

# 数据库查询 第一部分

基础查询词语

select

from

where

基本查询语句

查询参数指令

union、group by、order by、limit、and、or

常用函数

group\_concat()、database()、version()



重庆橙子科技

有的时候为了绕过waf防火墙会将同一条命令变形处理

## 基本查询语句

```
>select * from users where id=1;
```

#select+列名(\*代表所有) from+表名 where+条件语句

```
>select * from users where id in ('3');
```

#从users表格，查询所有包含id为3

重庆橙子科技

```
>select * from users where id=(select id from users where username=('admin'));
```

#子查询 优先执行 () 内查询语句

联合查询，可以将union看成and，作用是前后查询语句的结果连接起来(前提是两者查询出来列数相同，不同的话记得在后面补充)

# 查询参数指令

union

```
>select id from users union select email_id from emails;
```

#查询并合并数据显示

```
>select * from users where id=6 union select * from emails where id=6;
```

ERROR: have a different number of columns 联合注入前后表格列数必须相等

重庆橙子科技



填充列不需要管他里面的数据是多少，只需要知道他是增加列数用的

# 查询参数指令

union

```
>select id from users union select email_id from emails;
```

#查询并合并数据显示

```
>select * from users where id=6 union select * from emails where id=6;
```

ERROR: have a different number of columns 联合注入前后表格列数必须相等

```
>select * from users where id=6 union select *,3 from emails where id=6;
```

#3为填充列

重庆橙子科技

