

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](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

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

版权



[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

封神台 - 掌控安全在线演练靶场

[首页](#)

[靶场](#)

[社区](#)

[公告](#)

[导航](#)

[CTF](#)

[个人中心](#)

[注销](#)

- 公开课基础演练靶场 >
- 正式课 - 从入门到进阶 >
- 工具篇 - 从Kali入门学安全
- 训练营 - 0基础学SQL注入
- Kali训练营 - 玩转工具 >
- AWD提升靶场 >
- 技能实战篇演练靶场
- 2019网络空间竞赛
- 基础练习场

比赛名称	分数	状态	突破	查看详情
第一章: 为了女神小芳! 【配套课时: SQL注入攻击原理 实战演练】	5	正常进行	6183次	查看
第二章: 遇到困难! 绕过WAF过滤! 【配套课时: SQL注入攻击原理 实战演练】	10	正常进行	3028次	查看
第三章: 爆破管理员账户登录后台【配套课时: burp到支付和爆破 实战演练】	10	正常进行	117次	完成
第四章: 为了更好的权限! 留言板! 【配套课时: cookie伪造目标权限 实战演练】	10	正常进行	1846次	查看
第五章: 进击! 拿到Web最高权限! 【配套课时: 绕过防护上传木马 实战演练】	15	正常进行	1129次	查看
第六章: SYSTEM! POWER! 【配套课时: webshell控制目标 实战演练】	15	正常进行	801次	查看
第七章: GET THE PASS! 【技能点: 进程中抓下管理员明文密码】	20	正常进行	334次	查看
萌新也能找CMS漏洞	1	正常进行	0次	查看

https://blog.csdn.net/weixin_43965597

第三章: 爆破管理员账户登录后台【配套课时: burp到支付和爆破 实战演练】 (Rank: 10)

第二关拿到密码后, 虽然在admin路径中成功登录后台, 但那竟然是一个假后台! 不过没关系, 尤里也遇到过不少假后台, 他决定换个思路入手, 通过信息收集..... 它找到了女神的另一个购物网站, 尤里决定从这个网站入手.....

(注: 字典加助教领取)

[传送门](#)

Flag:

[提交Flag](#)

https://blog.csdn.net/weixin_43965597



关于公司 MORE >

最近更新

- 大米CMS手机开发专版 2014-02-24
- 大米cms1.21发布 2013-02-20

联系我们 MORE >

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

你的位置: 首页 > 用户登陆

用户名

密码

验证码:

[立即注册](#) [忘记密码?](#)

一个假网做的还挺完备

公司产品 Product

- 移动互联网开发
- JAVA软件开发

点击排行 Hot

- 大米手机CMS
- 大米测试产品
- 测试产品
- 大米CMS手机开发专版

联系我们 Contact

地址：成都市建设南路88号
电话：028-98765432
传真：028-98765430
手机：15982072714
网址：www.damicms.com
邮编：610000

你的位置：首页 > 产品展示 > 移动互联网开发



大米CMS手机开发专版

更新：2014-02-24 09:56:18 点击：48

型号：M002456J

颜色：灰色

价格：**5400 元**

数量：

[立即购买](#) [加入购物车](#)

介绍

大米CMS手机开发专版大米CMS手机开发专版大米CMS手机开发专版大米CMS手机开发专版

评论

以下是网友对 大米CMS手机开发专版 的评论：
暂时还没有评论



https://blog.csdn.net/weixin_43965597

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

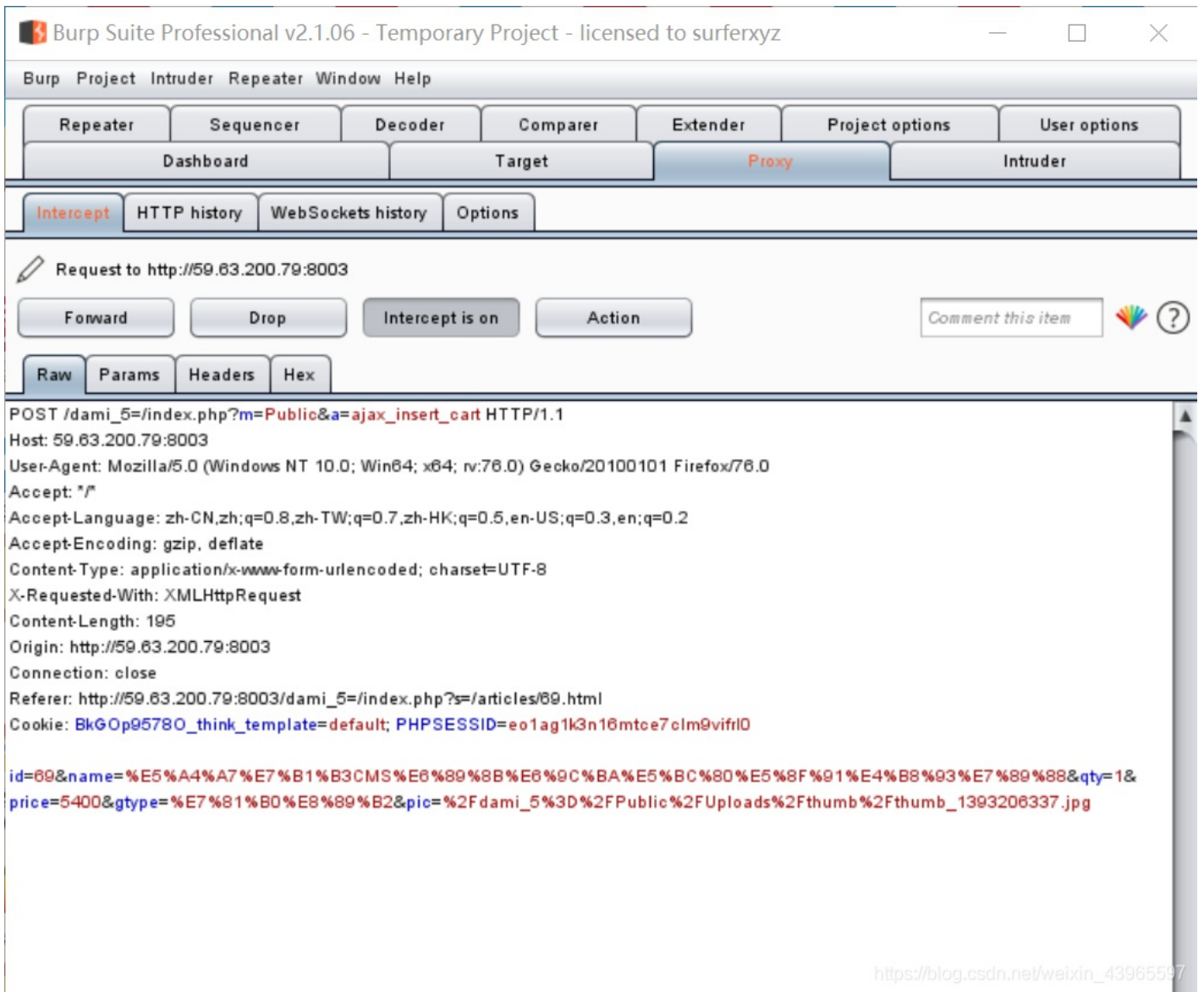
首先打开BS，然后打开代理，最后将商品加入购物车

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

* 你的位置: 首页 > 用户下单

订单列表

编号	名称	型号	数量	单价	小计
69	 大米CMS手机开发专版	灰色	1	5.400	5.4

送货地址(可修改)

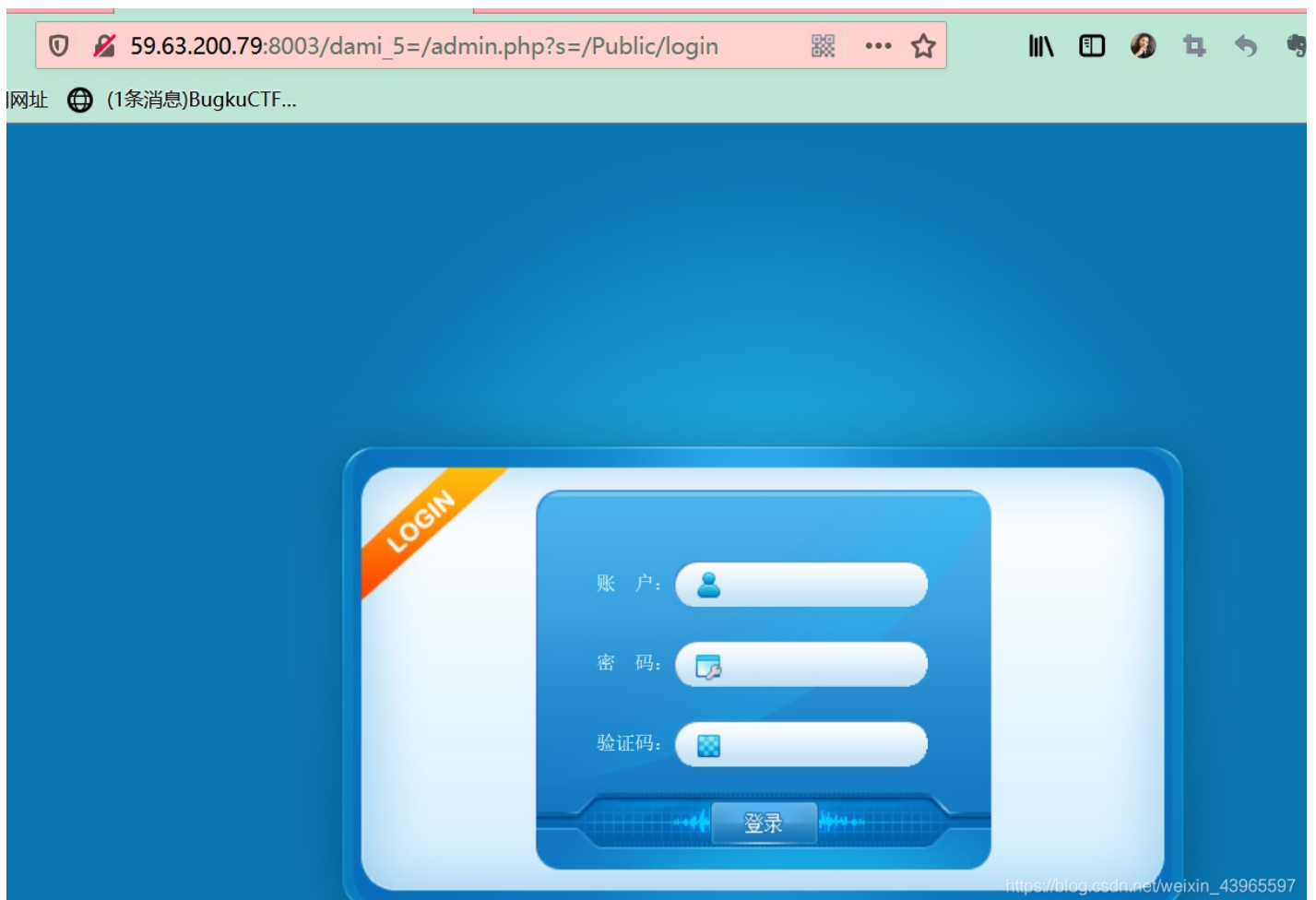
https://blog.csdn.net/weixin_43965597

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

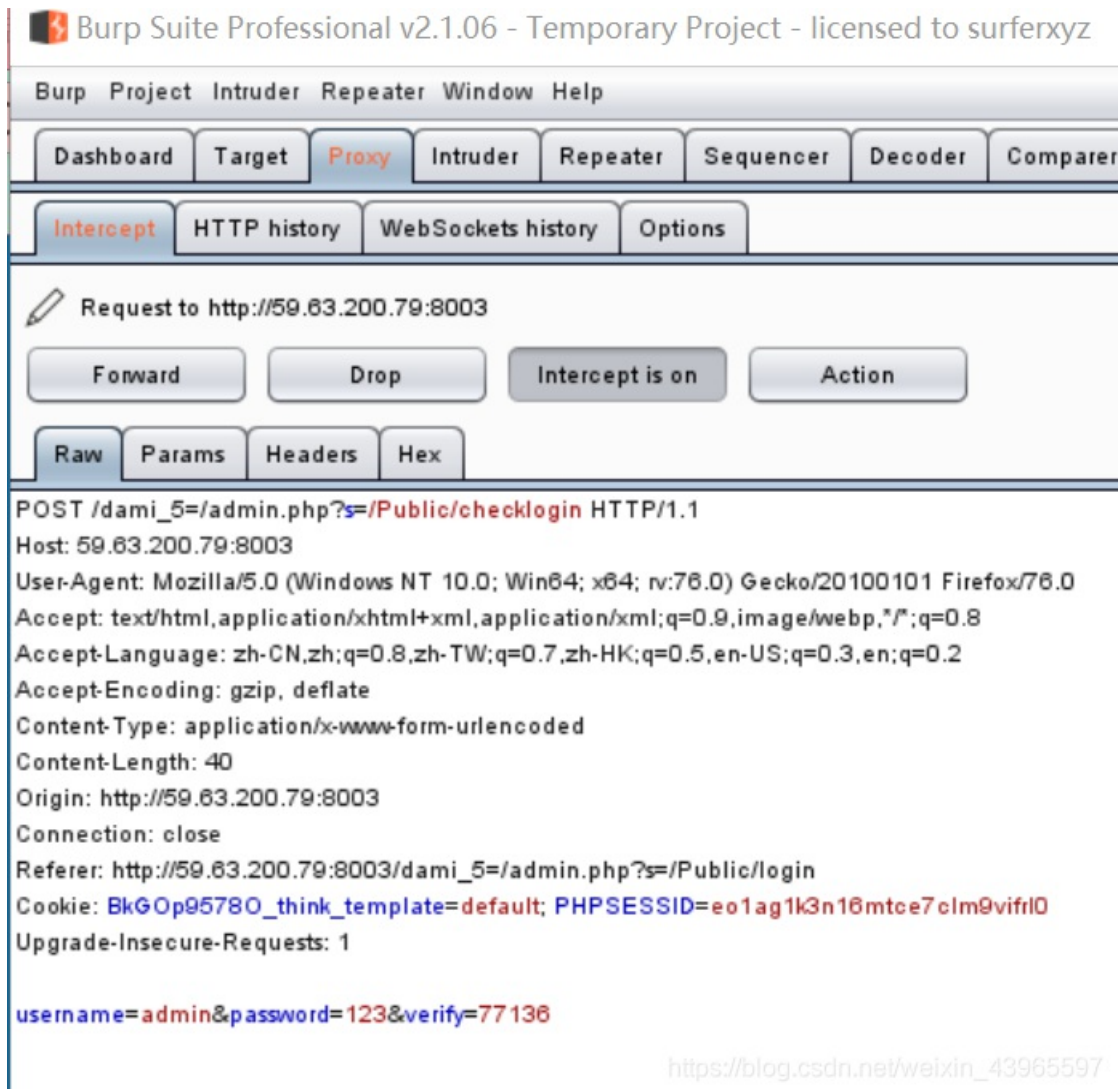
看看报的错是什么

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

Id,key什么的说明就是当前页面



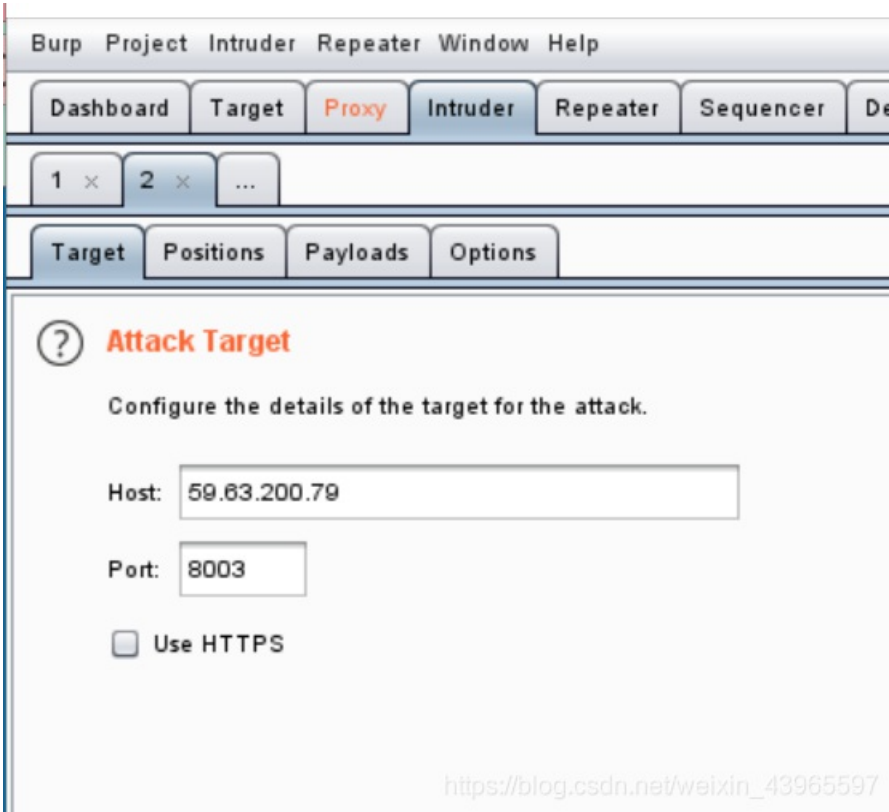
The screenshot shows the Burp Suite interface with the Proxy tab selected. The intercepted request is a POST to `http://59.63.200.79:8003/dami_5=/admin.php?s=/Public/checklogin`. The request body contains the following data:

```
POST /dami_5=/admin.php?s=/Public/checklogin HTTP/1.1
Host: 59.63.200.79:8003
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:76.0) Gecko/20100101 Firefox/76.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;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: 40
Origin: http://59.63.200.79:8003
Connection: close
Referer: http://59.63.200.79:8003/dami_5=/admin.php?s=/Public/login
Cookie: BkGOp9578O_think_template=default; PHPSESSID=eo1ag1k3n16mtce7clm9vifrl0
Upgrade-Insecure-Requests: 1

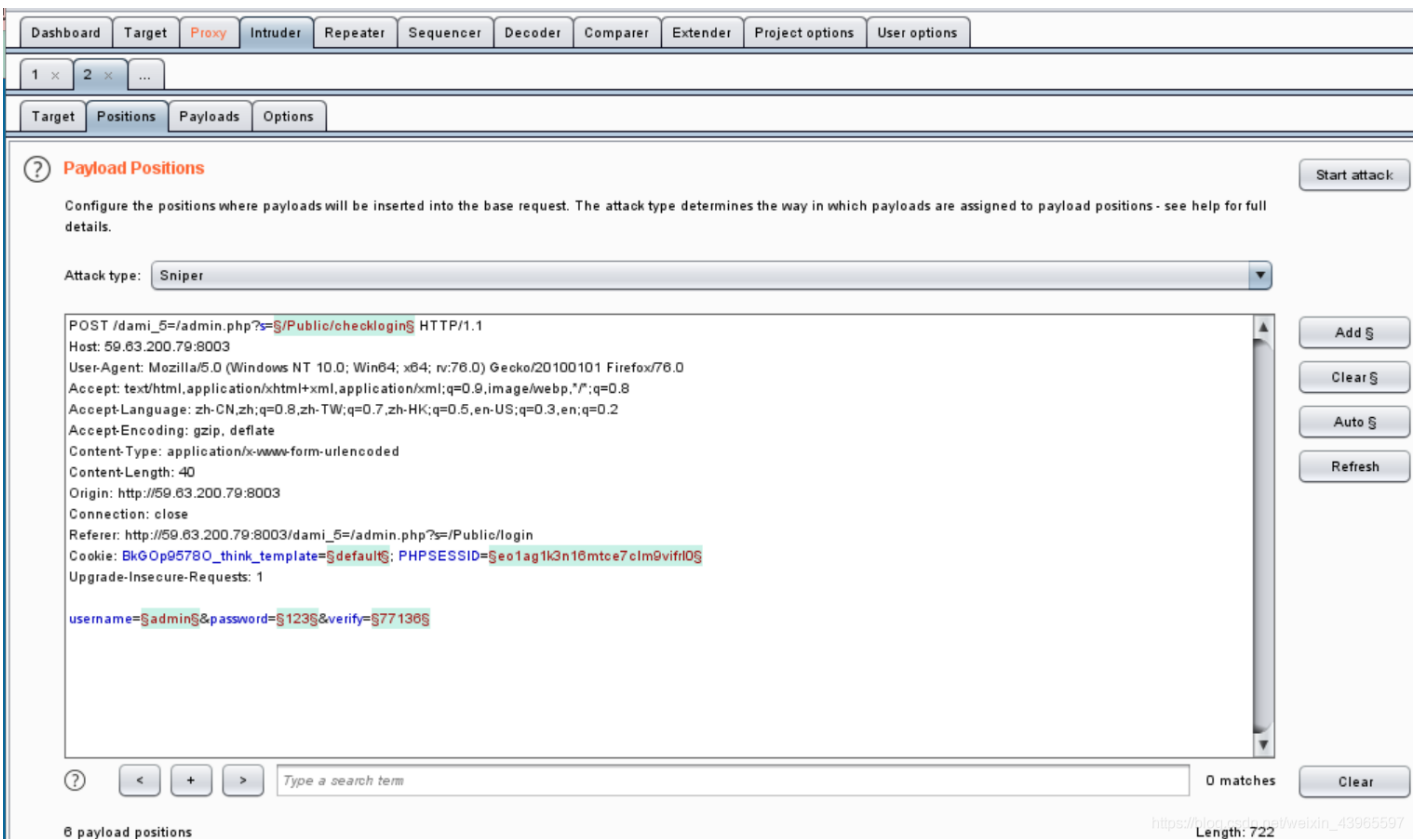
username=admin&password=123&verify=77136
```

The URL `https://blog.csdn.net/weixin_43965597` is visible in the bottom right corner of the screenshot.

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

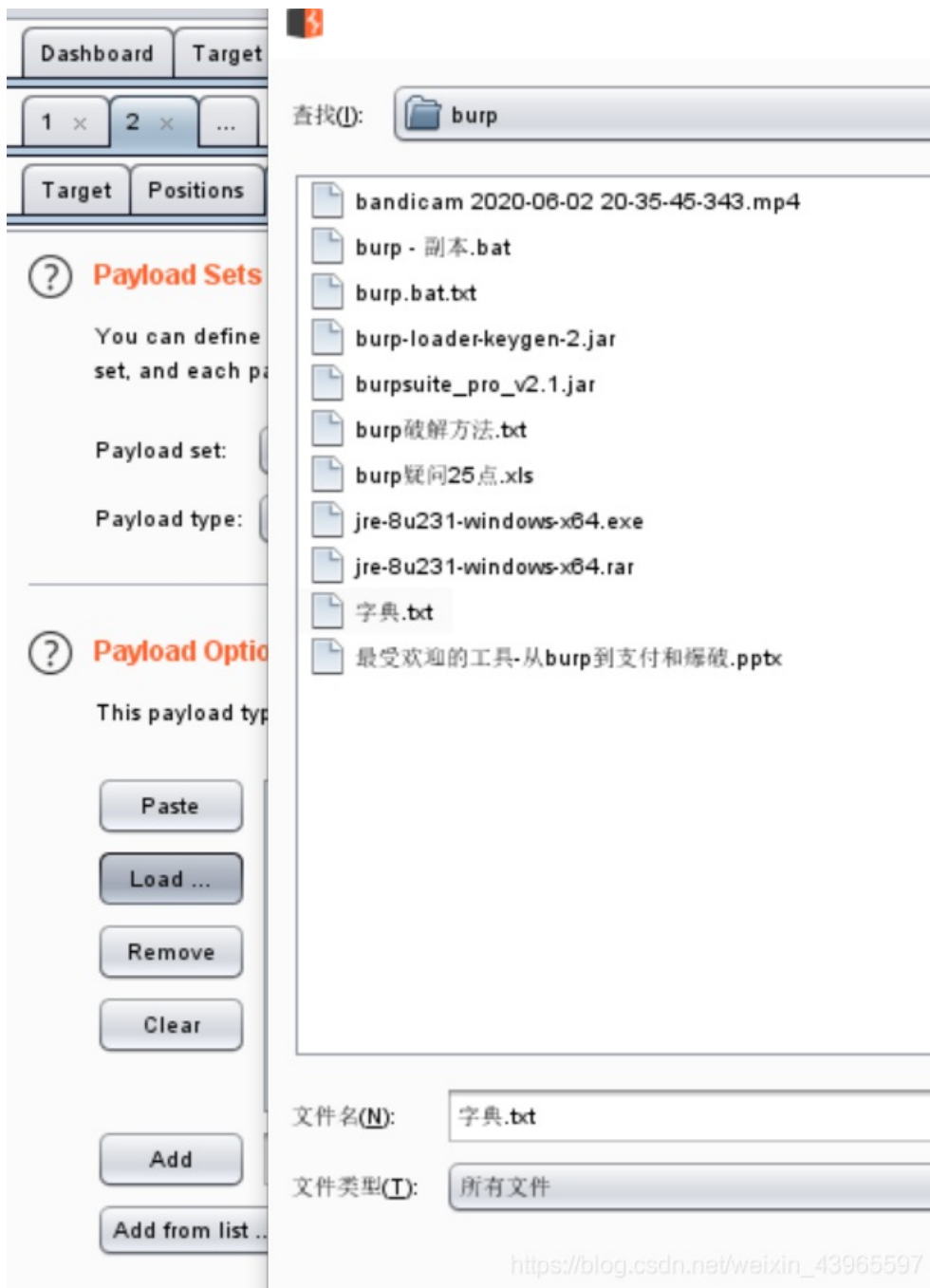
双击数据再点击Add就能标绿了



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

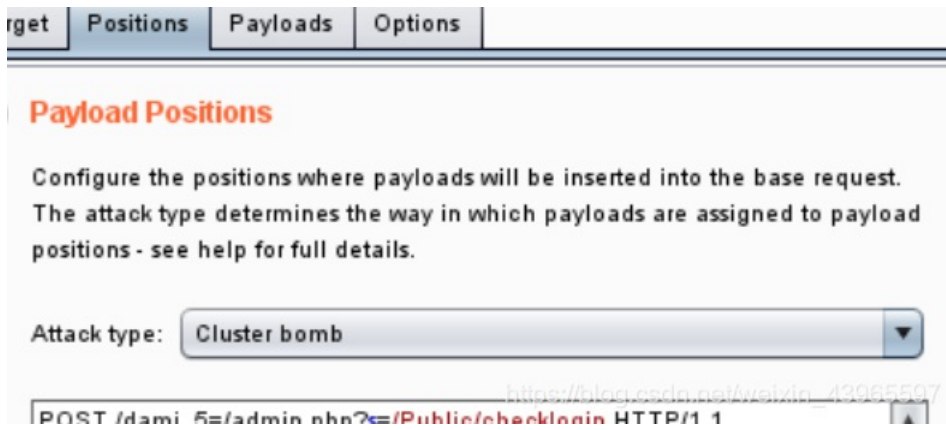
为什么选了两个爆破点

出来用字典的只有一个爆破点呢?????? 迷惑



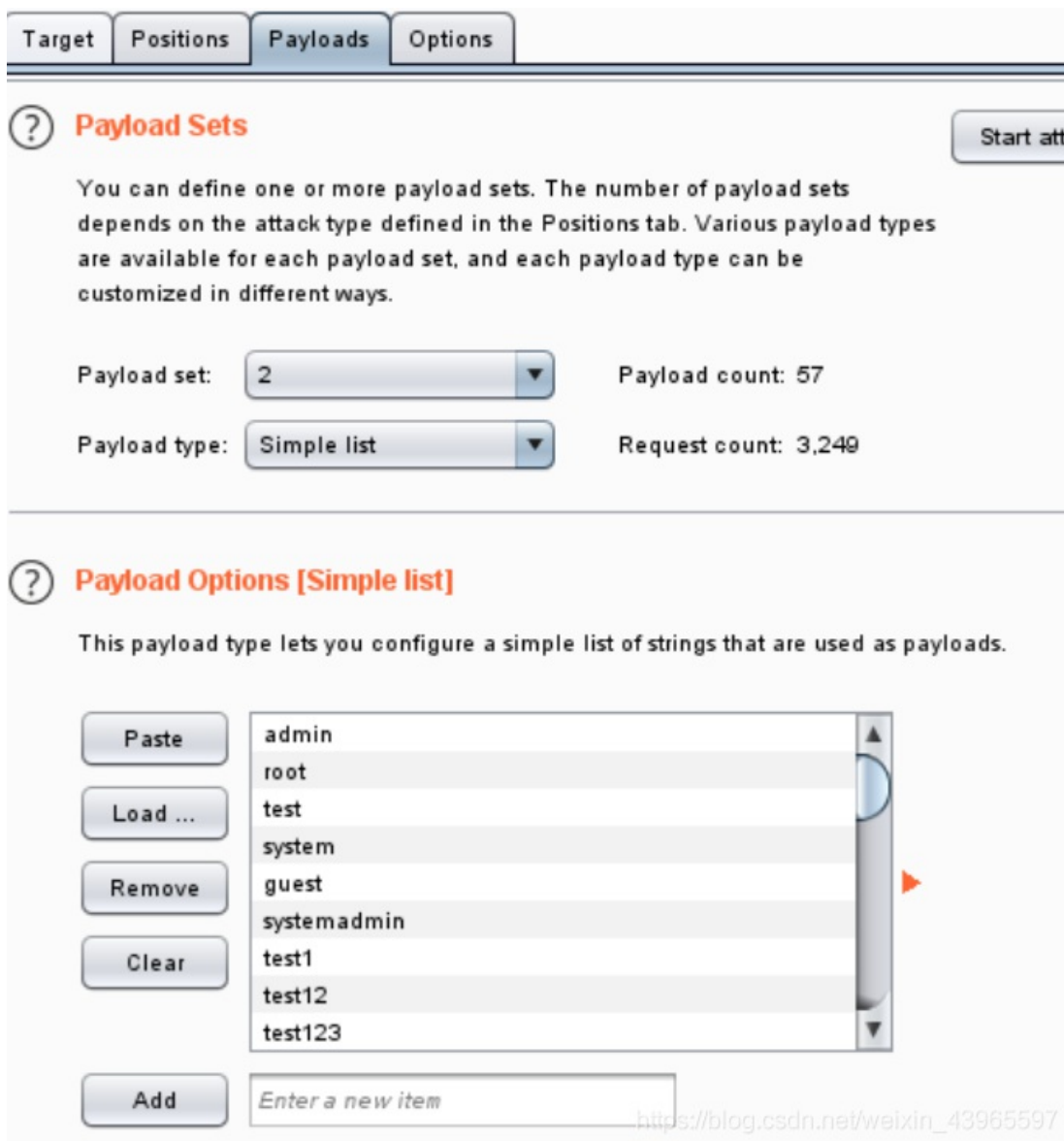
又看了看视频发现了我漏了一个小点

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	<input type="checkbox"/>	<input type="checkbox"/>	487	
14	zkaq	admin	200	<input type="checkbox"/>	<input type="checkbox"/>	1633	
71	zkaq	root	200	<input type="checkbox"/>	<input type="checkbox"/>	1633	
128	zkaq	test	200	<input type="checkbox"/>	<input type="checkbox"/>	1633	
185	zkaq	system	200	<input type="checkbox"/>	<input type="checkbox"/>	1633	
242	zkaq	guest	200	<input type="checkbox"/>	<input type="checkbox"/>	1633	
299	zkaq	systemadmin	200	<input type="checkbox"/>	<input type="checkbox"/>	1633	
356	zkaq	test1	200	<input type="checkbox"/>	<input type="checkbox"/>	1633	
413	zkaq	test12	200	<input type="checkbox"/>	<input type="checkbox"/>	1633	
470	zkaq	test123	200	<input type="checkbox"/>	<input type="checkbox"/>	1633	
527	zkaq	admin888	200	<input type="checkbox"/>	<input type="checkbox"/>	1633	
584	zkaq	admin123456	200	<input type="checkbox"/>	<input type="checkbox"/>	1633	
641	zkaq	admin888888	200	<input type="checkbox"/>	<input type="checkbox"/>	1633	

1219 of 3249 https://blog.csdn.net/weixin_43965697/

登入后台

59.63.200.79:8003/dami_5=/admin.php?s=/Index/index

大米内容管理系统

管理首页 扩展字段 栏目管理 内容管理 清理缓存 一键升级 网站首页 大米官网

您使用的是大米CMS未进行商业授权, 请尽快购买 设置授权码

系统信息

文章总数: 22 未审核: 0 [管理]	栏目总数: 19 [管理]	评论总数: 1 未审核: 0 [管理]
幻灯文章: 2 [管理] [清理幻灯附件]	链接总数: 1 [管理] [添加]	留言总数: 3 未审核: 0 [管理]
操作系统: WINNT	运行环境: Apache/2.4.23 (Win32) OpenSSL/1.0.2j PHP/5.4.45	PHP运行方式: apache2handler
上传附件限制: 2M	执行时间限制: 30秒	服务器时间: 2020年7月2日 20:14:43
北京时间: 2020年7月2日 20:14:43	服务器域名/IP: 59.63.200.79 [59.63.200.79]	剩余空间: 9650.21M
register_globals: OFF	magic_quotes_gpc: NO	magic_quotes_runtime: NO

系统缓存清理

注意: 此操作作用于清空Web和Admin下runtime文件夹,更新系统配置或修改系统模板后请及时更新缓存

快捷管理

https://blog.csdn.net/weixin_43965597

找到flag

p.s. 代理一定记得随用随关随用随关

