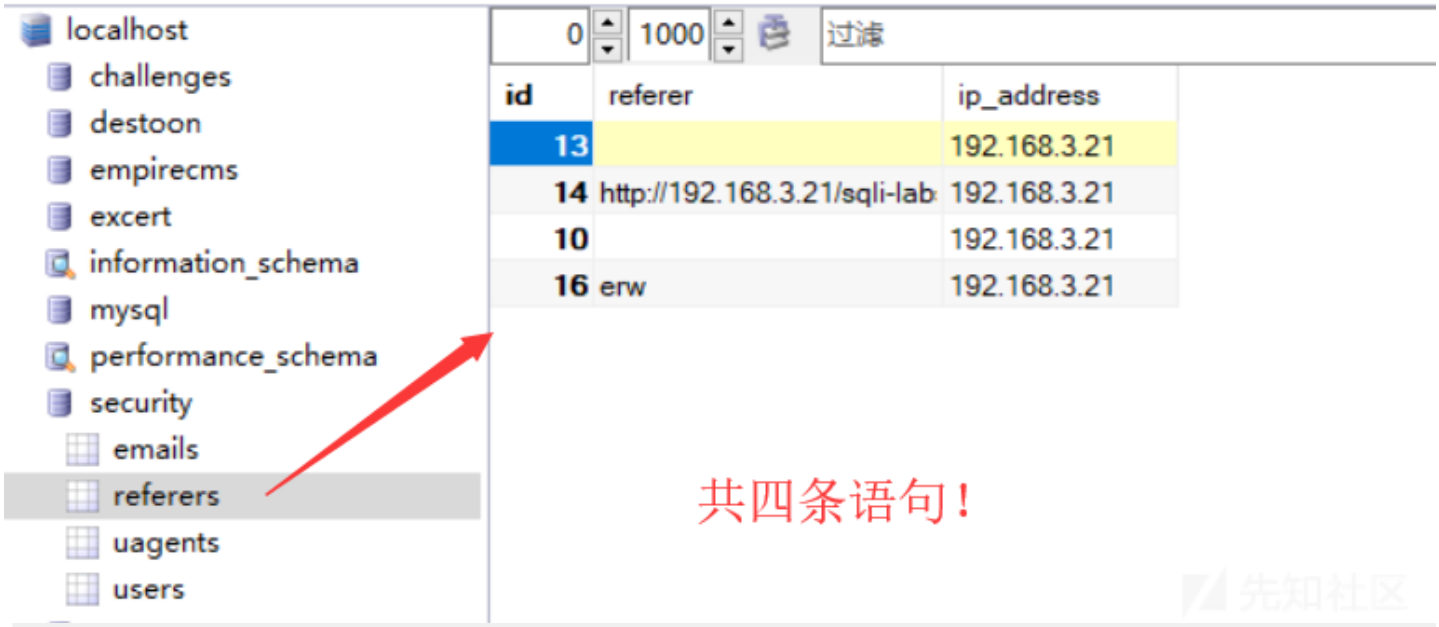
mysql报错注入的脑回路

pers**** / 2019-10-27 08:49:00 / 浏览数 4244 新手 入门资料 顶(0) 踩(0)

1.提出问题：

对于这个问题，出发点是看见报错注入分析中（https://xz.aliyun.com/t/253）说，“010和101开头的序列不会产生报错”。当时就在想按照原理不应该是确定4位才可以保证




```
1  select floor(rand(1)*2),count(*) from referers group by floor(rand(1)*2);
```

信息 | Result 1 | Result 2 | 概况 | 状态

floor(rand(1)*2)	count(*)
0	2
1	2

```
2  select floor(rand(1)*2) from referers;
```

信息 | Result 1 | Result 2 | 概况 | 状态

floor(rand(1)*2)
0
1
0
0

为啥floor(rand(1)2)中产生的序列是0100，但count（ ）后结果却是0和1分别出现2次？

按照当下思路的分析（默认你会分析rand(0)*2），这里的结果是0和1 各是1次。但这里为什么出现的是2次呢？刚开始我也充满了疑问。。。

2.问题分析与解决。

- 问题一：
  答案：上述文章中关于0,1,0和1,0,1序列即可避免报错，这一说法是错误的。要保证无论如何都不会报错必须，至少确定4位序列，即0,1,0,0或0,0,1,1或1,0,1,1或1,1,0,0。（有且只有这四种）
  论证：为什么三位不行？

```
1 select floor(rand(-7)*2) from referers;
```

信息 | Result 1 | 概况 | 状态

floor(rand(-7)*2)
0
1
0
1


```
1 select count(*) from referers group by floor(rand(-7)*2);
```

信息 | 状态

```
select count(*) from referers group by floor(rand(-7)*2)
1062 - Duplicate entry '1' for key 'group_key'
时间: 0.001s
```


- 问题二:
  出现这种问题的原因是没有清楚理解count（），floor（rand（）2），group by（）这三个函数的内涵。
  mysql官方有给过提示，就是查询的时候如果使用rand()的话，该值会被计算多次，那这个"被计算多次"到底是什么意思，就是在使用group by的时候，floor(rand(0)2)会被执行一次，如果虚表不存在记录，插入虚表的时候会再被执行一次。即当虚表中已经出现有0和1这两个键的时候，则rand函数只会执行一
  select count() from referers group by floor(rand(1)2);
  这条语句中count()的值数相加是等于referers表中的条数的，而floor(rand(1)2)的值，一部分，用于验证虚表中是否有这键，另一部分则是虚表中的键和对相同键的累加
  > referers条目数。
  好了，理解到这里已经成功一半多了。可能你还是不懂上面floor（rand（1）*2）产生的0100的序列，可最后count后居然0和1各占两个。先在我们用例子来说明一下。

举例：
users是一个条数比referers多的表，通过此命令我们可以发现rand（1）更长的序列，我们就可以分析出，
select count() from referers group by floor(rand(1)2);
第一次查询，虚表中添加的键是1（rand执行2次）；
第二次查询，虚表中添加的键是0（rand执行2次）；
第三次查询，结果是0（rand执行1次）；
第四次查询，结果是1（rand执行1次）。
最后查询语句select执行了共4次，rand共执行了6次。
所以最后会产生开篇那样两个键的值都是2的结果。

```
1 select floor(rand(1)*2) from users;
```

信息 | Result 1 | 概况 | 状态

floor(rand(1)*2)
0
1
0
0
0
1
1
0
0
0
0
0
1
1
0

1. 0 条回复

- 动动手指，沙发就是你的了！