

mysql 基础讲解

讲师：跃琪



合天网安实验室-大规模开放在线网安实验教学平台

www.hetianlab.com





公司介绍

公司愿景：培养未来的网络力量

公司官网：<http://www.heetian.com>

湖南合天智汇信息技术有限公司作为国内卓越的网络靶场与人才培养解决方案提供商，主要有**合天网安实验室**和**合天网络靶场**两大产品体系。

目录

➤ 01. mysql数据库基础

➤ 02. sql注入常用语句

➤ 03. 其他数据库介绍



/01

mysql 数据库基础



查询流程



什么是数据库

每个人家里都会有冰箱，冰箱是用来干什么的？冰箱是用来存放食物的地方。

同样的，**数据库是存放数据的地方**。正是因为有了数据库后，我们可以直接查找数据。例如你每天使用余额宝查看自己的账户收益，就是从数据库读取数据后给你的。



数据库：存放数据
(DB,database)

↓ 查找数据



欧耶，余额宝今天收益10元

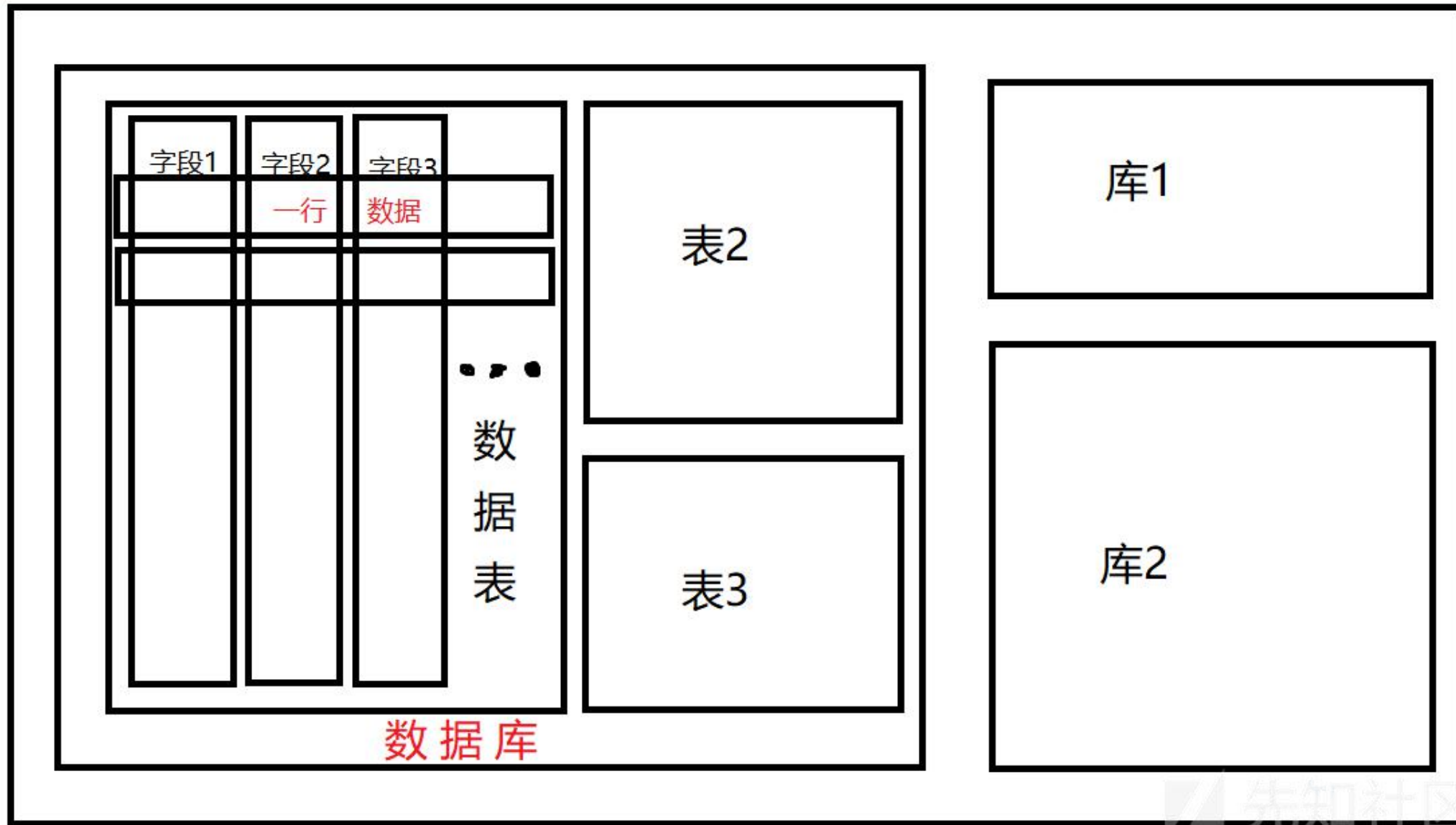
SQL简介

SQL是一门数据库语言。
它可以让你存储和操作数据。



常见的SQL数据库有
Mysql, SQL server,
oracle、sybase、db2。

数据库结构





数据类型

数值类型

类型	大小	范围 (有符号)	范围 (无符号)	用途
TINYINT	1 字节	(-128, 127)	(0, 255)	小整数值
SMALLINT	2 字节	(-32 768, 32 767)	(0, 65 535)	大整数值
MEDIUMINT	3 字节	(-8 388 608, 8 388 607)	(0, 16 777 215)	大整数值
INT或 INTEGER	4 字节	(-2 147 483 648, 2 147 483 647)	(0, 4 294 967 295)	大整数值
BIGINT	8 字节	(-9,223,372,036,854,775,808, 9 223 372 036 854 775 807)	(0, 18 446 744 073 709 551 615)	极大整数值
FLOAT	4 字节	(-3.402 823 466 E+38, -1.175 494 351 E-38), 0, (1.175 494 351 E-38, 3.402 823 466 351 E+38)	0, (1.175 494 351 E-38, 3.402 823 466 E+38)	单精度 浮点数值
DOUBLE	8 字节	(-1.797 693 134 862 315 7 E+308, -2.225 073 858 507 201 4 E-308), 0, (2.225 073 858 507 201 4 E-308, 1.797 693 134 862 315 7 E+308)	0, (2.225 073 858 507 201 4 E-308, 1.797 693 134 862 315 7 E+308)	双精度 浮点数值
DECIMAL	对DECIMAL(M,D) ，如果M>D，为 M+2否则为D+2	依赖于M和D的值	依赖于M和D的值	小数值

数据类型

字符串类型

类型	大小	用途
CHAR	0-255字节	定长字符串
VARCHAR	0-65535 字节	变长字符串
TINYBLOB	0-255字节	不超过 255 个字符的二进制字符串
TINYTEXT	0-255字节	短文本字符串
BLOB	0-65 535字节	二进制形式的长文本数据
TEXT	0-65 535字节	长文本数据
MEDIUMBLOB	0-16 777 215字节	二进制形式的中等长度文本数据
MEDIUMTEXT	0-16 777 215字节	中等长度文本数据
LOBLOB	0-4 294 967 295字节	二进制形式的极大文本数据
LONGTEXT	0-4 294 967 295字节	极大文本数据

SQL约束

含义：一种限制，用于限制表中的数据，为了保证表中数据的准确性和可靠性。

分类：六大约束

1. NOT NULL：非空，用于保证该字段的值不能为空。例如学生表的学生姓名及学号等等。
2. DEFAULT：默认值，用于保证该字段有默认值。例如学生表的学生性别
3. PRIMARY KEY：主键，用于保证该字段的值具有唯一性并且非空。例如学生表的学生学号等。
4. UNIQUE：唯一，用于保证该字段的值具有唯一性，可以为空。例如注册用户的手机号，身份证号等。
5. CHECK：检查约束（MySQL不支持），检查字段的值是否为指定的值。
6. FOREIGN KEY：外键，用于限制两个表的关系，用于保证该字段的值必须来自于主表的关联列的值，在从表添加外键约束，用于引用主表中某些的值。例如学生表的专业编号

添加约束的实际：

1. 创建表时
2. 修改表时

新建数据、表

语法格式

Create database; 新建数据库

Create table 表名

(字段名1 数据类型 约束,
字段名2 数据类型 约束);

```
mysql>  
mysql>  
mysql> create database zonehh;  
Query OK, 1 row affected (0.00 sec)  
mysql>
```

```
mysql> create table admin(username varchar(30) not null);  
Query OK, 0 rows affected (0.11 sec)  
  
mysql>  
mysql>  
mysql> show tables;  
+-----+  
| Tables_in_zonehh |  
+-----+  
| admin             |  
+-----+  
1 row in set (0.00 sec)  
  
mysql> _
```

```
| test  
| tingshop  
| typecho  
| tyshop  
| ultrax  
| vlcms  
| web_identity  
| wecenter  
| xsser  
| zonehh  
| 222CMS  
+-----+  
1  
48 rows in set (0.00 sec)
```



数据库如何执行

举例：mysql数据库的增删改查语句

增：insert into 表名 (字段名1, 字段名2,)
values (v1,v2,.....);

INSERT INTO student(id,name,grade)

VALUES(1,'zhangshan',98);

删：delete from 表名 where 条件;

改：update 表名 set 字段= '值' 【where 条件】;

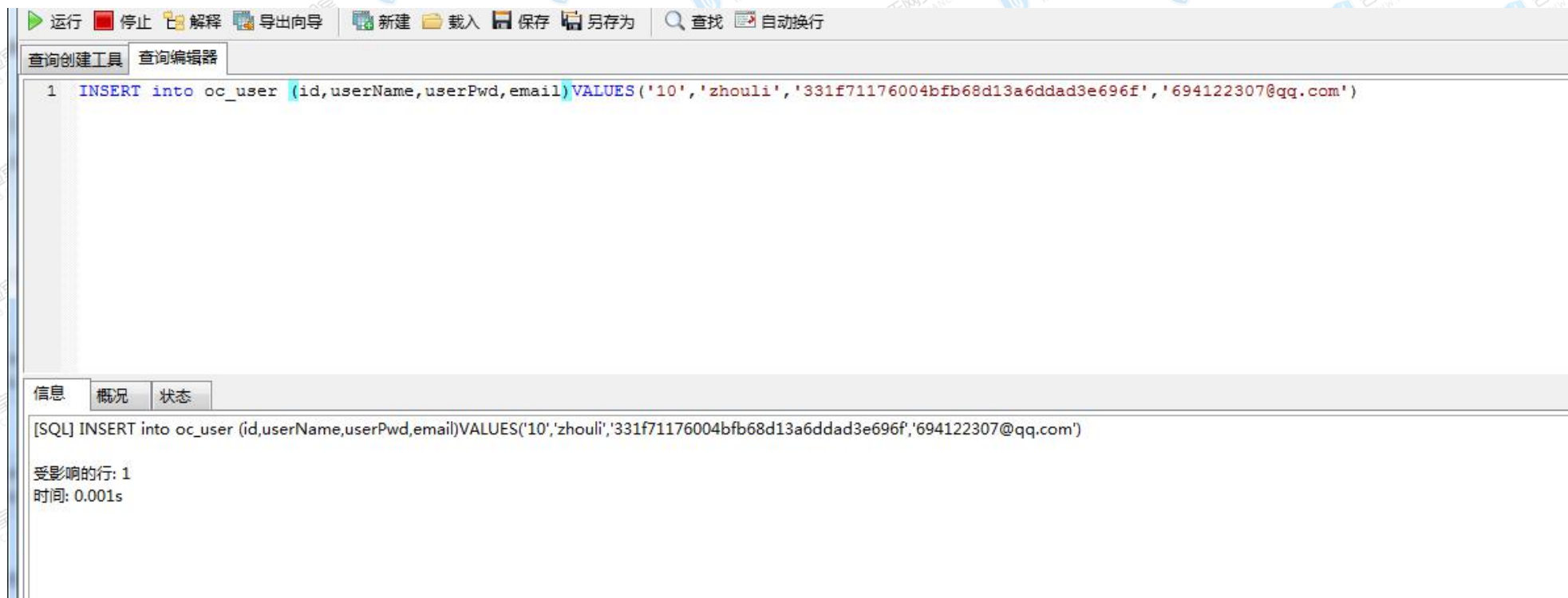
查：select */字段列表 from 表名 【where 条件】



增加一个表

举例：mysql数据库的增删改查语句

增：insert into 表名 (例1, 例2,) values (v1,v2,.....);
INSERT INTO student(id,name,grade) VALUES(1,'zhangshan',98);



删除

删: delete from 表名 where 条件;

查询创建工具 查询编辑器

```
1 DELETE from oc_user where id=10;
```

信息 结果1 概况 状态

id	adminLevel	userName	userPwd	email	phone	message	validated	validateKey	sex
8	1	root	331f71176004bfb68d13a	644730532@qq.com		(Null)	0 (Null)		0
9	0	zoneBAI	331f71176004bfb68d13a	381547123@qq.com		(Null)	0 (Null)		0
10	0	zhanghong	331f71176004bfb68d13a	650000@qq.com	(Null)	(Null)	0 (Null)		0



改

update 表名 set 字段= '值' 【where 条件】;





查询表里面的内容

查： select */字段列表 from 表名 【where 条件】

文件(F) 编辑(E) 格式(O) 查看(V) 窗口(W) 帮助(H)

运行 停止 解释 导出向导 新建 载入 保存 另存为 查找 自动换行 网格查看

查询创建工具 查询编辑器

```
1 select * from oc_user;
```

信息 结果1 概况 状态

id	adminLevel	userName	userPwd	email	phone	message	valid
8	1	root	331f71176004bfb68d13a	644730532@qq.com		(Null)	
9	0	zoneBAI	331f71176004bfb68d13a	381547123@qq.com		(Null)	



Order by 排序

语法格式

Select * from 表名 order by 列名

语句用于根据指定的列对结果集进行排序

order by 特性 当order by的数字

大于当前的列数时候就会报错

sql注入利用这个特性来判断列数以及

显示位

运行

停止

解释

导出向导

新建

载入

保存

另存为

查找

自动换行

网格查看

表单查看

备注

查询创建工具

查询编辑器

1

select * from oc_user order by id

信息

结果1

概况

状态

id	adminLevel	userName	userPwd	email	phone	message	validated	validateKey
8	1	root	331f71176004bfb68d13a	644730532@qq.com		(Null)	0	(Null)
9	0	zoneBAI	331f71176004bfb68d13a	381547123@qq.com		(Null)	0	(Null)



Order by 排序

语法格式

Select * from 表名 order by 列名

语句用于根据指定的列对结果集进行排序

order by 特性 当order by的数字

大于当前的列数时候就会报错

sql注入利用这个特性来判断列数以及

显示位

查询创建工具 查询编辑器

```
1 select * from oc_user order by 24
```

信息 概况 状态

[SQL] select * from oc_user order by 24

[Err] 1054 - Unknown column '24' in 'order clause'

id	adminLevel	userName	userPwd	email	phone	message	validated	validateKey	sex	avatar
8	1	root	331f71176004bfb68d13a	644730532@qq.com		(Null)	0	(Null)	0	(Null)
9	0	zoneBAI	331f71176004bfb68d13a	381547123@qq.com		(Null)	0	(Null)	0	(Null)



Limit控制输出

语法格式

Select * from 表名 limit 开始位置 数量

这里的作用主要是用来控制输出数据的数量

例如我们在注入的时候如果无回显的情况下可以

控制数据然后来进行对比

查询创建工具 查询编辑器

1 select * from oc_user limit 0,2

id	adminLevel	userName	userPwd	email	phone	message
8	1	root	331f71176004bfb68d13a1	644730532@qq.com		(Null)
9	0	zoneBAI	331f71176004bfb68d13a1	381547123@qq.com		(Null)



Limit控制输出

语法格式

Select * from 表名 limit 开始位置 数量

这里的作用主要是用来控制输出数据的数量

例如我们在注入的时候如果无回显的情况下可以

控制数据然后来进行对比

查询创建工具

查询编辑器

```
1 select * from oc_user limit 0,1
```

信息

结果1

概况

状态

id	adminLevel	userName	userPwd	email	phone	n
8	1	root	331f71176004bfb68d13a1	644730532@qq.com		0

查询创建工具

查询编辑器

```
1 select * from oc_user limit 1,2
```

信息

结果1

概况

状态

id	adminLevel	userName	userPwd	email	phone	n
9	0	zoneBAI	331f71176004bfb68d13a1	381547123@qq.com		1



mysql注释符妙用

语法格式

1. 注释符可以替换空格
2. 内联注释：`/*!*/`
`/* */` 在mysql中是多行注释 但是如果里面加了! 那么后面的内容会被执行
3. 单行注释符后面加换行也是可以执行的

`/**/`

`#`

`---`

The screenshot shows a MySQL command-line interface with the following query and results:

```
1 select * from /**/oc_user
```

The results are displayed in a table with the following columns: id, adminLevel, userName, userPwd, email, phone, message, validated, validateKey, sex, and a partial column 'a'.

id	adminLevel	userName	userPwd	email	phone	message	validated	validateKey	sex	a
8	1	zoneBAI	da2c3f4bcded9926c6	644730532@qq.com		(Null)	0	(Null)	0	
9	0	zhangsna	da2c3f4bcded9926c6	zhangsan@163.com	(Null)	(Null)	0	(Null)	0	



mysql注释符妙用

```
1 select * from /*!loc_user*/
```



信息	Result 1	剖析	状态								
	id	adminLevel	userName	userPwd	email	phone	message	validated	validateKey	sex	avat
	8	1	zoneBAI	da2c3f4bcd9926c6	644730532@qq.com		(Null)	0	(Null)	0	(Nul
	9	0	zhangsna	da2c3f4bcd9926c6	zhangsan@163.com	(Null)	(Null)	0	(Null)	0	(Nul



mysql注释符妙用

保存 查询创建工具 美化 SQL 代码段 文本

127.0.0.1 xsser 运行

```
1 select * from--
2 oc_user
```

信息	Result 1	剖析	状态		
	id	adminLevel	userName	userPwd	email
▶	8	1	zoneBAI	da2c3f4bced9926c6 6447	
	9	0	zhangsna	da2c3f4bced9926c6 zhang	

127.0.0.1 xsser

```
1 select * from#
2 oc_user
```

信息	Result 1	剖析	状态	
	id	adminLevel	userName	userPwd
▶	8	1	zoneBAI	da2c3f4bced9926
	9	0	zhangsna	da2c3f4bced9926



mysql版本信息收集和路径

几个常用的:

version() @@version: 版本信息

@@datadir : 返回当前数据库所在路径

@@version_compile_os: 操作系统版本

session_user(): 连接数据库的用户名

system_user(): 系统用户名

database(): 当前数据库

```
1 select @@version;
```

信息	结果 1	剖析	状态
----	------	----	----

@@version

▶ 5.5.53

```
1 select version();
```

信息	结果 1	剖析	状态
----	------	----	----

version()

▶ 5.5.53



mysql版本信息收集和路径

```
1 select @@datadir;
```

信息	结果 1	剖析	状态
----	------	----	----

@@datadir

► D:\yp\gj\phpstudy\PHPTutorial\MySQL\data\

```
1 select session_user() ;
```

信息	结果 1	剖析	状态
----	------	----	----

session_user()

► root@localhost

```
1 select @@version_compile_os;
```

信息	结果 1	剖析	状态
----	------	----	----

@@version_com

► Win32

```
1 select system_user() ;
```

信息	结果 1	剖析	状态
----	------	----	----

system_user()

► root@localhost

```
1 select database() ;
```

信息	结果 1	剖析	状态
----	------	----	----

database()

► security

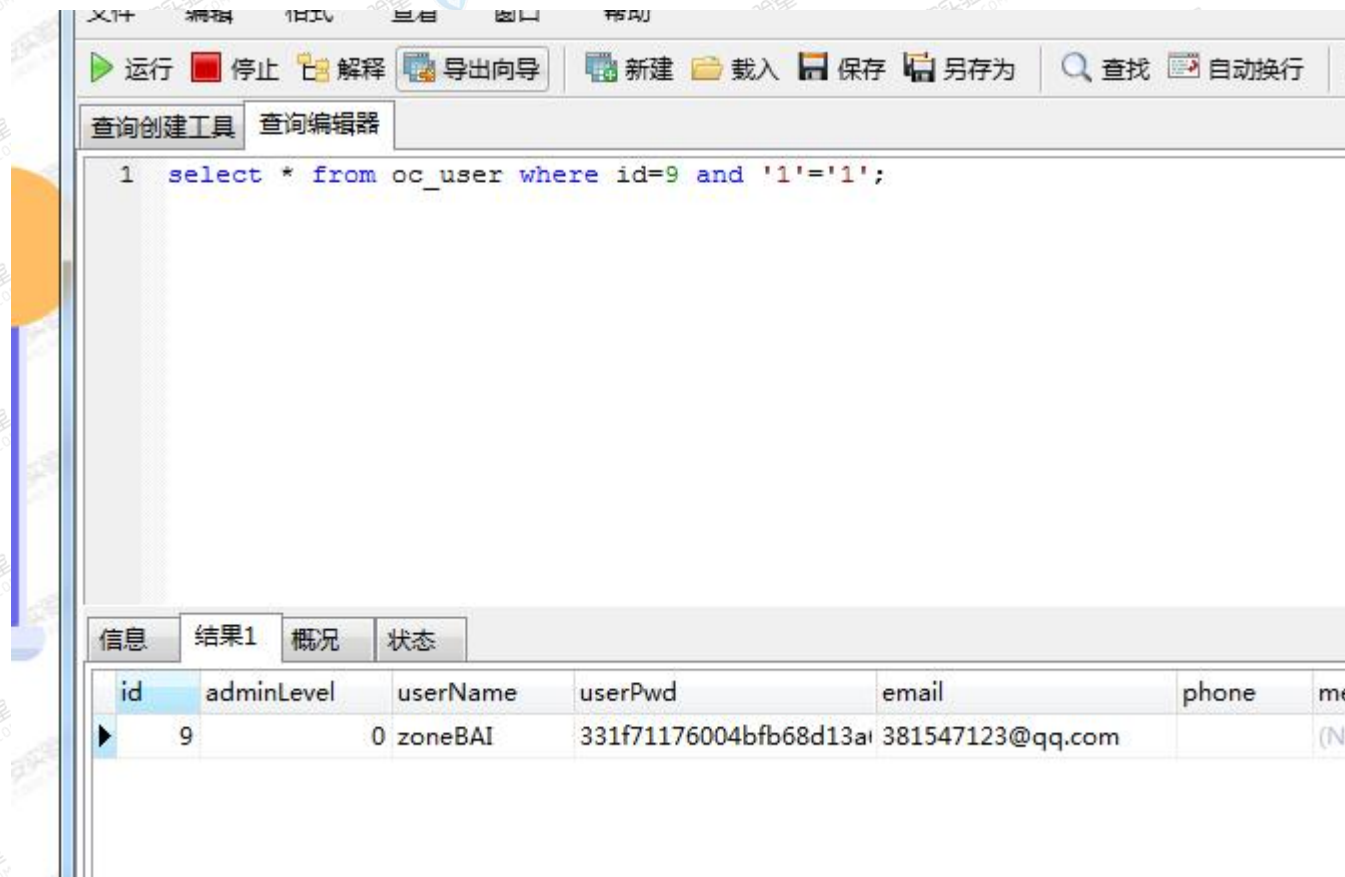


mysql里面常用的逻辑函数

and && 与
or || 或

真 and 真 真
真 and 假 假

真 or 假 真
假 or 假 假



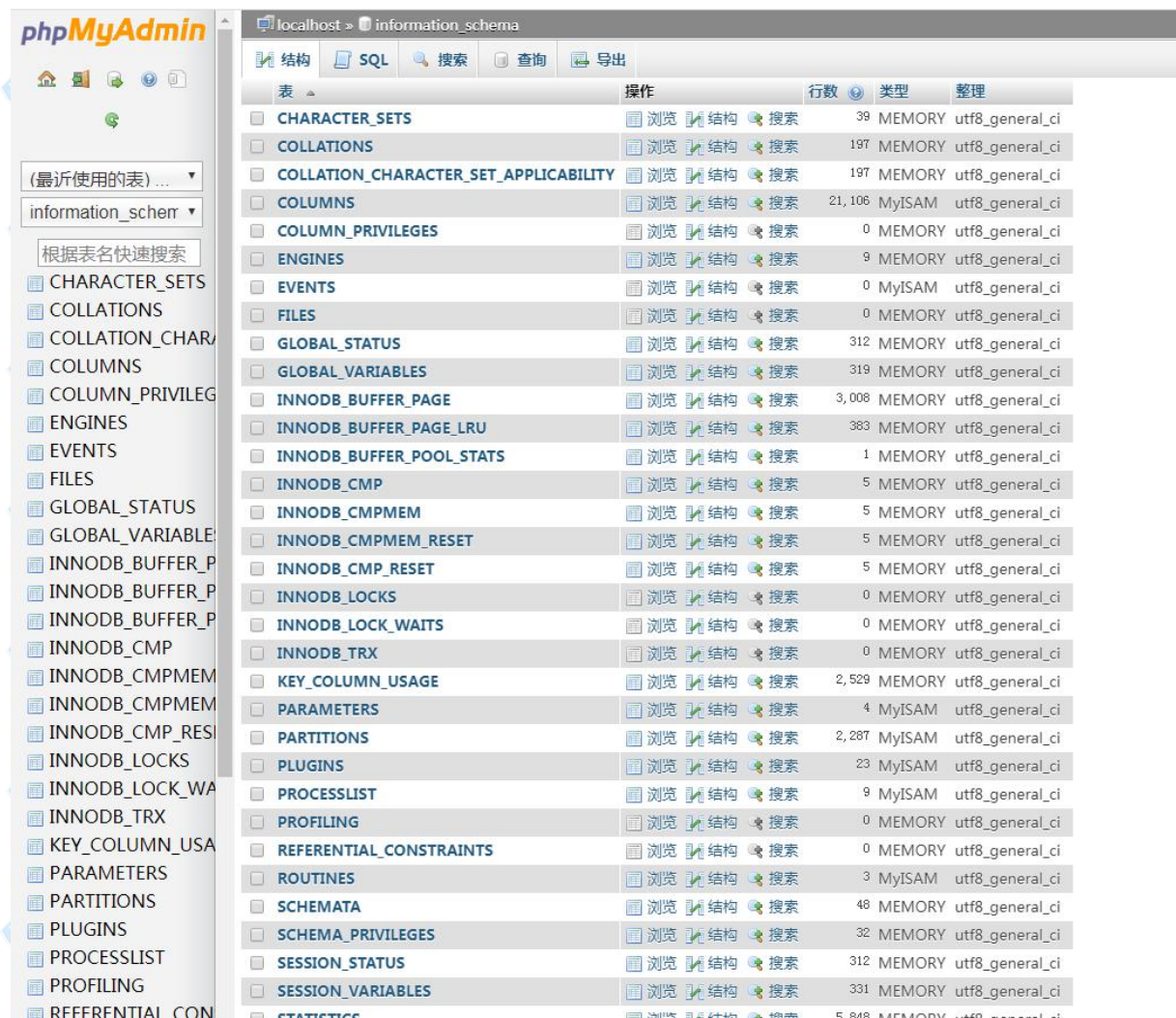


/02

Information_schema

Information_schema

Mysql 5.0以上, Mysql 自带了
Information_schema这个数据库
, 5.0以下是没有的



The screenshot shows the phpMyAdmin interface for the 'information_schema' database. The left sidebar lists various system tables, and the main panel displays a table of these tables with columns for name, operation, row count, type, and collation.

表	操作	行数	类型	整理
CHARACTER_SETS	浏览 结构 搜索	39	MEMORY	utf8_general_ci
COLLATIONS	浏览 结构 搜索	197	MEMORY	utf8_general_ci
COLLATION_CHARACTER_SET_APPLICABILITY	浏览 结构 搜索	197	MEMORY	utf8_general_ci
COLUMNS	浏览 结构 搜索	21,106	MyISAM	utf8_general_ci
COLUMN_PRIVILEGES	浏览 结构 搜索	0	MEMORY	utf8_general_ci
ENGINES	浏览 结构 搜索	9	MEMORY	utf8_general_ci
EVENTS	浏览 结构 搜索	0	MyISAM	utf8_general_ci
FILES	浏览 结构 搜索	0	MEMORY	utf8_general_ci
GLOBAL_STATUS	浏览 结构 搜索	312	MEMORY	utf8_general_ci
GLOBAL_VARIABLES	浏览 结构 搜索	319	MEMORY	utf8_general_ci
INNODB_BUFFER_PAGE	浏览 结构 搜索	3,008	MEMORY	utf8_general_ci
INNODB_BUFFER_PAGE_LRU	浏览 结构 搜索	383	MEMORY	utf8_general_ci
INNODB_BUFFER_POOL_STATS	浏览 结构 搜索	1	MEMORY	utf8_general_ci
INNODB_CMP	浏览 结构 搜索	5	MEMORY	utf8_general_ci
INNODB_CMPMEM	浏览 结构 搜索	5	MEMORY	utf8_general_ci
INNODB_CMPMEM_RESET	浏览 结构 搜索	5	MEMORY	utf8_general_ci
INNODB_CMP_RESET	浏览 结构 搜索	5	MEMORY	utf8_general_ci
INNODB_LOCKS	浏览 结构 搜索	0	MEMORY	utf8_general_ci
INNODB_LOCK_WAITS	浏览 结构 搜索	0	MEMORY	utf8_general_ci
INNODB_TRX	浏览 结构 搜索	0	MEMORY	utf8_general_ci
KEY_COLUMN_USAGE	浏览 结构 搜索	2,529	MEMORY	utf8_general_ci
PARAMETERS	浏览 结构 搜索	4	MyISAM	utf8_general_ci
PARTITIONS	浏览 结构 搜索	2,287	MyISAM	utf8_general_ci
PLUGINS	浏览 结构 搜索	23	MyISAM	utf8_general_ci
PROCESSLIST	浏览 结构 搜索	9	MyISAM	utf8_general_ci
PROFILING	浏览 结构 搜索	0	MEMORY	utf8_general_ci
REFERENTIAL_CONSTRAINTS	浏览 结构 搜索	0	MEMORY	utf8_general_ci
ROUTINES	浏览 结构 搜索	3	MyISAM	utf8_general_ci
SCHEMATA	浏览 结构 搜索	48	MEMORY	utf8_general_ci
SCHEMA_PRIVILEGES	浏览 结构 搜索	32	MEMORY	utf8_general_ci
SESSION_STATUS	浏览 结构 搜索	312	MEMORY	utf8_general_ci
SESSION_VARIABLES	浏览 结构 搜索	331	MEMORY	utf8_general_ci
STATISTICS	浏览 结构 搜索	5,848	MEMORY	utf8_general_ci

Information_schema

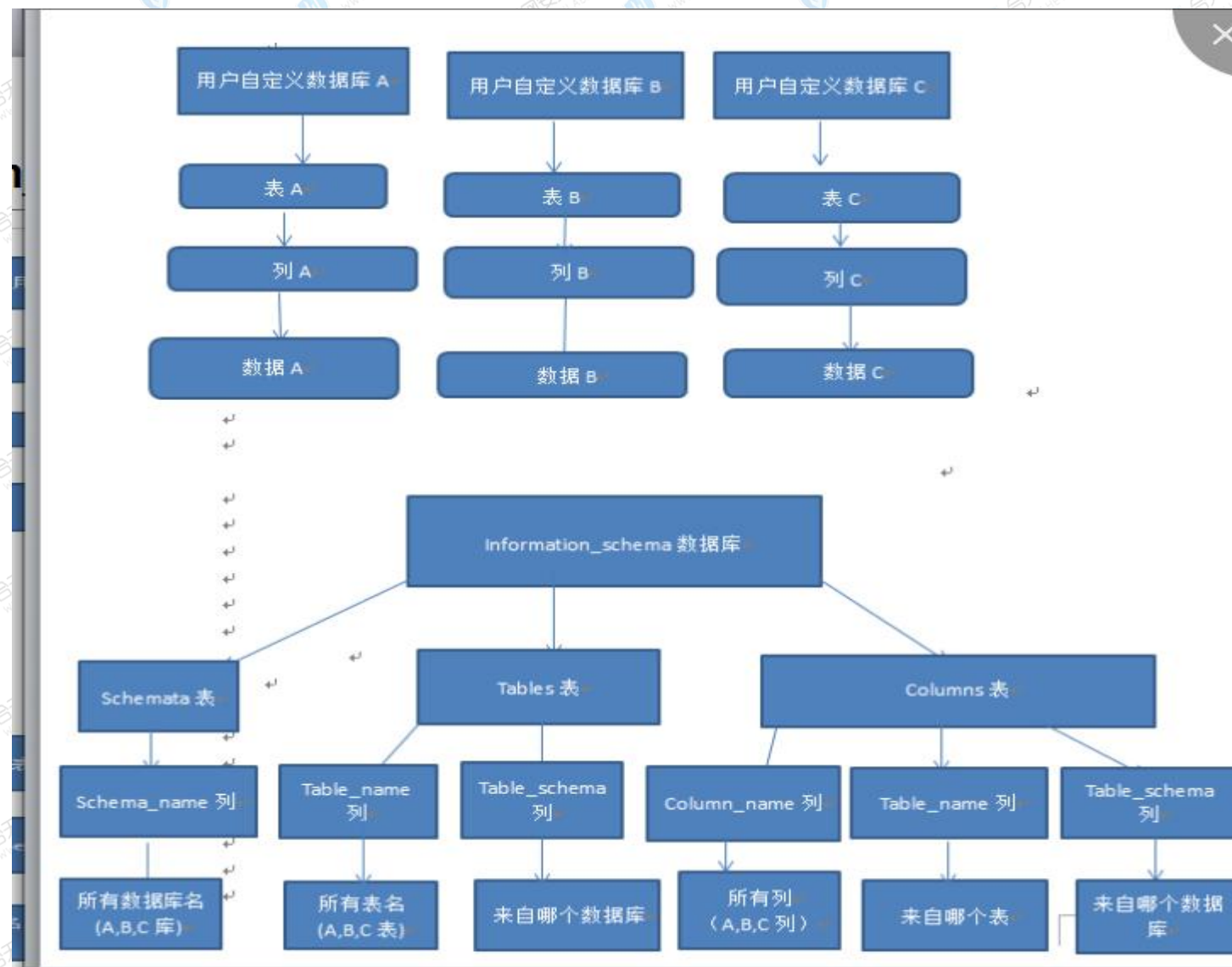
重点两个：

Information_schema.tables

所有表名

information_schema.columns

所有列名

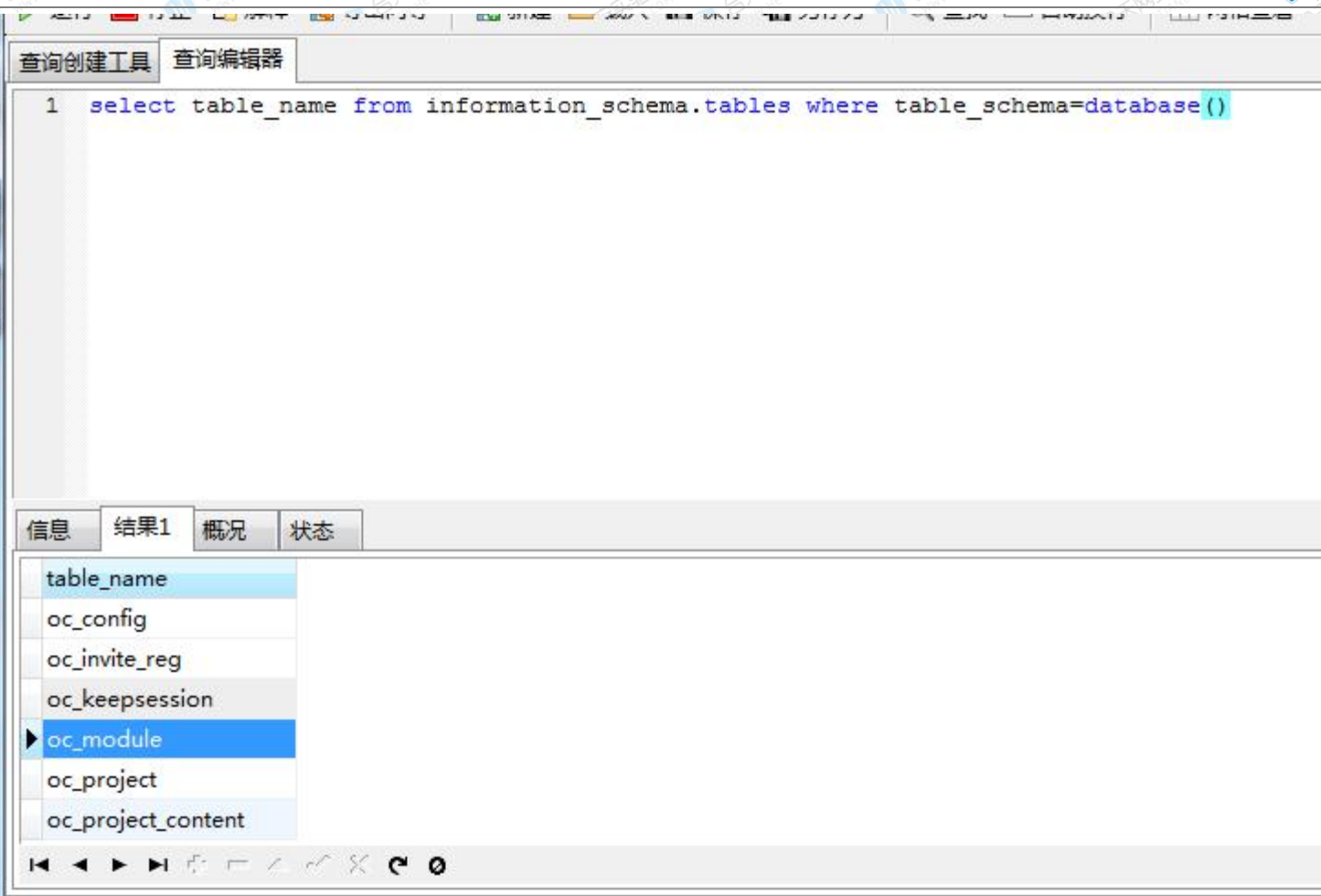
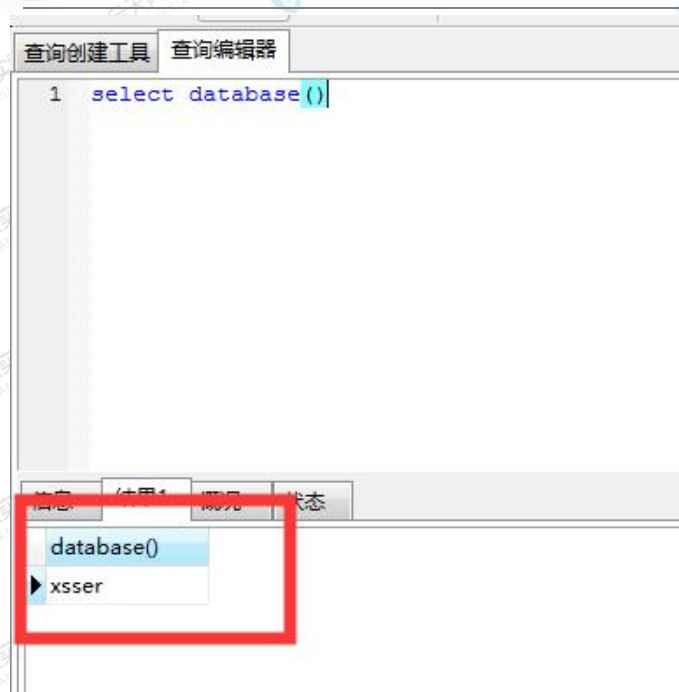




利用语句查询效果

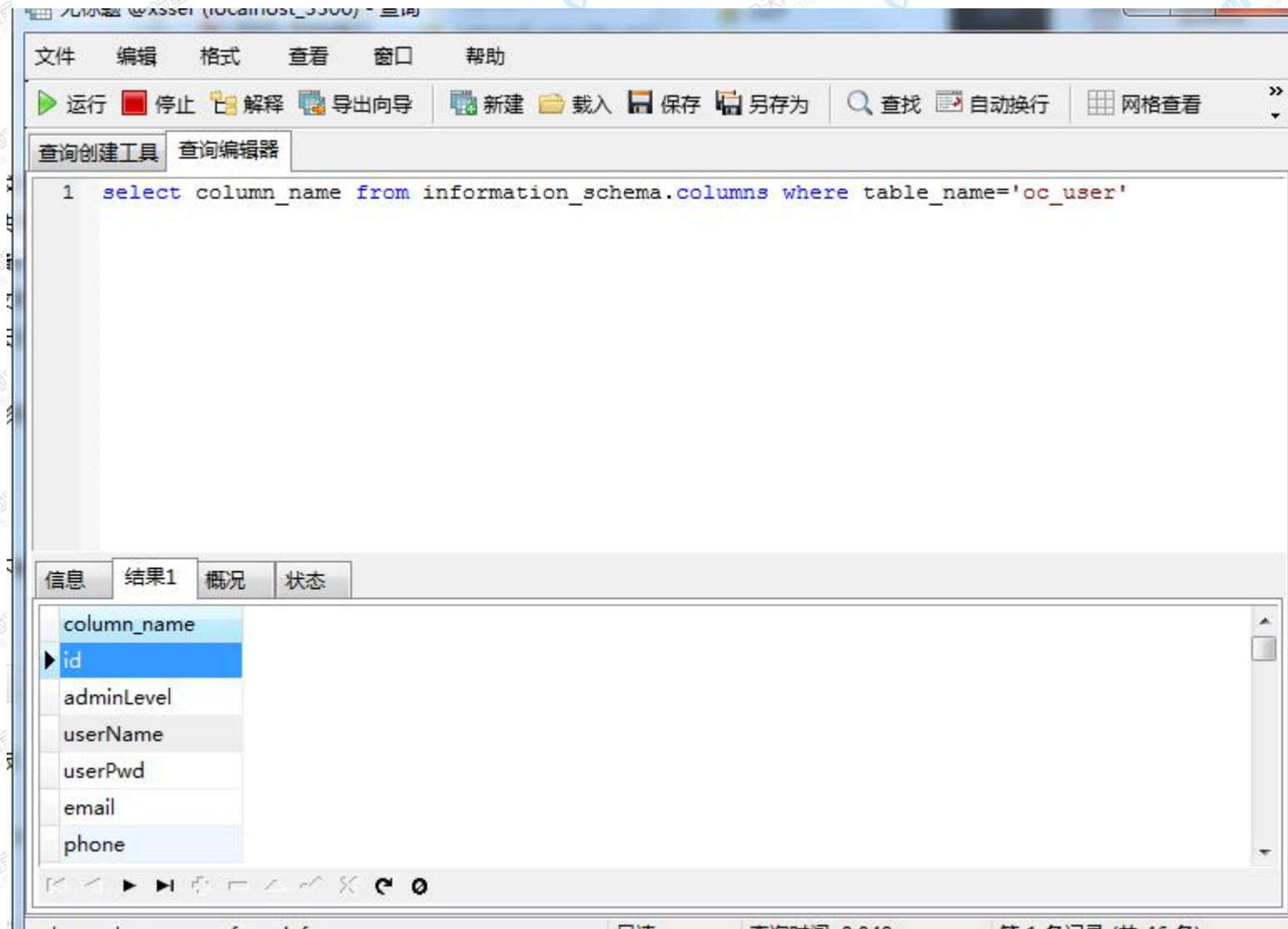
```
select database(); 当前所在的数据库  
select table_name from information_schema.tables  
where table_schema=database()  
查询当前数据库的表名  
select column_name from  
information_schema.columns where  
table_name='oc_user'
```


利用语句查询效果





利用语句查询效果





sql注入常用的语句

举例联合查询语句：union select UNION 操作符用于合并两个或多个 SELECT 语句的结果集

查询创建工具 查询编辑器

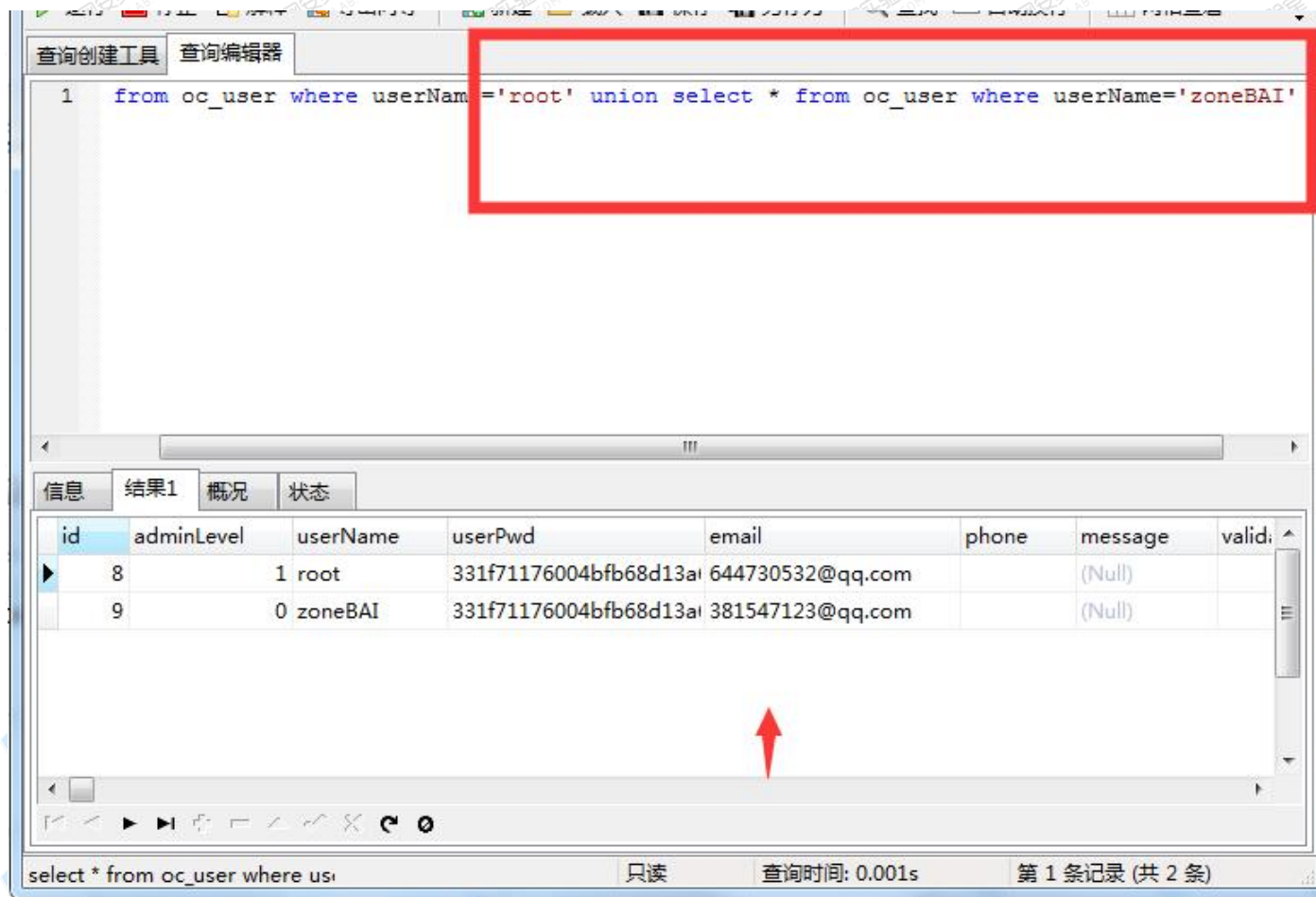
```
1 select * from oc_user where userName='root';
```

结果1

id	adminLevel	userName	userPwd	email	phone	message	valida
8	1	root	331f71176004bfb68d13a	644730532@qq.com		(Null)	

sql注入常用的语句

举例联合查询语句：union select UNION 操作符用于合并两个或多个 SELECT 语句的结果集



The screenshot shows a SQL query editor with a query window and a results window. The query window contains the following SQL statement:

```
1 from oc_user where userName='root' union select * from oc_user where userName='zoneBAI'
```

The results window displays the following table:

id	adminLevel	userName	userPwd	email	phone	message	valid
8	1	root	331f71176004bfb68d13a1	644730532@qq.com		(Null)	
9	0	zoneBAI	331f71176004bfb68d13a1	381547123@qq.com		(Null)	

The status bar at the bottom indicates the query time is 0.001s and the first record is displayed out of two records.



/03

其他数据库

SQL server, oracle、sybase、db2、access

常见的一般是

oracle 的增删改查

<https://www.cnblogs.com/garyzhuang/p/9670411.html>

SQL server

<https://blog.csdn.net/wujakf/article/details/78331663>

access

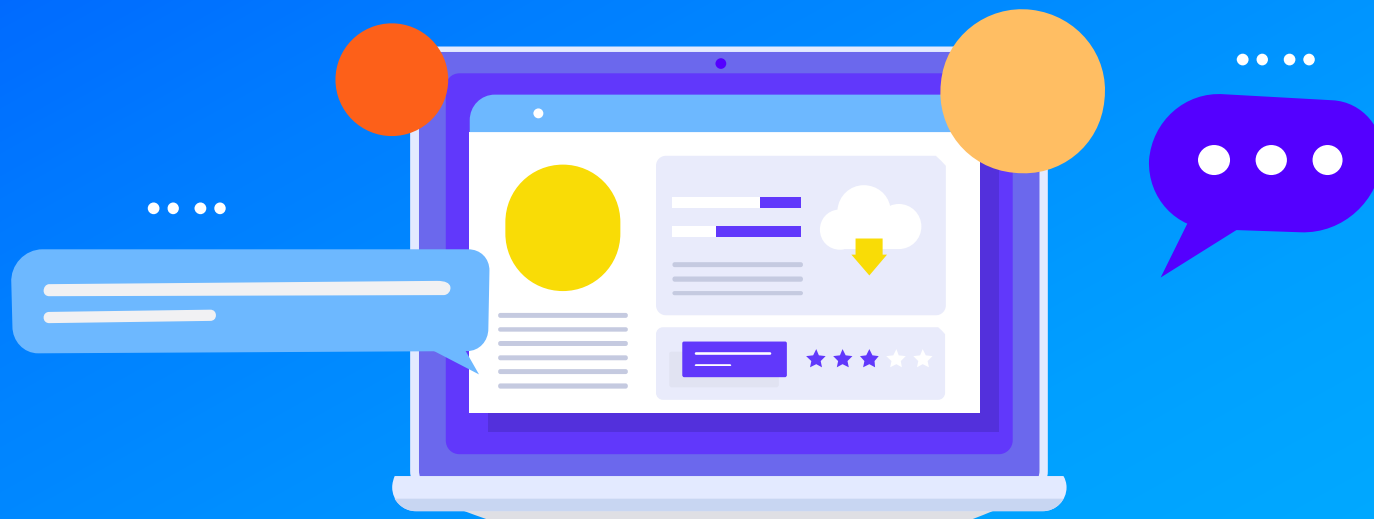
插入 : insert intotable1(field1,field2) values(value1,value2)

删除 : delete from table1where 范围

更新 : update table1 setfield1=value1 where

范围查找 : select * from table1

where field1 like ' %value1%'



感谢聆听

湖南合天智汇信息技术有限公司

www.hetianlab.com