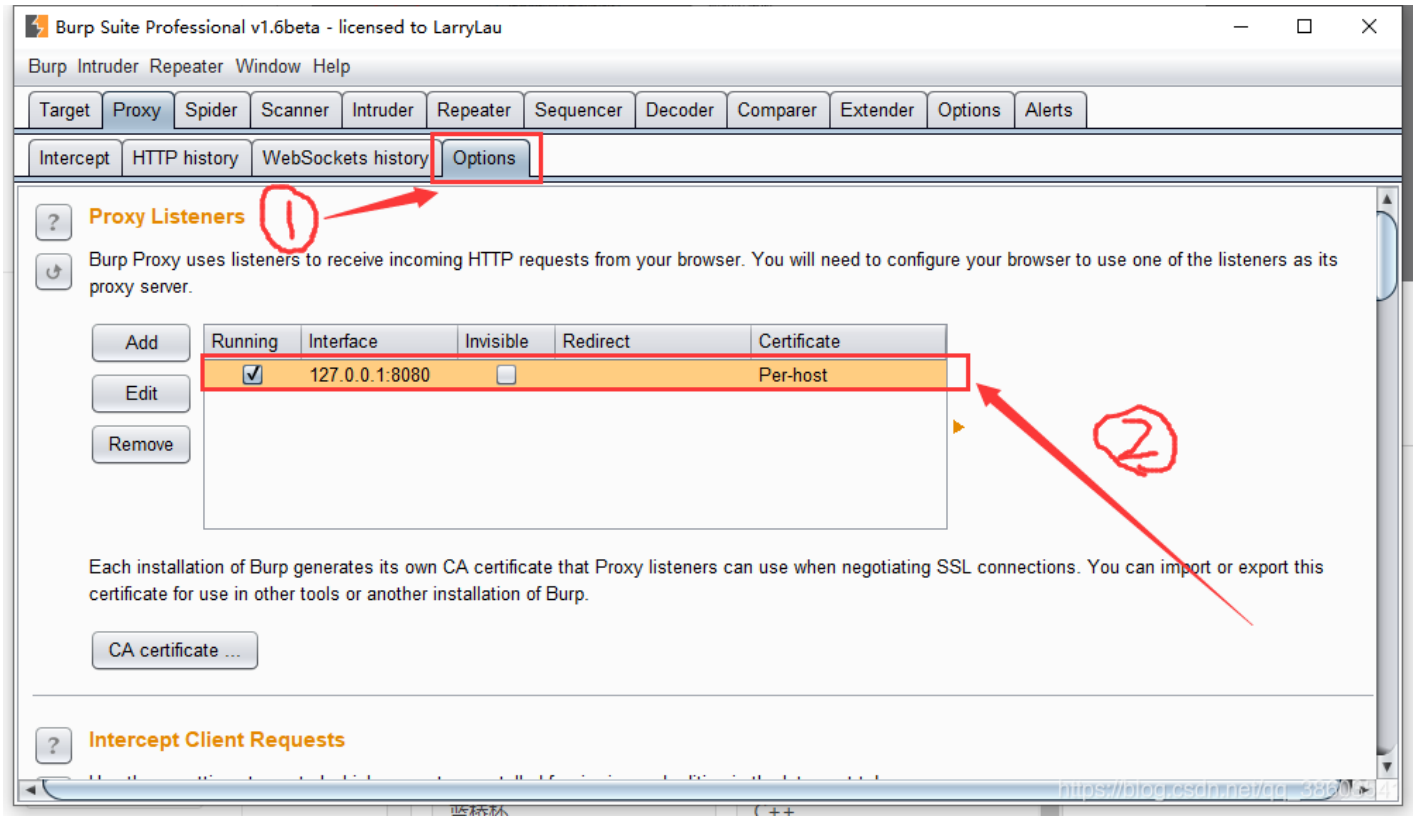
第一步，设置代理，这里推荐使用火狐浏览器，功能很强大滴。





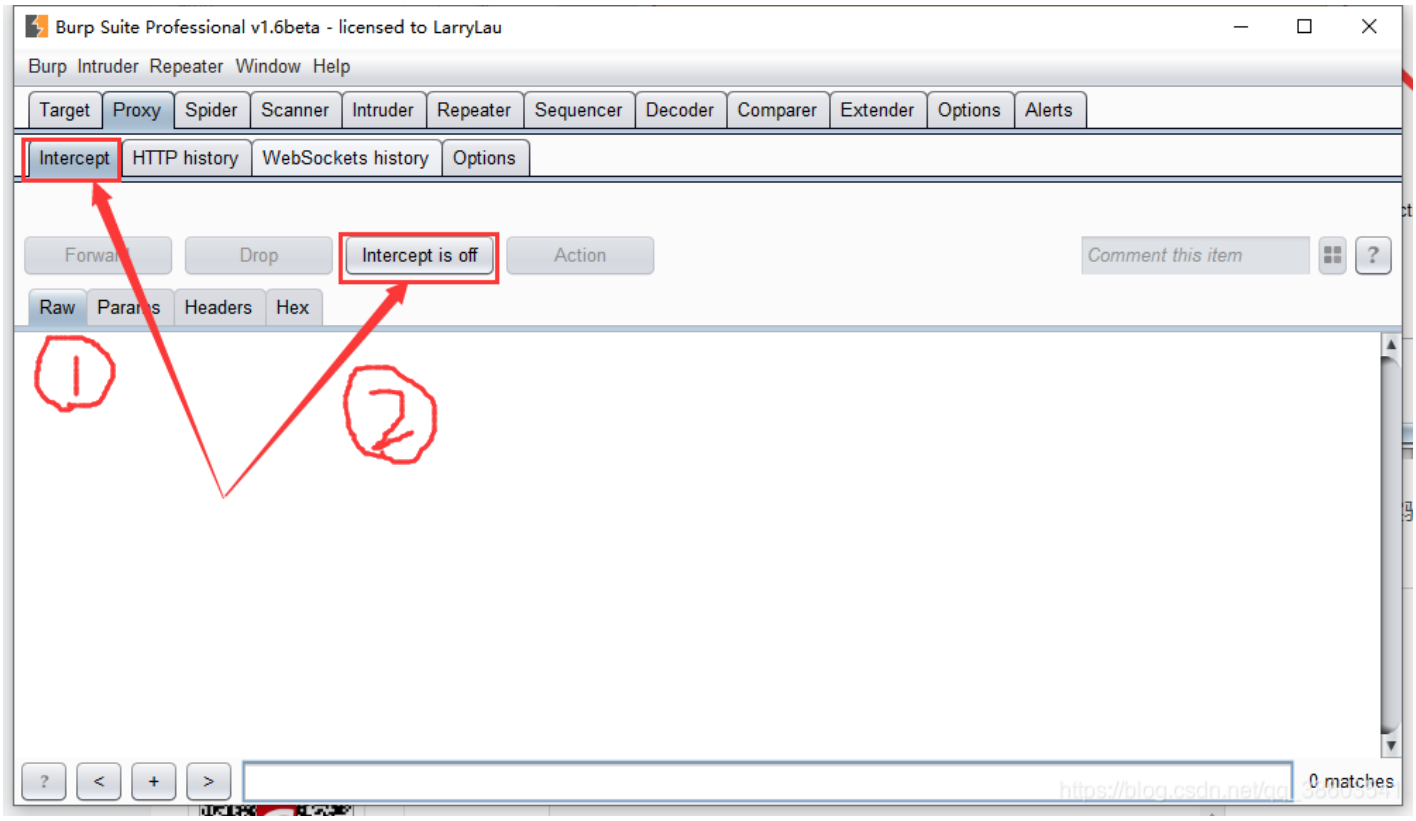
设置好代理之后，我们打开著名的爆破工具：burpsuite，设置一下，进行抓包实验。

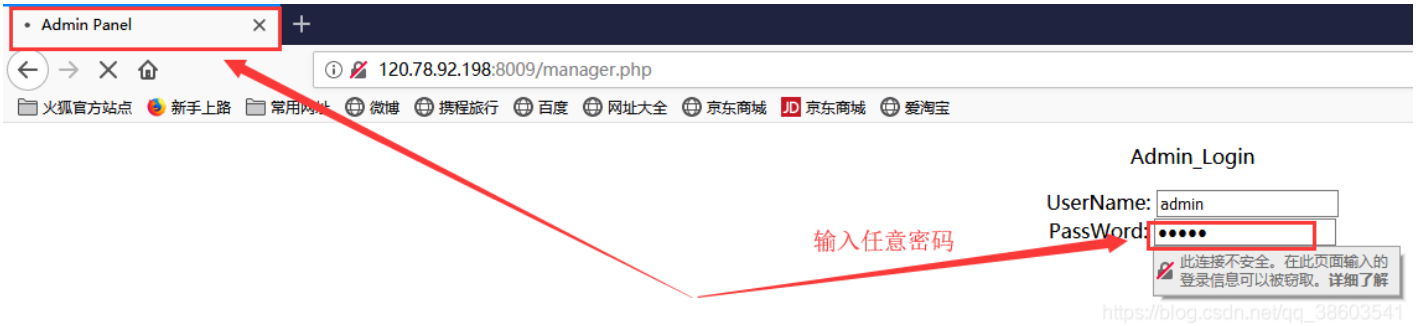
第二步，配置burpsuite。

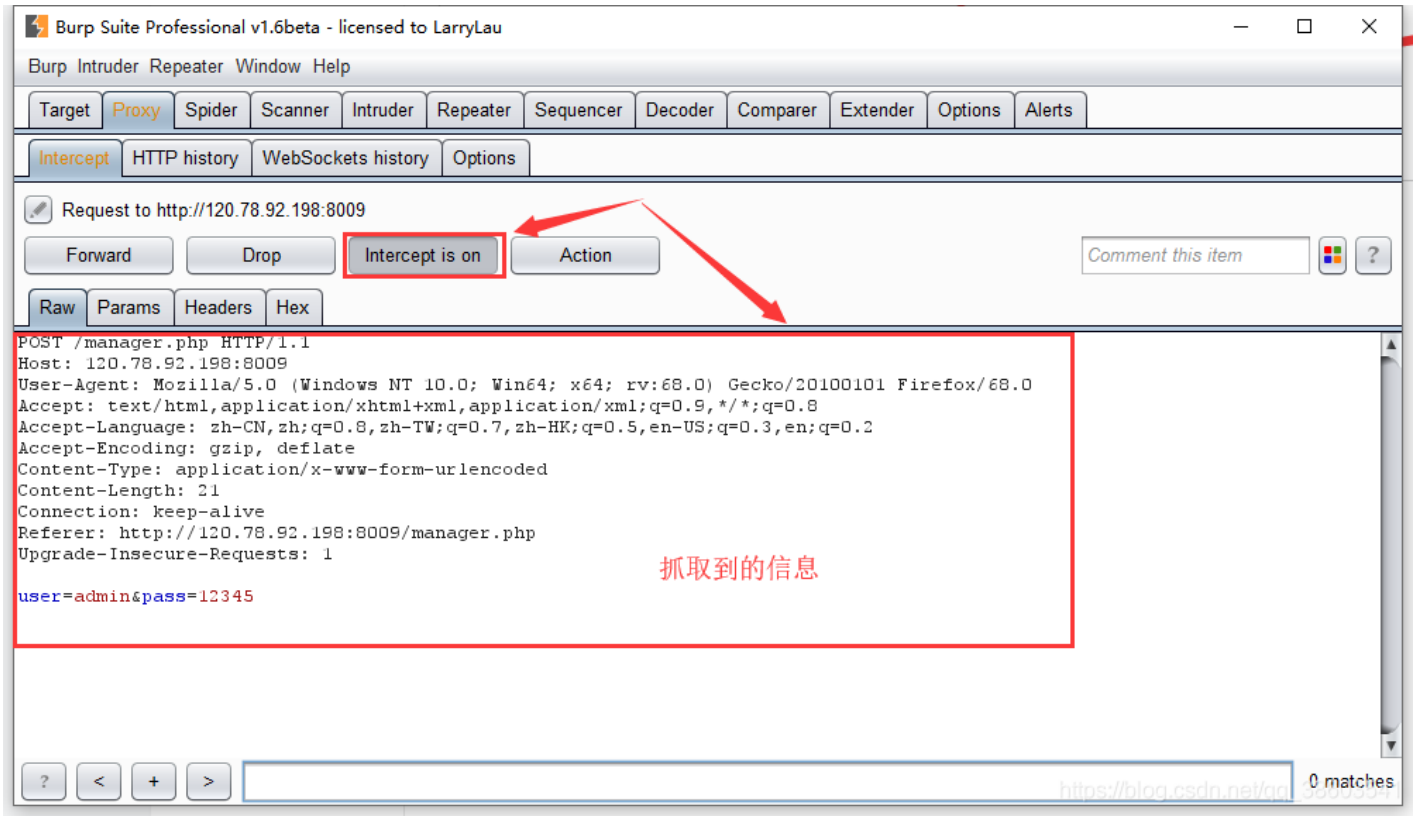


这里使用本地默认的IP和端口就行，127.0.0.1端口号8080，然后点击Intercept，进行下一步实验操作。

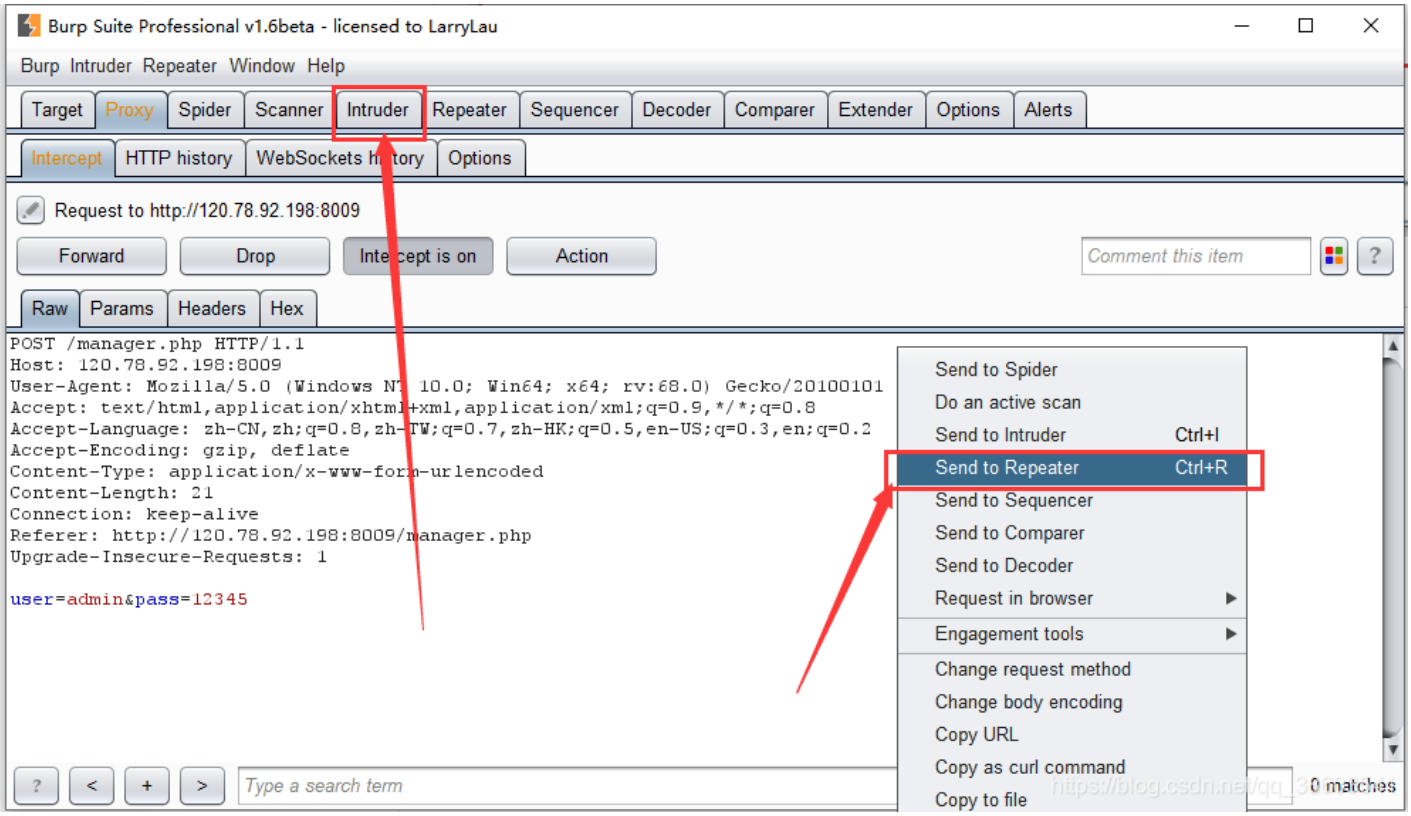
点击Intercept is off。点击之后这个按钮它会变成Intercept is on，然后回到我们的浏览器下，关掉刚刚我们配置的代理服务器，在密码输入框内输入任意字符串，回车。这个时候你会发现，浏览器的该页面有一个圈圈会不停的转呀转，没事啊，这说明正在抓包。现在，我们回到BurpSuite下，已经可以发现到我们已经将信息抓到了。


Burp Suite Professional v1.6beta - licensed to LarryLau
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
Drop
Intercept is off
Action
Comment this item
Raw Headers Hex
1
2
0 matches

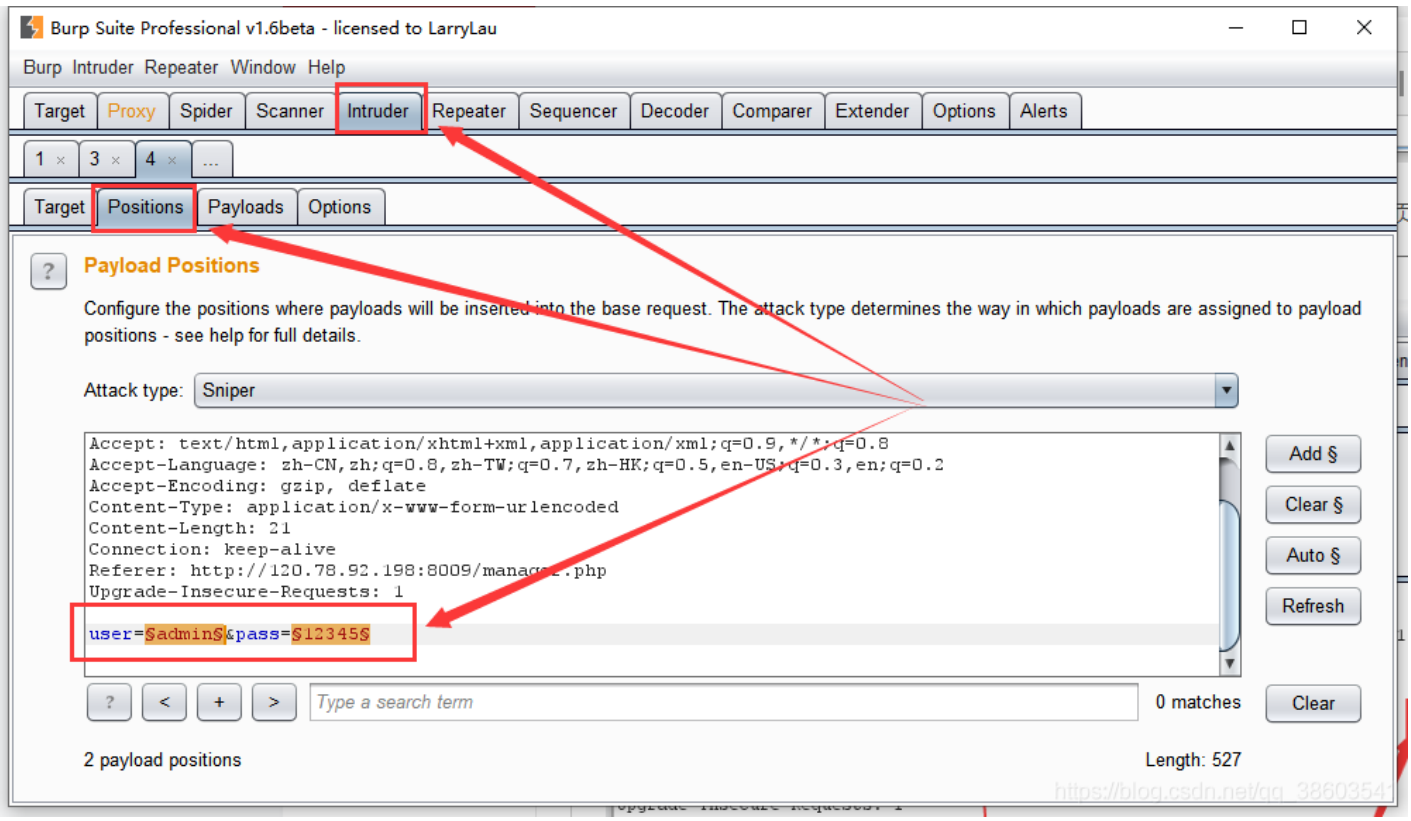

Admin Panel
120.78.92.198:8009/manager.php
Admin_Login
UserName: admin
PassWord:
输入任意密码
此连接不安全。在此页面输入的登录信息可以被窃取。详细了解


Burp Suite Professional v1.6beta - licensed to LarryLau
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
Request to http://120.78.92.198:8009
Forward
Drop
Intercept is on
Action
Comment this item
Raw Params Headers Hex
POST /manager.php HTTP/1.1
Host: 120.78.92.198:8009
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 21
Connection: keep-alive
Referer: http://120.78.92.198:8009/manager.php
Upgrade-Insecure-Requests: 1
抓取到的信息
user=admin&pass=12345
0 matches

在该页面的空白处，单击鼠标右键，选择Send to Repeater，点击之后注意观察页面顶部的Intruder按钮。

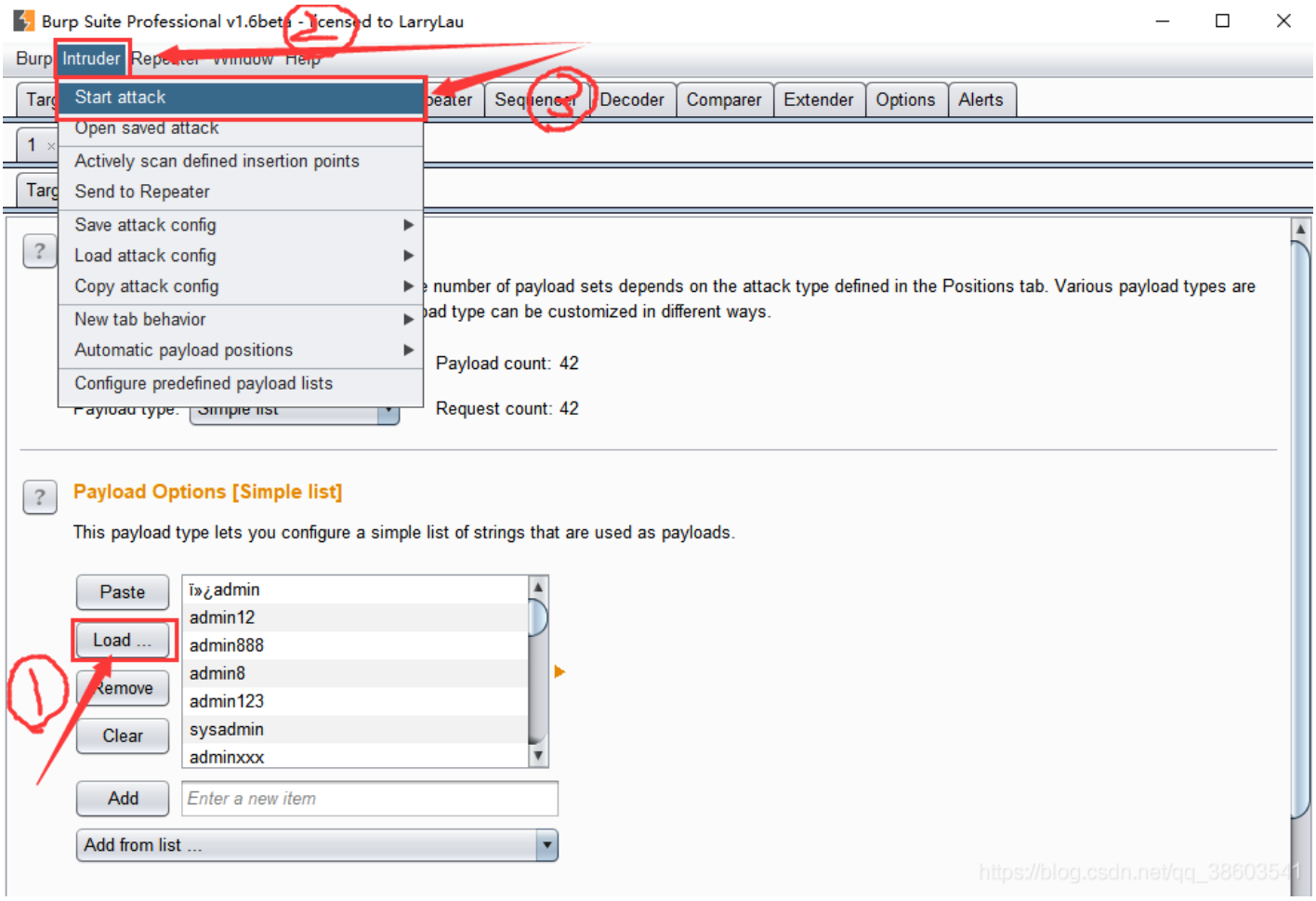


切换到burpsuite中的Intruder下的Position，这个时候我们可以看到一个重要的信息被标注了起来，我们现在爆破的是密码，并不需要爆破用户名，因此我们只选择密码就可以，把标注的用户名的参数取消掉就行，怎么取消？选中点击右边的Clear。

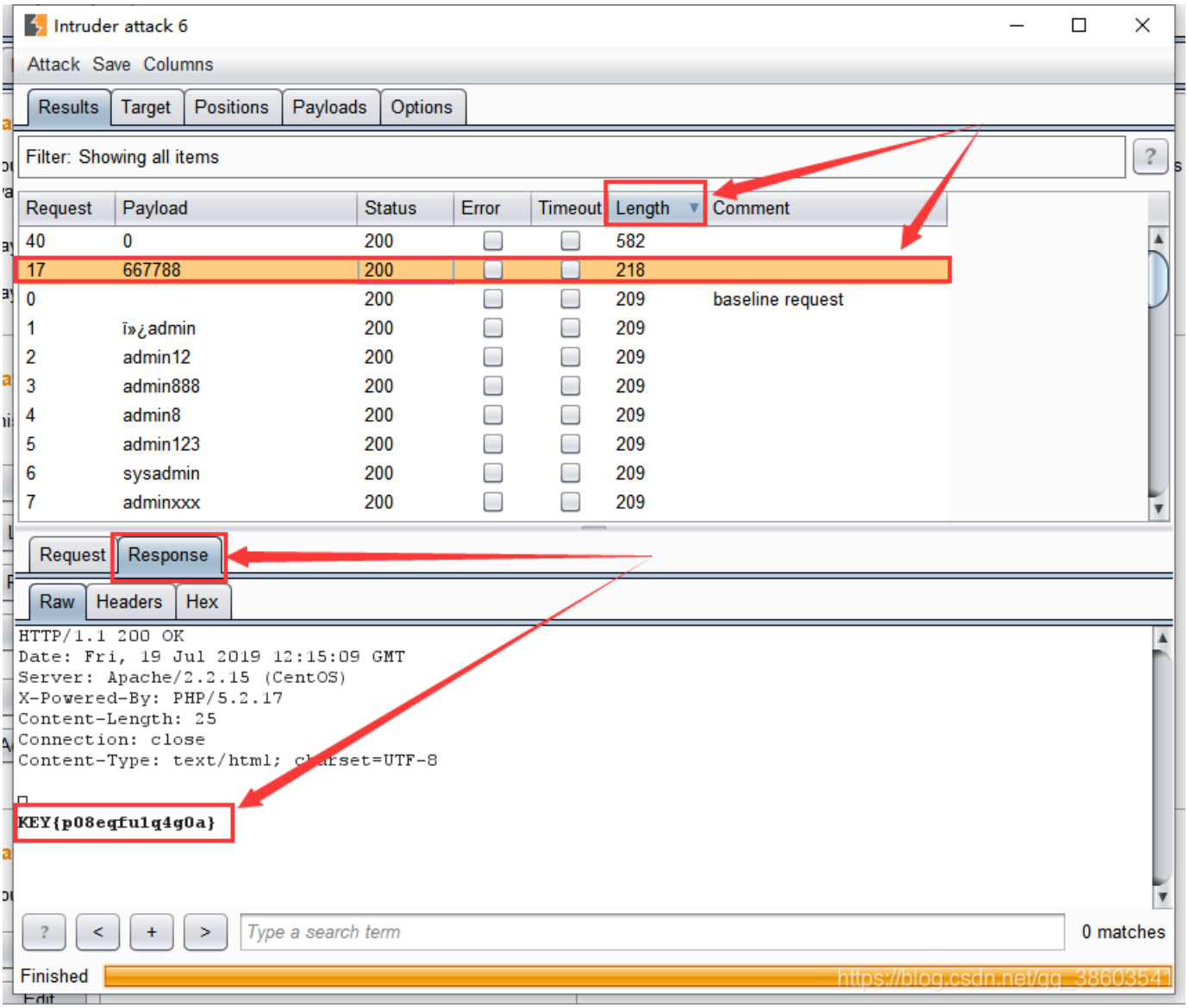


之后，切换到Payloads下，并选择左侧的Load…添加密码字典，点击确定。

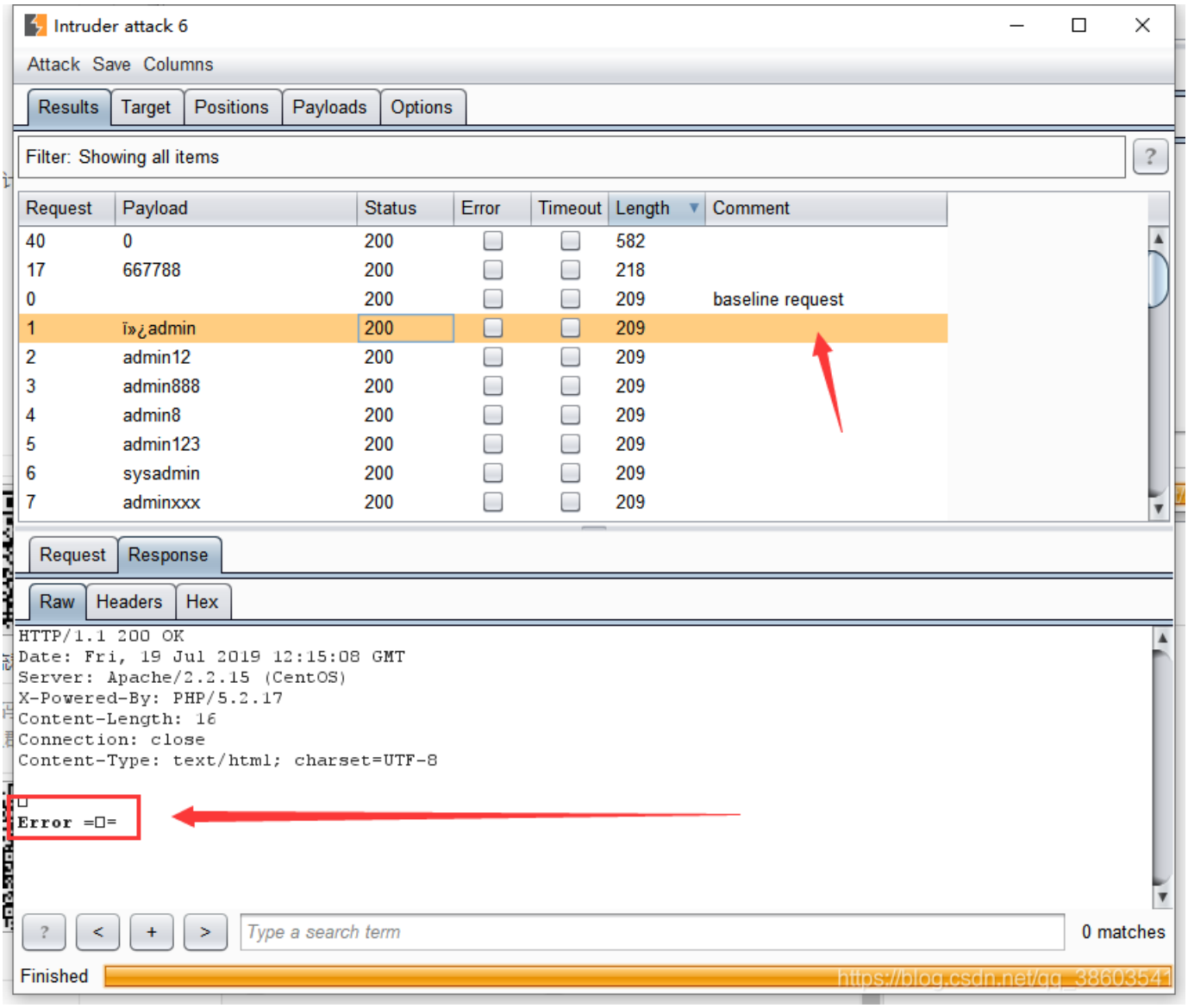
然后，选择最上方的Intruder下的Start attack开始进行密码破解。



由于密码字典是我自己现做的一个简单的密码字典，所以很快我们就可以破解完成。破解完成之后，我们点击length进行排个序看看有没有不同的信息，排序之后，我们发现了长度为218的这一项比较特殊，点击之后跟其他选项反馈的信息都不一样，这样基本上就能判定这个就是密码了……



其它选项爆出的信息，全都是Error这肯定不是啦！



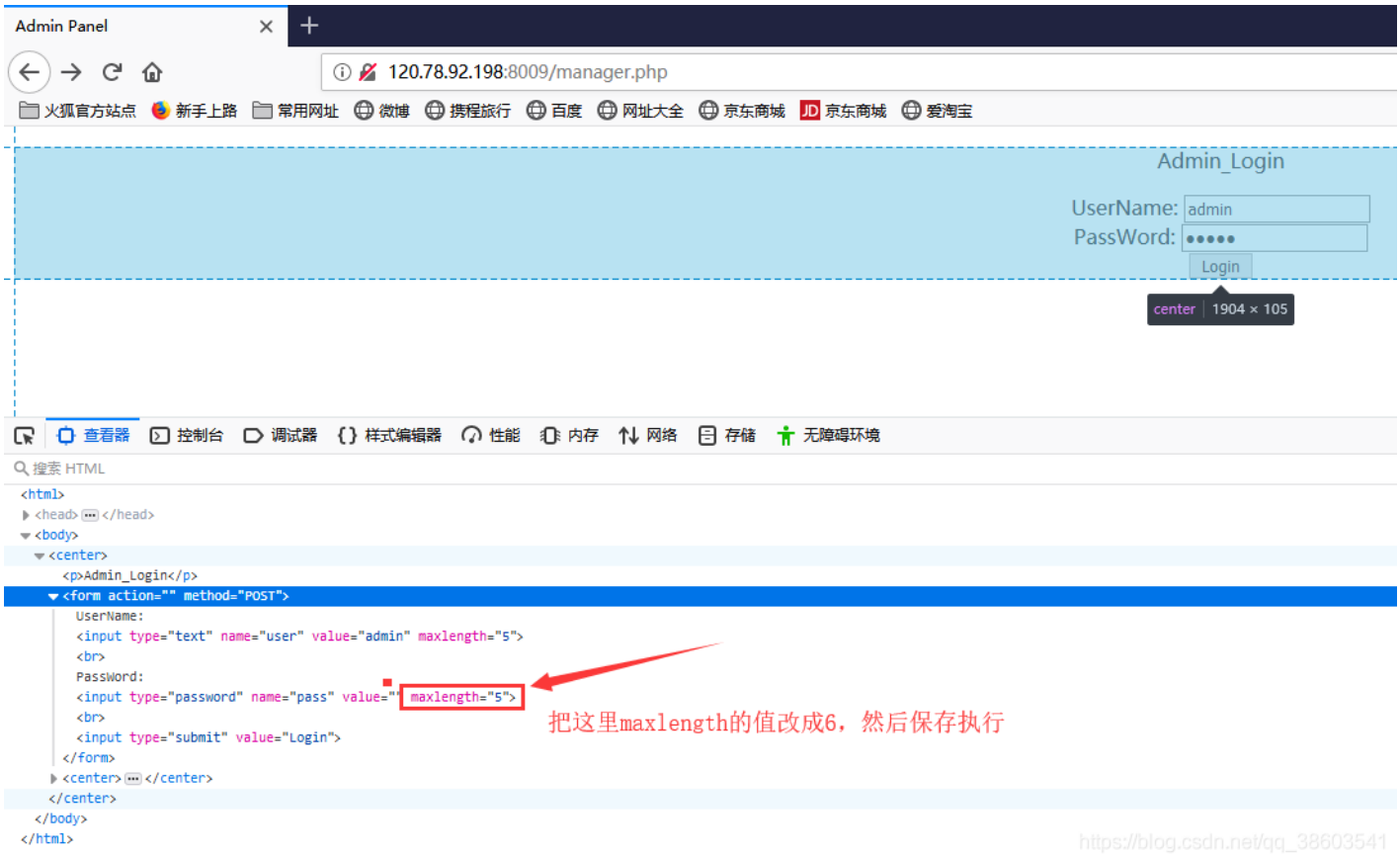
好！现在我们将密码爆破出来以后就可以去网页上进行验证了！

现在我们回到浏览器里，关掉服务代理，输入刚刚爆破出来的密码，进行测试。

测试结果……嗯？？？小老弟怎么回事？？？不对？？？破解出的密码不对？？？怀疑人生了，啊~

细心一点，看看网页还有什么猫腻……

哎~等等……破解出来的是6位数的密码，为什么密码输入框只能输入5位数，F12看看源代码吧……果然，给限制了，这就好办了，把maxlength的值改成6保存，然后输入密码，稳稳的OK。



执行之后，再次输入破解出的6位数密码……哎~这返回的结果有点熟悉啊~这不是CTF的经常用到的答案格式嘛，哈哈哈哈哈

over！结束！