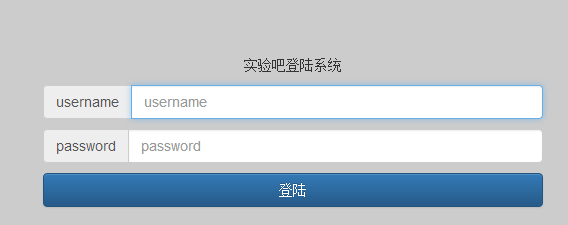
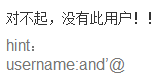
题目界面如下



首先使用手动拟态模糊测试尝试探测注释

使用测试语句 andor’@#



发现 or 和 # 被过滤，其余可被保留

偷笑，说好的都过滤呢

猜测程序中使用的sql语句

select ...from ....where username =' ' and password = ' '

构造

select ...from ....where username=''='' and password=''=''

即'=''