

SQL注入基础--判断闭合形式

SQL注入基础-判断闭合形式

SQL语句的闭合形式大概如下几种：

```
SELECT * FROM `users` WHERE id= 1;#整形闭合
SELECT * FROM `users` WHERE id='1'; #单引号闭合
SELECT * FROM `users` WHERE id="1";#双引号闭合
SELECT * FROM `users` WHERE id=('1');#单引号加括号
SELECT * FROM `users` WHERE id=("1");#双引号加括号
```

1.整形闭合


```
SELECT * FROM `users` WHERE id= 1;#整形闭合
```

模拟注入：


```
?id=1'
?id=1"
```

```
SELECT * FROM `users` WHERE id= 1';
SELECT * FROM `users` WHERE id= 1";
```

错误

MySQL 返回: 

#1064 - You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '' ;#整形闭合 LIMIT 0, 25' at line 1

MySQL 返回: 

#1064 - You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '' ; LIMIT 0, 25' at line 1

2.单引号闭合

```
SELECT * FROM `users` WHERE id='1'; #单引号闭合
```

模拟注入：

```
?id=1'
?id=1"
```

```
SELECT * FROM `users` WHERE id= '1';
```

报错

```
ersion for the right syntax to use near '' 1'; LIMIT 0, 25' at line 1
```

```
SELECT * FROM `users` WHERE id= '1';
```

可以运行

✓ 正在显示第 0 - 0 行 (共 1 行, 查询花费 0.0004 秒。)

```
SELECT * FROM `users` WHERE id='1'
```

如果写成这样:

```
SELECT * FROM `users` WHERE id= '1'-- ';
```

mysql 不会把后面那个单引号注释掉, 并且会把整个1'-作为查询条件, 可以成功查询和1是一样的! 任何闭合方式都这样在没有遇到相对应的闭合时, 都会把这个符号当做一个整体, 注释符也没用!!

3.双引号闭合

```
SELECT * FROM `users` WHERE id="1";#双引号闭合
```

模拟注入:

```
?id=1'  
?id=1"
```

```
SELECT * FROM `users` WHERE id="1";
```

```
SELECT * FROM `users` WHERE id="1"
```

```
SELECT * FROM `users` WHERE id="1"";
```

报错

```
to use near ' "1""; LIMIT 0, 25' at line 1
```

总结

遇到SQL注入第一步判断闭合:

首先尝试:

```
?id=1'  
?id=1"
```

1如果都报错, 则为整形闭合。

2如果单引号报错, 双引号不报错。

然后尝试

```
?id=1'+
```

无报错则单引号闭合。

报错则单引号加括号。

3如果单引号不报错，双引号报错。

然后尝试

```
?id=1"-+
```

无报错则双引号闭合。

报错则双引号加括号。

多层括号同理