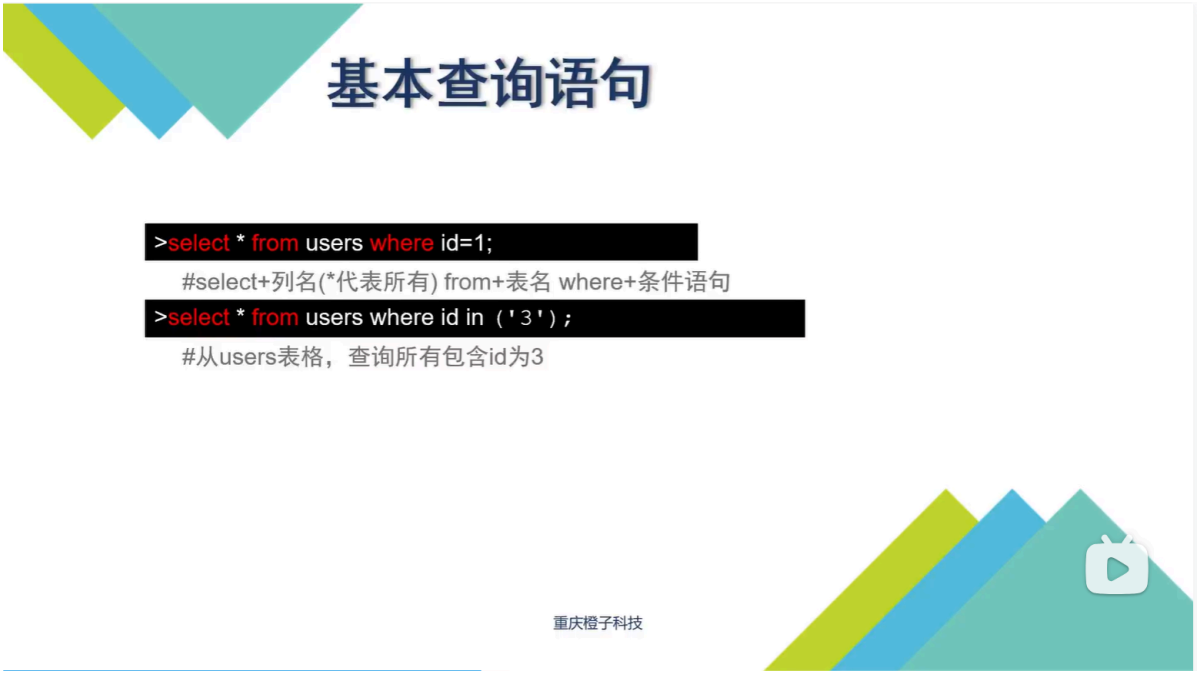
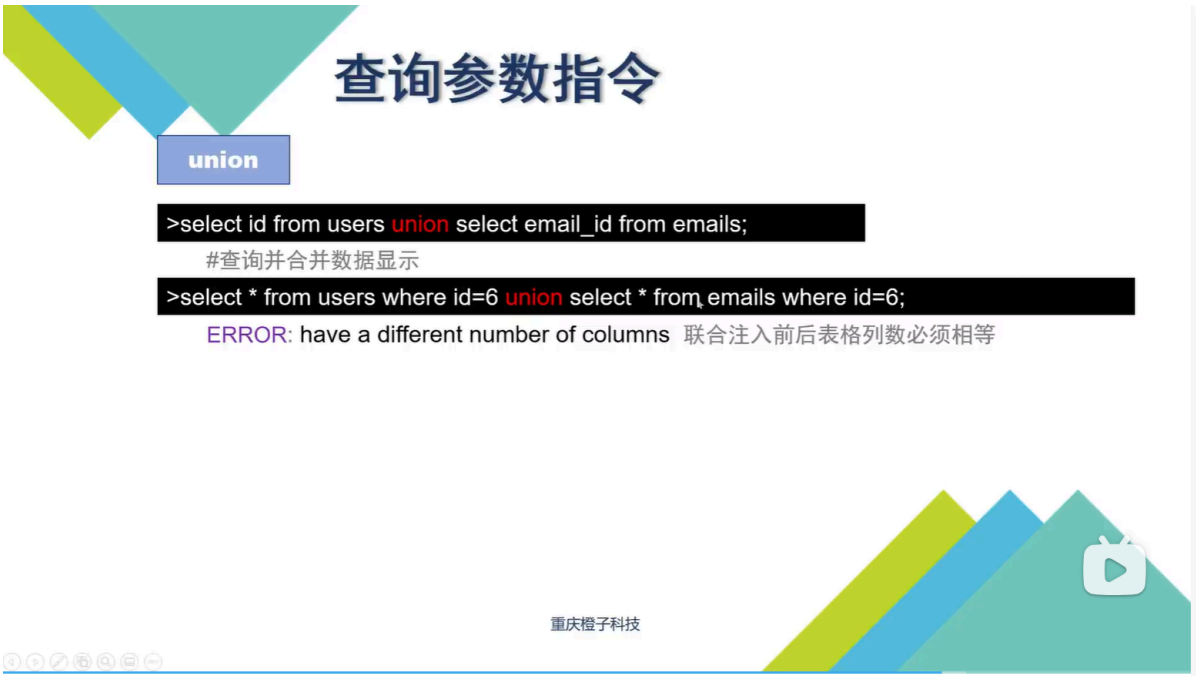
数据库查询 第一部分

有的时候为了绕过waf防火墙会将同一条命令变形处理




```
>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)



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