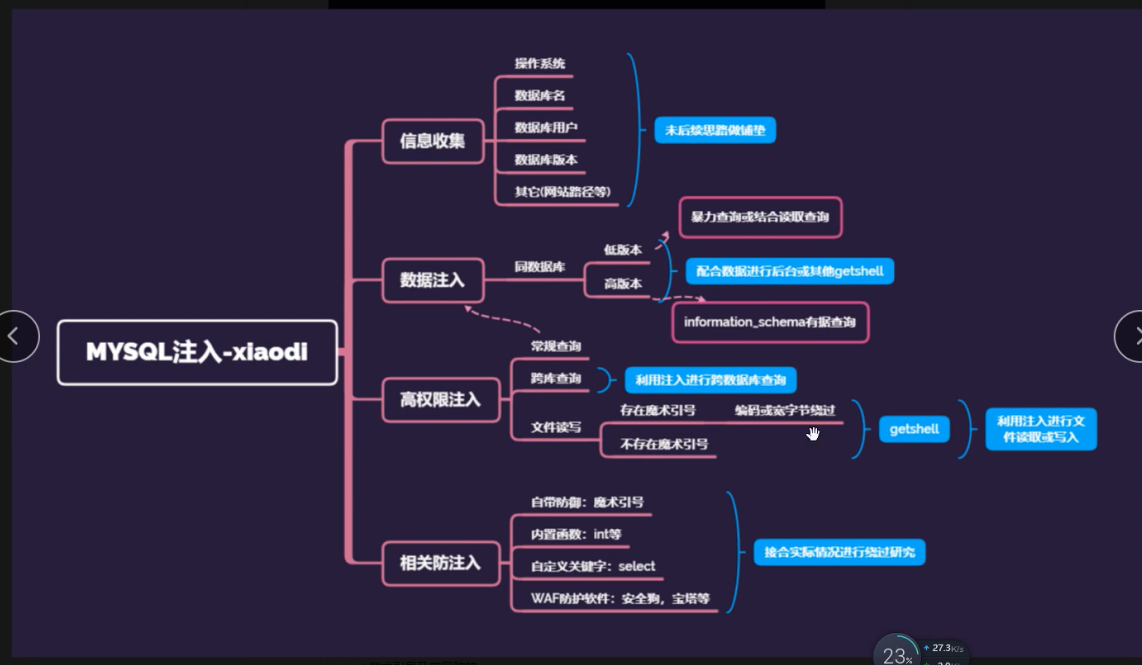
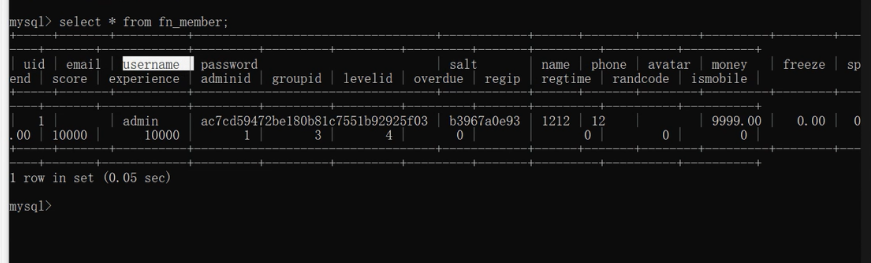
# 9.MYSQL注入

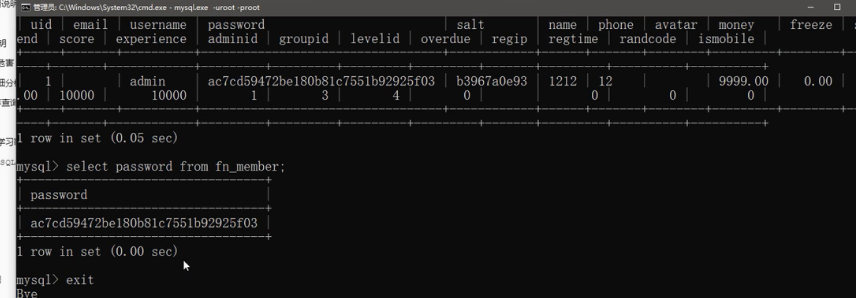
1. 思维导图



1. SQL注入语句
   1. 显示数据库
      1. show databases;
   2. 使用数据库
      1. use 数据库名;
   3. 查询数据表
      1. show tables;
   4. 查询列名
      1. select \* from 数据表名;
         1. 实例：



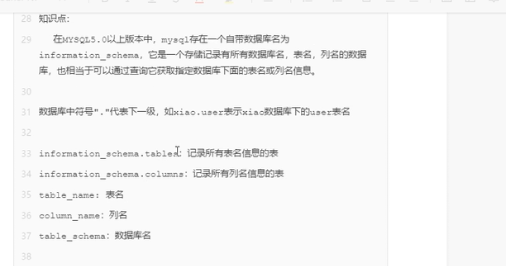
* + 1. select password from 数据库名;
       1. 实例：



1. 如何判断注入点
   1. 老方法：
      1. and 1=1 页面正确（与之前页面无区别）
      2. and 1=2 页面错误
   2. 新方法：
      1. SELECT \* FROM users WHERE id=1 LIMIT 0,1 正常
      2. SELECT \* FROM users WHERE id=1注入点xxx LIMIT 0,1 错误，说明带入数据库处理
      3. 出现404错误大概率没有注入
2. 注入步骤
   1. 判断注入
      1. 转到
   2. 猜解列名数量（字段数）order by x 错误与正确的正常值
      1. 在注入点后加入 union select 1,2,3,4
      2. 实例：



1. 信息收集
   1. 数据库版本
      1. version()
   2. 数据库名字
      1. database()
   3. 数据库用户
      1. user() root@localhost
   4. 操作系统
      1. @@version\_compile\_os
   5. 必要知识点
      1. 低版本猜解数据库名和表名，mysql5.0以上通过information——schema查询信息
      2. 数据库中“ . ”代表下一级



* 1. 实例：查询指定信息



1. 高权限注入
   1. 常规查询
   2. 跨库查询————利用注入进行跨数据库查询
   3. 文件读写————getshell————利用注入进行文件读取或写入
      1. 存在魔术引导
      2. 不存在魔术引导
2. 相关防注入————结合实际情况进行绕过研究
   1. 自带防御：魔术引号
   2. 内置函数：int等
   3. 自定义关键字：select
   4. WAF防护软件：安全狗，宝塔等