# Mysql

项目：搭建学生管理系统

1.建立数据库

Mysql -u root -p

CREATE DATABASE student\_sys

2.根据需求建立《学生信息表》《学生成绩表》

学生信息表

CREATE TABLE IF NOT EXISTS `studentinfo`(

`stu\_id` INT UNSIGNED AUTO\_INCREMENT,

`stu\_name` VARCHAR(25) NOT NULL,

`stu\_sex` VARCHAR(10) NOT NULL,

`stu\_num` VARCHAR(100)NOT NULL,

`stu\_code` VARCHAR(100)NOT NULL,

PRIMARY KEY ( `stu\_id` )

)ENGINE=InnoDB DEFAULT CHARSET=utf8;

学生成绩表

CREATE TABLE IF NOT EXISTS `studentrecord`(

`record\_id` INT UNSIGNED AUTO\_INCREMENT,

`stu\_num` VARCHAR(100)NOT NULL,

`match\_record` INT NOT NULL,

`datasec\_record` INT NOT NULL,

PRIMARY KEY ( `record\_id` )

)ENGINE=InnoDB DEFAULT CHARSET=utf8;

USE student\_sys;

SHOW TABLES;

SHOW COLUMNS FROM studentinfo;

SHOW COLUMNS FROM studentrecord;

/\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*/

/\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*/

--插入数据

/\* 学生信息 \*/

单条数据输入：

INSERT INTO studentinfo

(stu\_id, stu\_name,stu\_sex,stu\_num,stu\_code)

VALUES

("", "李三", "男","AT08474","62513257312636");

多条数据输入：

INSERT INTO studentinfo

(stu\_id, stu\_name,stu\_sex,stu\_num,stu\_code)

VALUES

("", "黄三", "男","AT08908","67346873246878"),

("", "张小丽", "女","AT08490","73984732984783");

/\* 学生成绩 \*/

多条数据输入：

INSERT INTO studentrecord

(record\_id, stu\_num,match\_record,datasec\_record)

VALUES

("", "AT08908", "80","85"),

("", "AT08474", "90","70"),

("", "AT08490", "95","95");

--查询数据

SELECT COUNT(\*) FROM studentinfo;

SELECT \* FROM studentinfo;

SELECT stu\_id,stu\_name,stu\_sex,stu\_num,stu\_code FROM studentinfo;

------ 显示条数查询

SELECT \* FROM studentinfo LIMIT 0,100;

------ 联合查询

SELECT stu\_id,stu\_name,stu\_sex,stu\_num,stu\_code

FROM studentinfo

UNION

SELECT ALL FROM studentrecord;

Example01

SELECT stu\_name,stu\_num

FROM studentinfo

UNION

SELECT match\_record,datasec\_record

FROM studentrecord;

------ 带条件查询

SELECT \* FROM studentinfo LIMIT 0,100;

SELECT \*

FROM studentinfo

WHERE stu\_name = "黄三";

------ 模糊查询 LIKE

SELECT \* FROM studentinfo LIMIT 0,100;

SELECT \*

FROM studentinfo

WHERE stu\_name LIKE "黄%";

SELECT \* FROM studentinfo LIMIT 0,100;

SELECT \*

FROM studentinfo

WHERE stu\_name LIKE "%黄%";

------ 排序 ORDER BY

SELECT field1, field2,...fieldN table\_name1, table\_name2...

ORDER BY field1 [ASC [DESC][默认 ASC]], [field2...] [ASC [DESC][默认 ASC]]

SELECT stu\_num,match\_record,datasec\_record

FROM studentrecord

WHERE match\_record >= 90

ORDER BY match\_record;

------ 分组 GROUP BY

SELECT match\_record,COUNT(\*) datasec\_record

FROM studentrecord

GROUP BY match\_record;

--删除数据

DELETE FROM studentinfo WHERE stu\_name = "黄三";

--更新数据

UPDATE table\_name SET field1=new-value1, field2=new-value2 [WHERE Clause]

UPDATE studentinfo

SET stu\_name="黄四"

WHERE stu\_name = "黄三";

/\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*/

/\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*/

--MYSQL注入

--https://websec.ca/kb/sql\_injection

学生系统 -> 学生信息登录

表单 $stu\_num = AT08908\

查询回来结果 result = SELECT \* FROM studentinfo WHERE stu\_num = '$stu\_num';

SELECT \* FROM studentinfo WHERE stu\_num = 'AT08908\';

if !empty(result)

登录成功

else

登录失败

学生系统 -> 成绩查询

表单 $match\_record = 90 AND 0;

查询回来结果 result = SELECT match\_record FROM studentrecord WHERE match\_record = $match\_record;

result = SELECT COUNT(match\_record) FROM studentrecord WHERE match\_record = 90 AND 0;

学生成绩表

CREATE TABLE IF NOT EXISTS `studentrecord`(

`record\_id` INT UNSIGNED AUTO\_INCREMENT,

`stu\_num` VARCHAR(100)NOT NULL,

`match\_record` INT NOT NULL,

`datasec\_record` INT NOT NULL,

PRIMARY KEY ( `record\_id` )

)ENGINE=InnoDB DEFAULT CHARSET=utf8;