

# 封神台靶场-第三章

原创

MrH 于 2020-07-12 00:27:25 发布 1675 收藏 1

分类专栏: [封神台-第三章](#) 文章标签: [渗透测试靶场](#)

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/Mr\\_helloworld/article/details/107293686](https://blog.csdn.net/Mr_helloworld/article/details/107293686)

版权



[封神台-第三章](#) 专栏收录该内容

1 篇文章 0 订阅

订阅专栏

## 第三章：爆破管理员账户登录后台

使用工具: 御剑后台扫描, burpsuit

进入网站后想进入管理后台页面, 试着在url地址后加/admin常试结果成功了, 如果不成功再用工具扫描如下:

ID	地址	HTTP响应
19	http://59.63.200.79:8004/error.asp	200
20	http://59.63.200.79:8004/search.asp	200
21	http://59.63.200.79:8004/shownews.asp	200
22	http://59.63.200.79:8004/vote.asp	200
23	http://59.63.200.79:8004/help.asp	200
24	http://59.63.200.79:8004/inc/foot.asp	200
25	http://59.63.200.79:8004/upload_other.asp	200
26	http://59.63.200.79:8004/download.asp	200
27	http://59.63.200.79:8004/Index.asp	200
28	http://59.63.200.79:8004/GetPassword.asp	200
29	http://59.63.200.79:8004/Image.asp	200
30	http://59.63.200.79:8004/ShowNews.asp	200
31	http://59.63.200.79:8004/Upload_Dialog.asp	200
32	http://59.63.200.79:8004/Upfile_Dialog.asp	200
33	http://59.63.200.79:8004/Upfile_Product.asp	200
34	http://59.63.200.79:8004/admin/ScuthideEditor/ewebeditor.asp	200
35	http://59.63.200.79:8004/admin/ScuthideEditor/PopUp.asp	200
36	http://59.63.200.79:8004/admin/admin.asp	200
37	http://59.63.200.79:8004/admin/cdn.asp	200
38	http://59.63.200.79:8004/admin123/admin.asp	200

登陆后台后使用bp暴力破解模块爆破账户密码 (这里我们知道账号密码就不具体演示了):

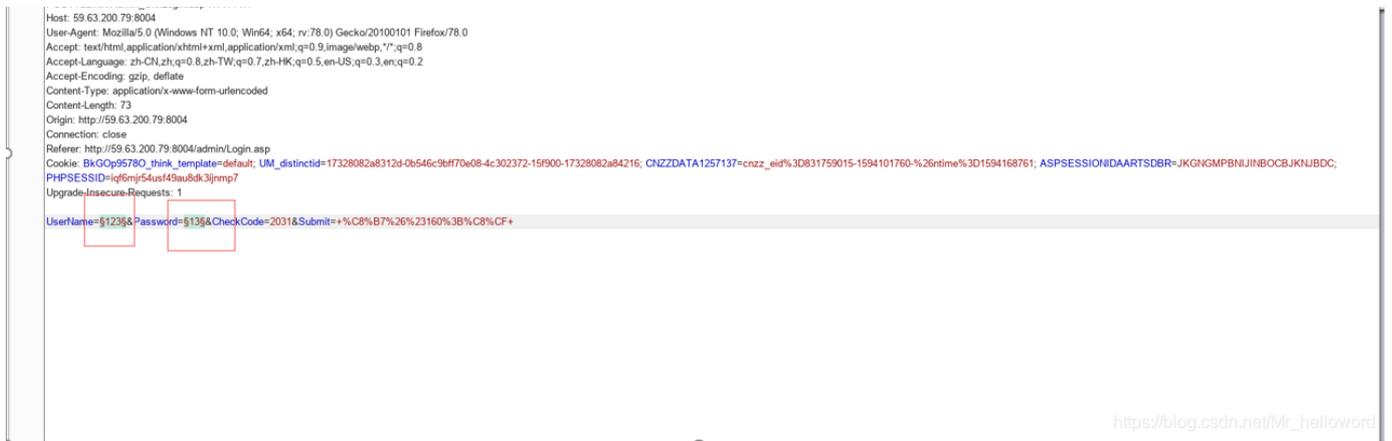
Target: Positions: Payloads: Options

② Payload Positions

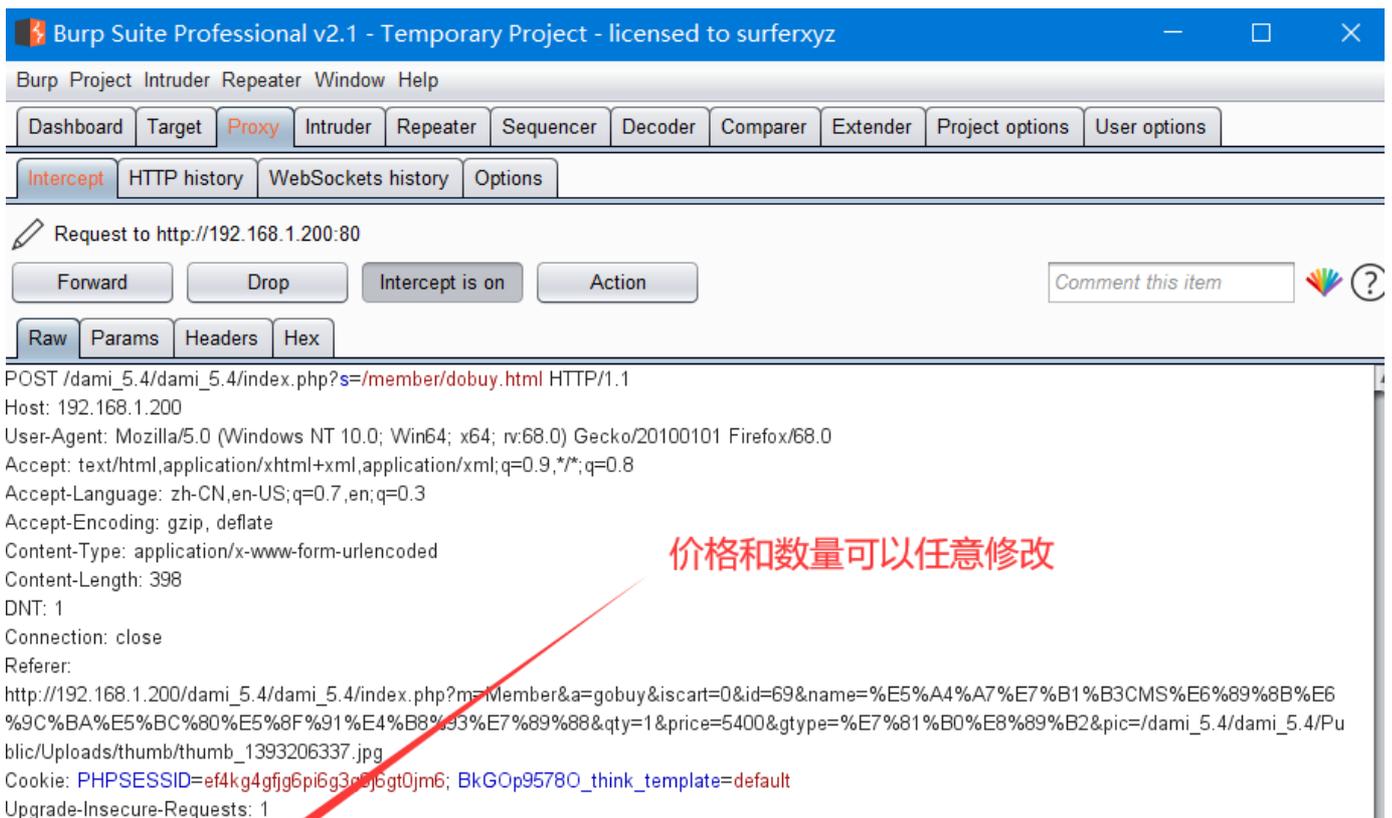
Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Cluster bomb

POST /admin/Admin\_ChkLogin.asp HTTP/1.1



### 3.使用bp修改数量价格



id%5B%5D=69&pic%5B%5D=%2Fdami\_5.4%2Fdami\_5.4%2FPublic%2FUploads%2Fthumb%2Fthumb\_1393206337.jpg&name%5B%5D=%E5%A4%A7%E7%B1%B3CMS%E6%89%8B%E6%9C%BA%E5%BC%80%E5%8F%91%E4%B8%93%E7%89%88&gtype%5B%5D=%E7%81%B0%E8%89%B3&qty%5B%5D=1&price%5B%5D=5400&realname=ggg&tel=17777777777&province=%E6%B2%B3%E5%8C%97&city=%E8%A1%A1%E6%B0%B4%E5%B8%82&area=%E6%B7%B1%E5%B7%9E%E5%B8%82&address=xsl&trade\_type=3&iscart=0

[https://blog.csdn.net/Mr\\_helloworld](https://blog.csdn.net/Mr_helloworld)

flag

竟然成功进入了后台！ 拿走通关KEY，迎接下一关吧！  
zkz{welcome-control}

3

[https://blog.csdn.net/Mr\\_helloworld](https://blog.csdn.net/Mr_helloworld)