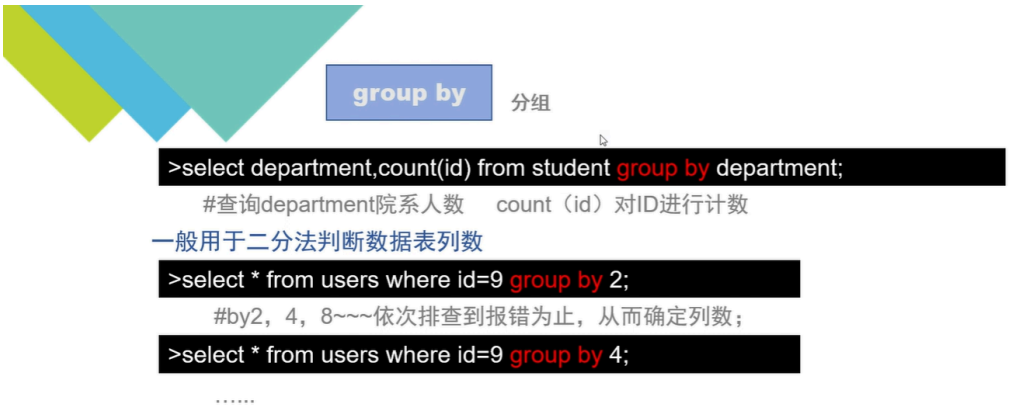
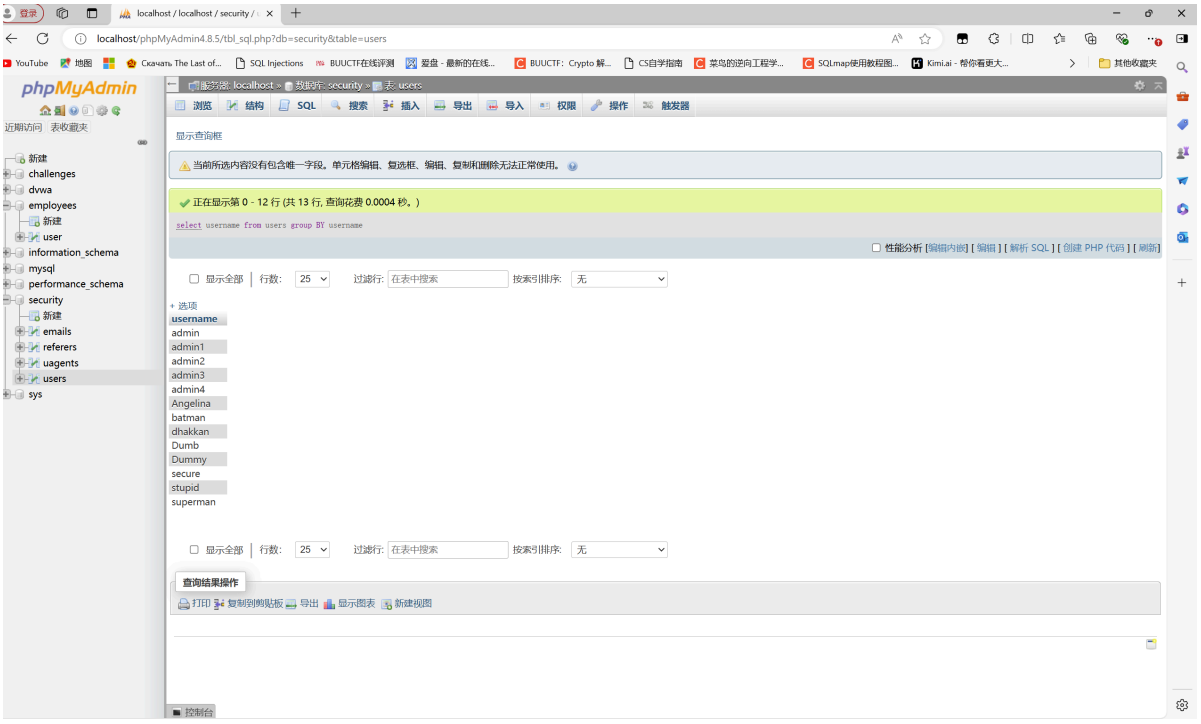
数据库查询第二部分

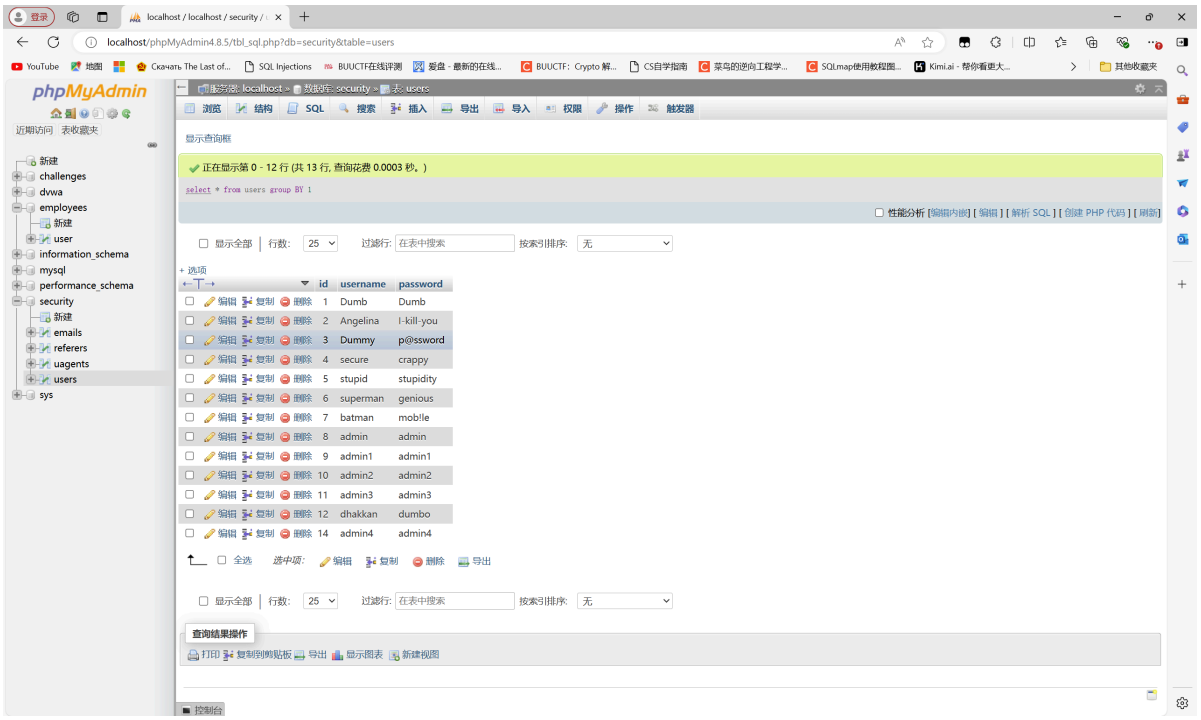
group by是用来分组的，也可以很好的进行判断列数，然后也可以很好的进行waf绕过(如果一个网站对order by判定严格的话我们就可以选用group by来绕过)



接下来详细讲解为什么group by能够通过分组来判断列数，`GROUP BY` 关键字后面跟着的列名用于指定数据库应该如何将数据分组，比如这里我们就对users表中的username以username进行分组，相同的放一起不同的分开放（这里全都不同）

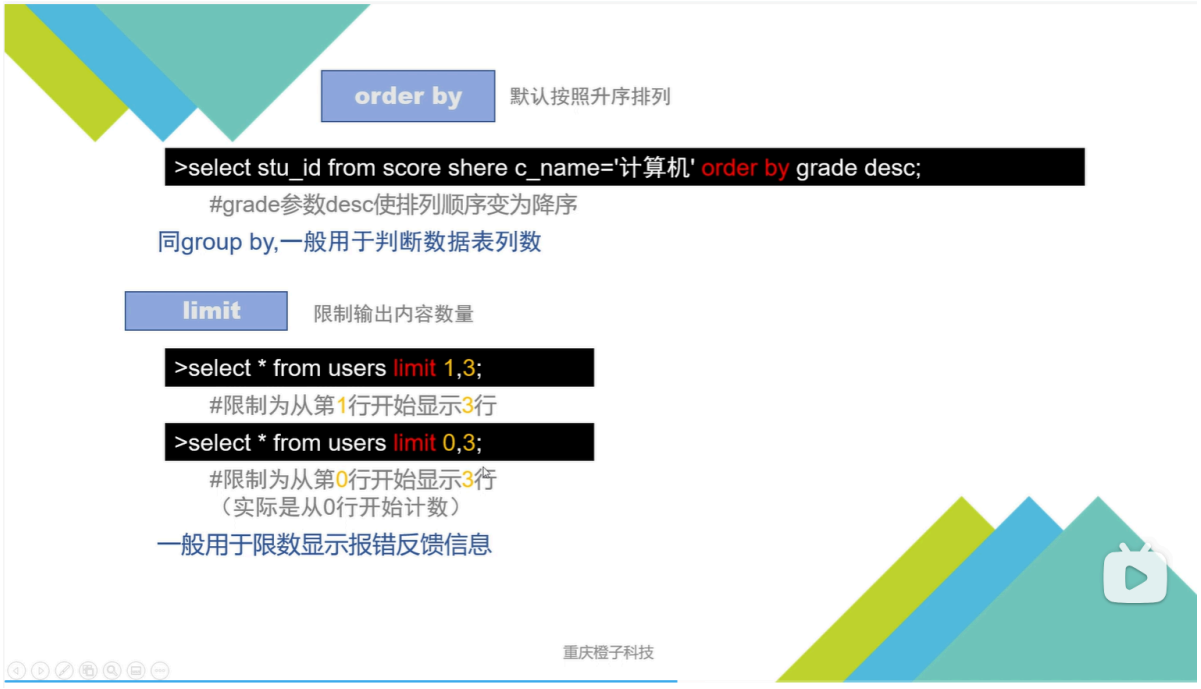


如果我们用select * from users group by 1，这里意思就是对整个users表进行分组且为一列，我们就不知道我们是要对哪个东西进行分类了（我们不知道这个表里有几列并且有啥），运行后如图所示

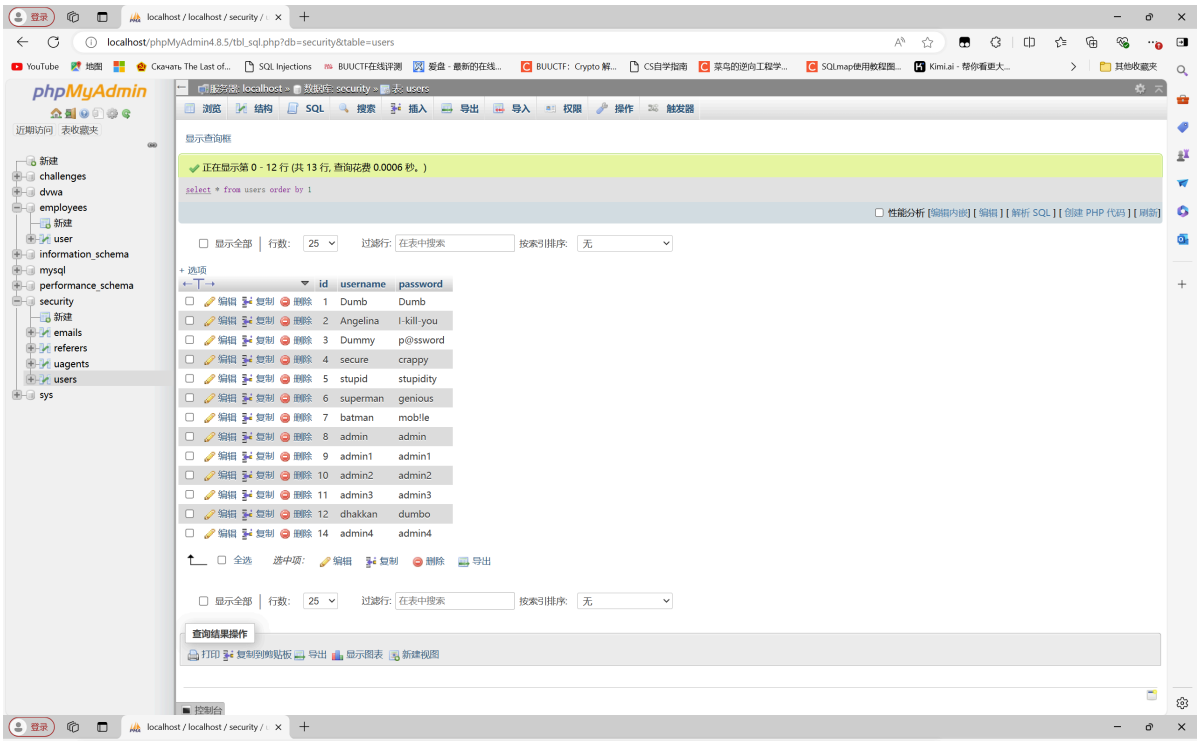


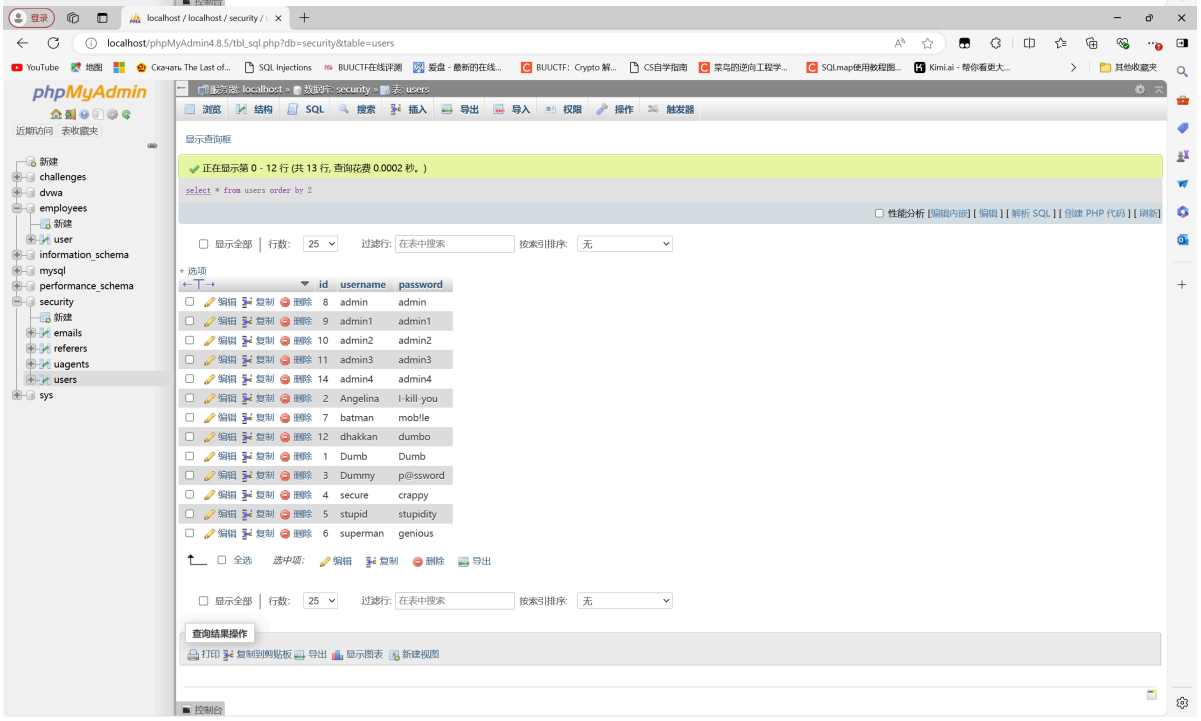
有结果说明该表至少有一列，接下来我们只要对这个表不停地进行不同列数分组，当报错无法分类的时候我们就可以知道这个表的列数是多少了。

接下来讲order by



order by的作用是对表中某一列的元素进行排序（具体某一列看order by后面加的字段）（默认升序）





使用limit限制字段时要注意limit是从0开始计数的，所以如果只回显第一行到第三行就要要写limit 0,2