# 封神台——BurpSuite入门（改包、爆破）

原创

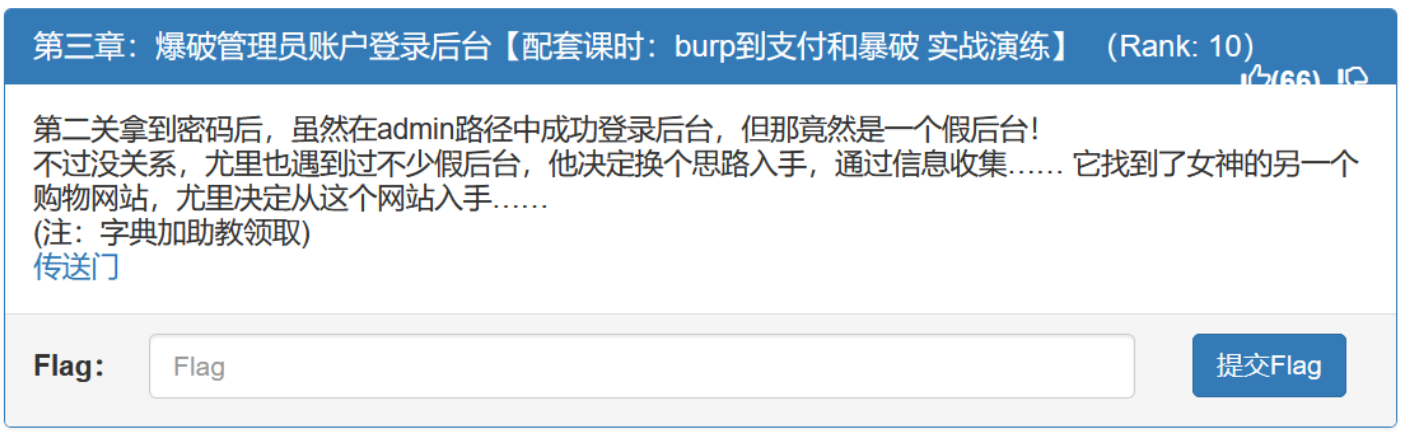
Zichel77 于 2020-07-04 10:38:46 发布 748 收藏 4
分类专栏： web学习 封神台 文章标签： 信息安全 Burp Suite

本文链接：https://blog.csdn.net/weixin_43965597/article/details/107120786



web学习 同时被 2 个专栏收录
65 篇文章 5 订阅
订阅专栏


封神台
5 篇文章 0 订阅
订阅专栏


点击传送门进来看到的就是一个很简陋的网站，我们来到一个网站就先注册一下，感受一下全面的服务


一个假网做的还挺完备


点击一个产品

看到他的设计如此之烂，什么也没有居然要价5400

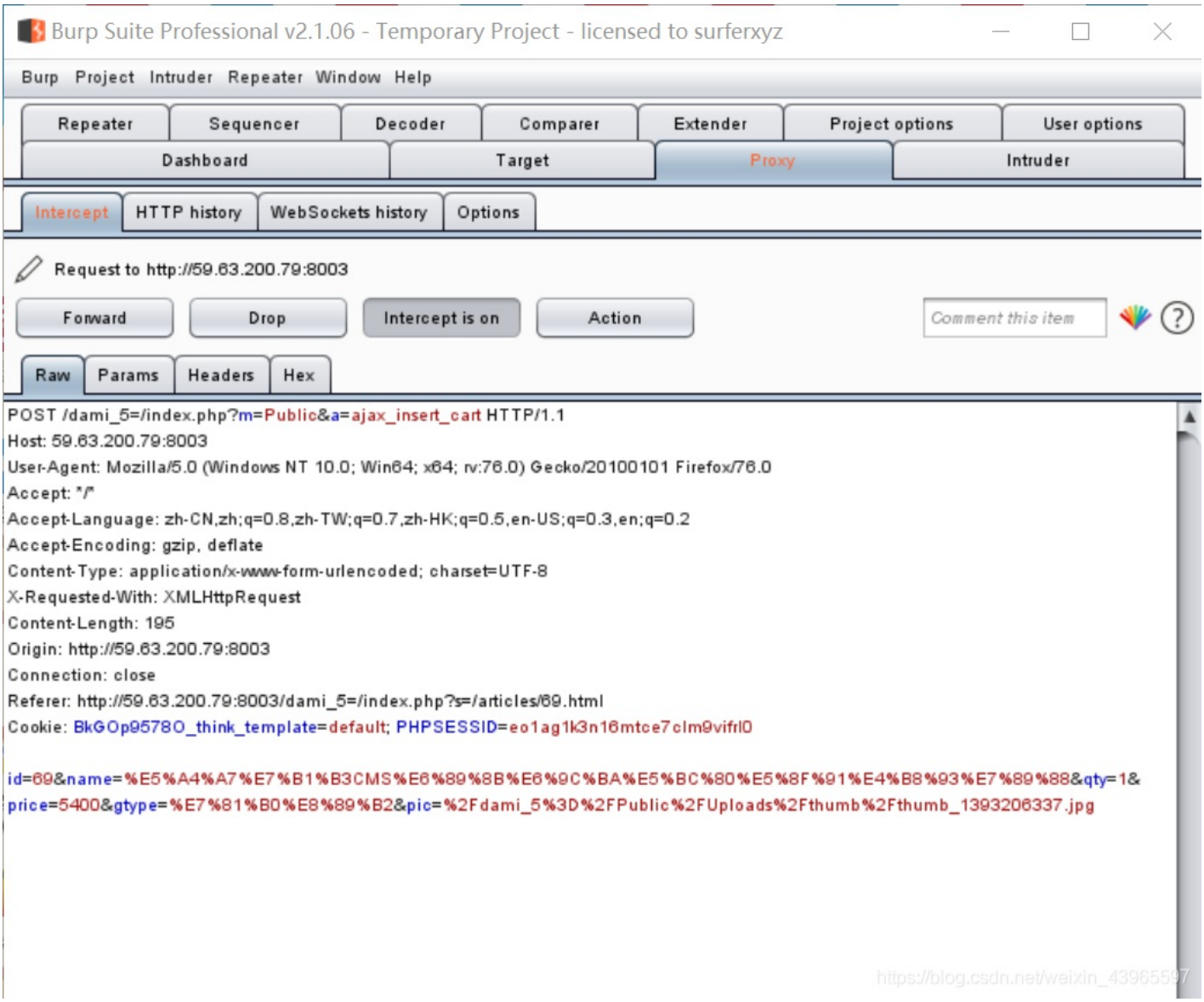
很多购物网站都存在着支付漏洞，于是我们抓个包试试看

首先打开BS，然后打开代理，最后将商品加入购物车

然后发现BS亮了

点进去点进去

抓到了包，然后




我们在密密麻麻的数据中看到了

Price=5400

```
id=69&name='
price=5400&gt
```

这似乎意味着

我们可以截到这个包之后，修改一下价格，然后再放包，这样价格就成功修改了！

于是发送到repeater

在5400中间加了一个点

```
&price=5.400&gt
```

然后SEND

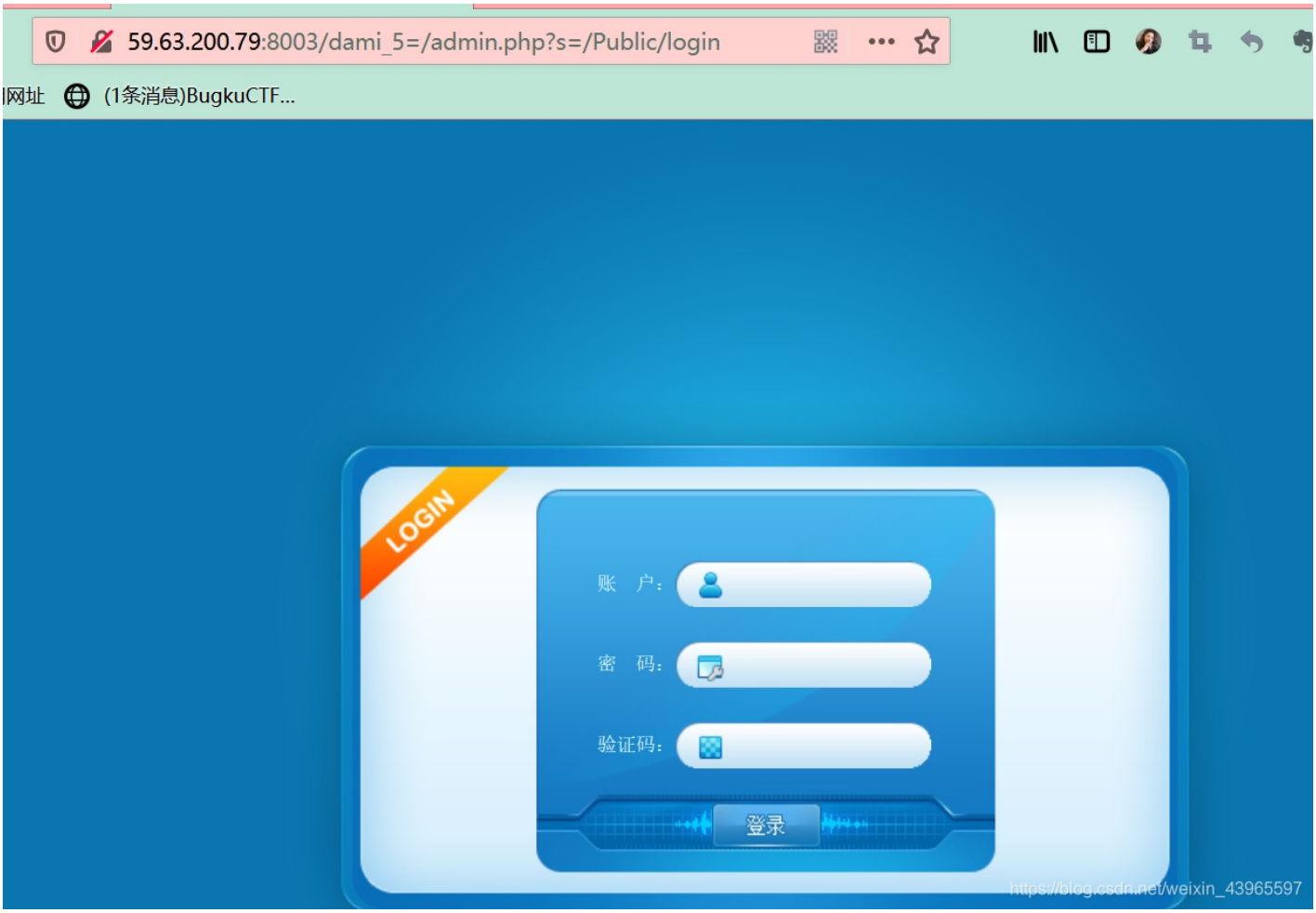
然后关掉代理，看看我们的购物车


哈！哈！哈！哈！哈

平时不要这么干

支付漏洞利用过了开心开心就行了(mss老师如是说）

我们的主要任务是攻入后台，就在url后面加上admin.php，就自动跳转到了这个页面




随便先输入几个试试

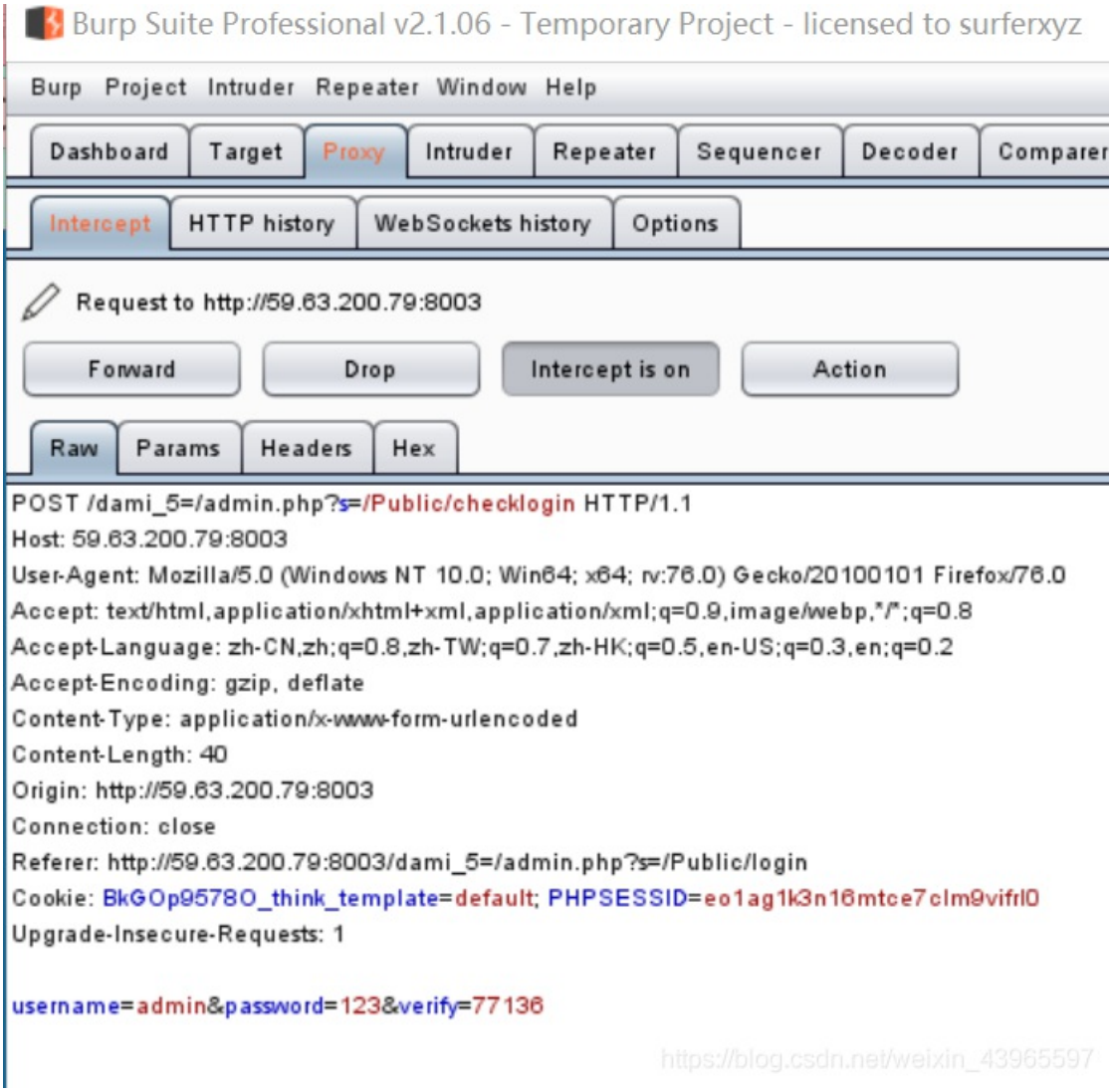
看看报的错是什么

都是账号不存在

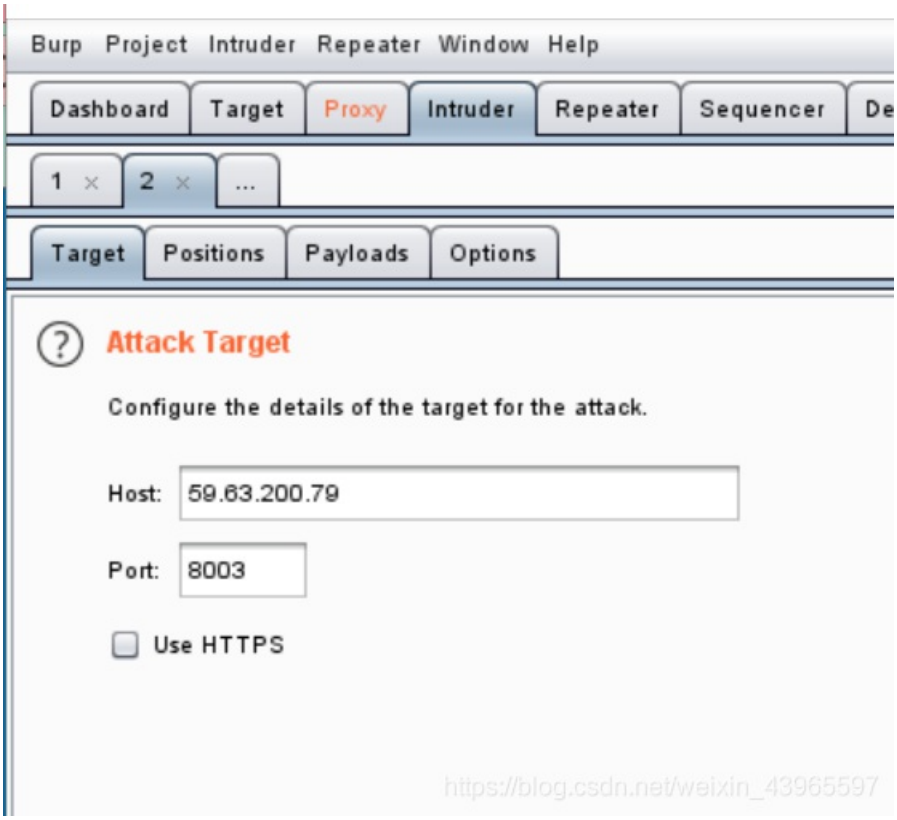
所以我们就是用BS来抓包爆破密码

在截到的很多包里发现了这么一个包

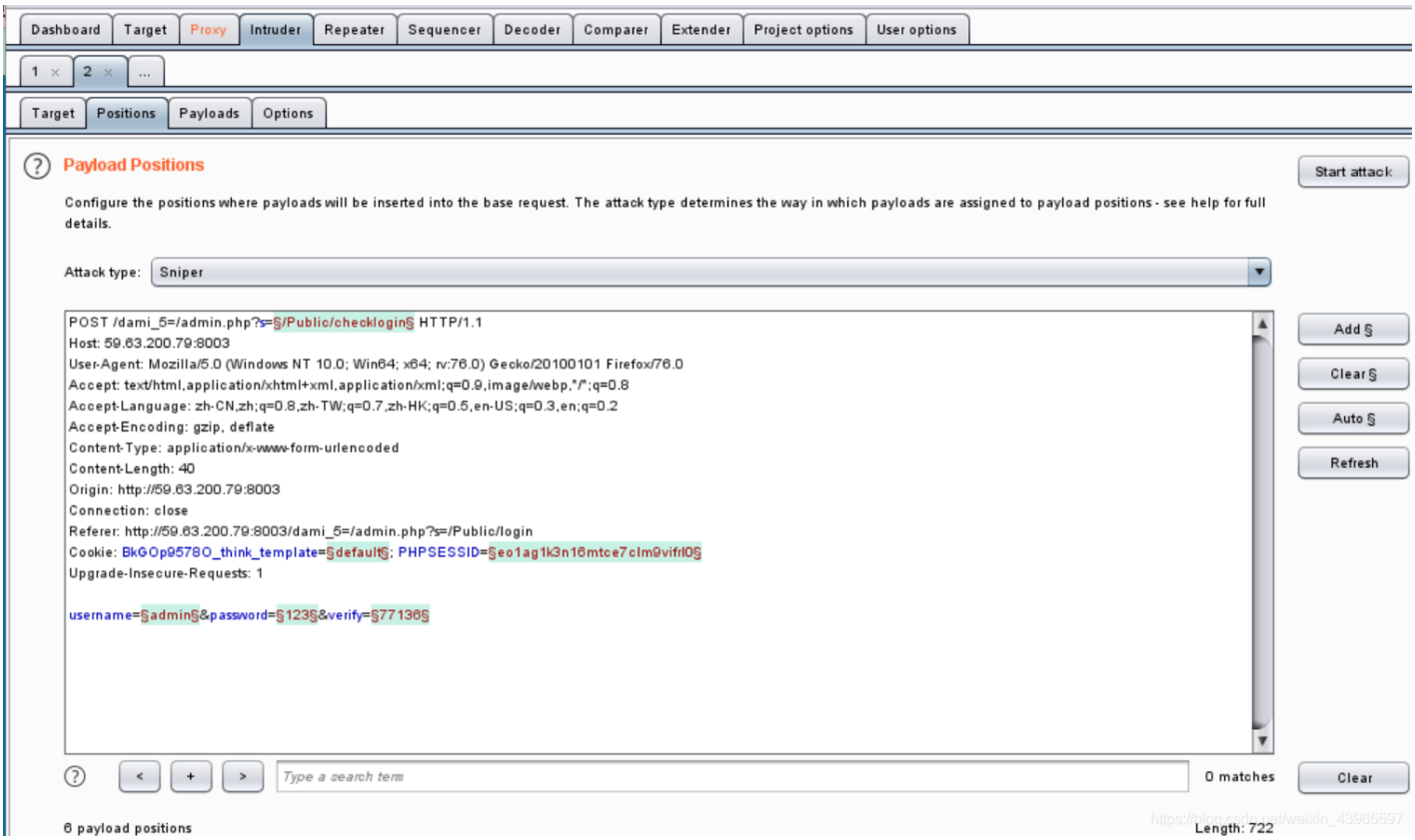
ld,key什么的说明就是当前页面




发送到intruder




点击position




发现BS自动标绿了几个数据项，其中我们需要的只有用户名和密码，所以我们就一键clear

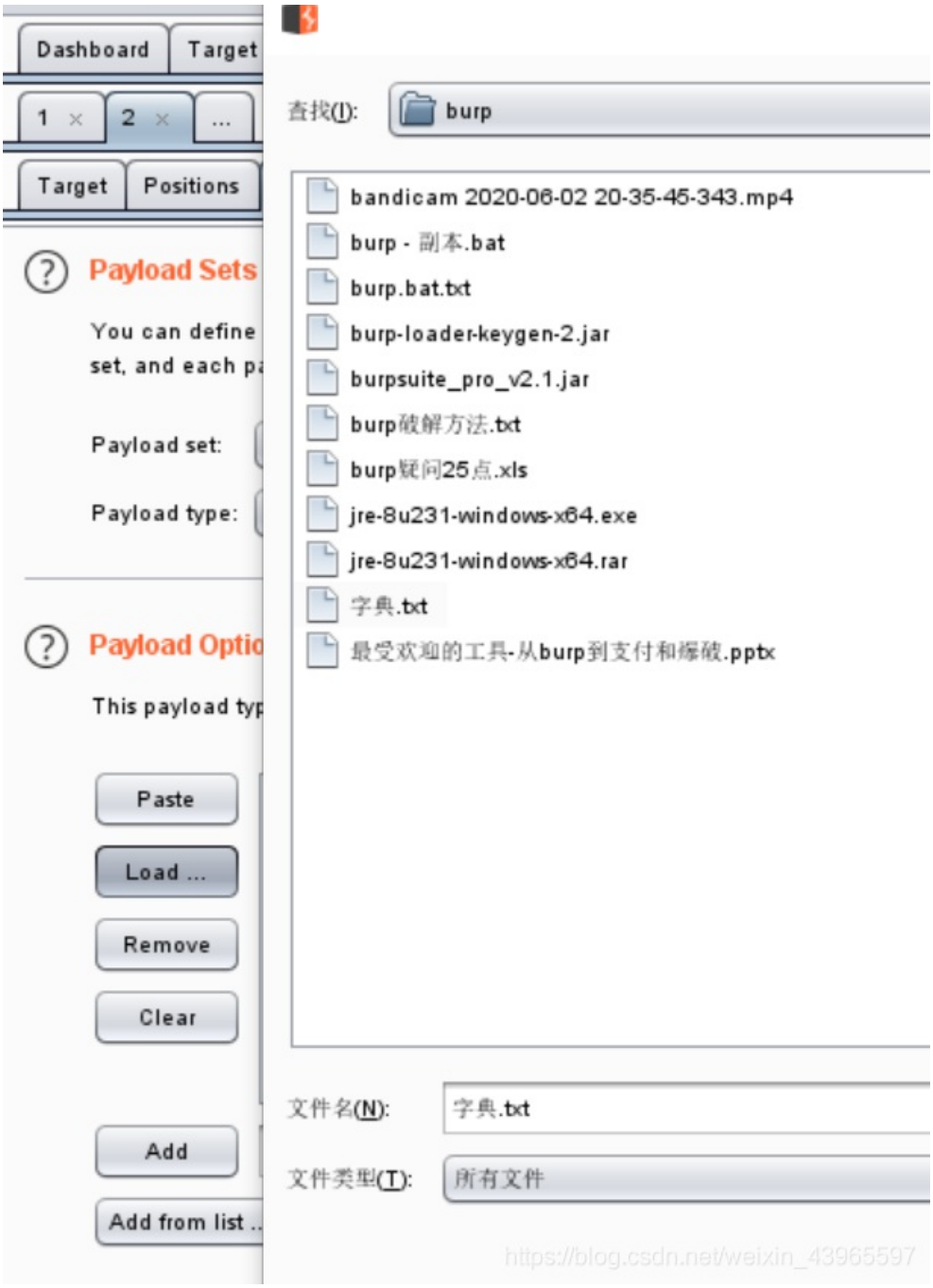
然后自行选择想要爆破的数据

双击数据再点击Add就能标绿了


再点击Payloads


由于我们是使用弱口令字典去一个个试密码，所以我们就要把弱口令字典手动添加到里面

选择Load来添加



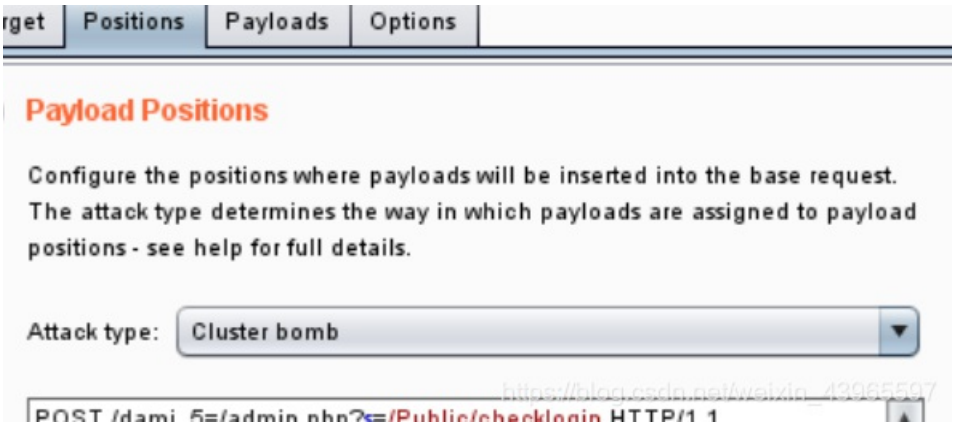

结果我就很无语

为什么选了两个爆破点

出来用字典的只有一个爆破点呢？？？？？？迷惑


又看了看视频发现了我漏了一个小点

在Position页面应该把Attack Type从Sniper改成Cluster Bomb




再去看Payload Set就有两个选项了

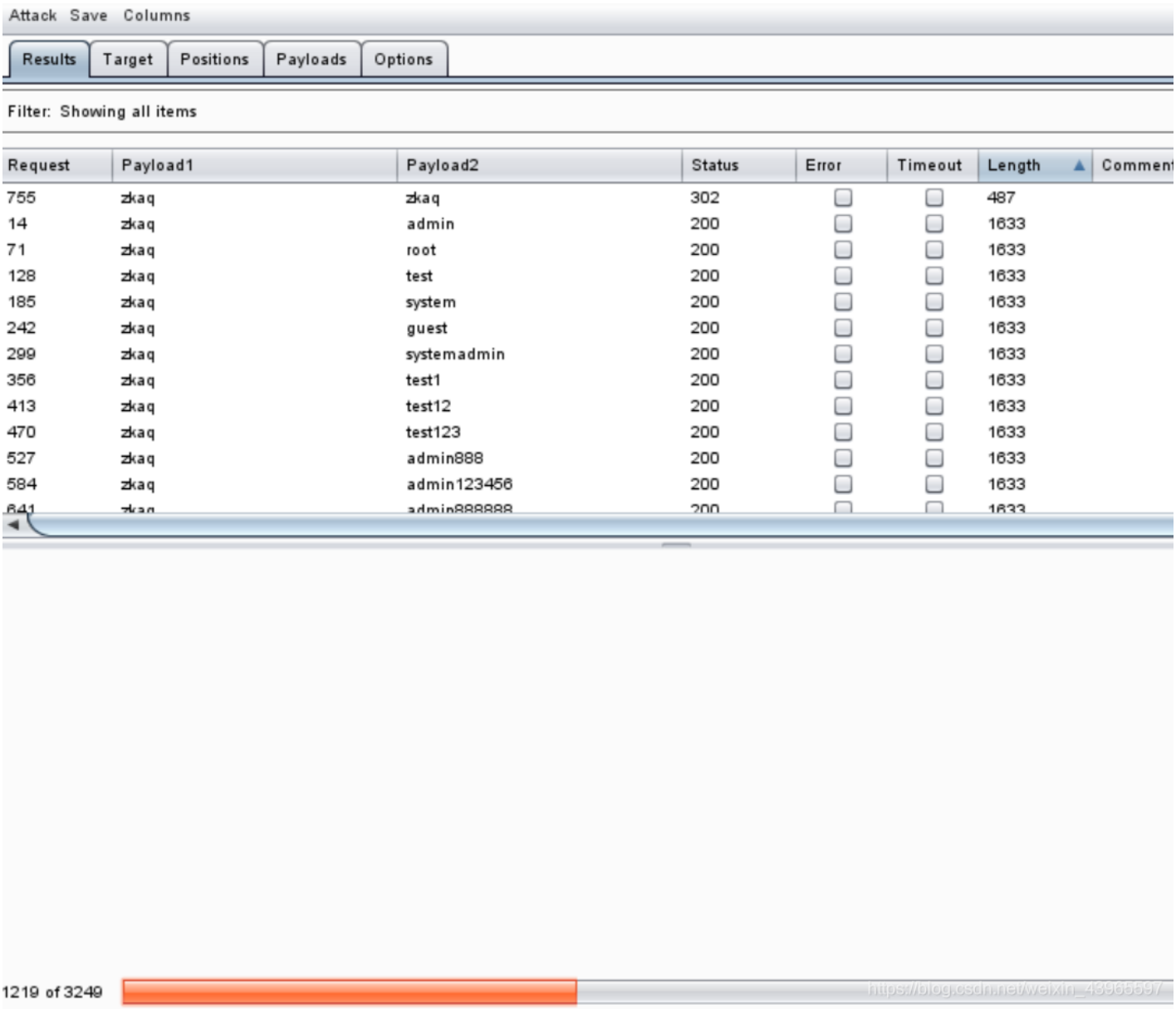
两个都加上字典


然后start attack

这是一个漫长的过程

为了及时看到不一样的弱口令，我们选择按Length升序排序

果然找到你


Attack Save Columns
Results Target Positions Payloads Options
Filter: Showing all items
Request Payload1 Payload2 Status Error Timeout Length Comment
755 zkaq zkaq 302 487
14 zkaq admin 200 1633
71 zkaq root 200 1633
128 zkaq test 200 1633
185 zkaq system 200 1633
242 zkaq guest 200 1633
299 zkaq systemadmin 200 1633
356 zkaq test1 200 1633
413 zkaq test12 200 1633
470 zkaq test123 200 1633
527 zkaq admin888 200 1633
584 zkaq admin123456 200 1633
1219 of 3249
https://blog.csdn.net/weixin_43965597

登入后台


找到flag

p.s. 代理一定记得随用随关随用随关