Atitit sql注入的防范

目录

[1.1. 检查数据类型 1](#_Toc22160)

[2. 有限操作DML 1](#_Toc23001)

[2.1. 限制执行函数黑名单机制 2](#_Toc18362)

[2.2. 限制执行系统sp 2](#_Toc17812)

[2.3. 限制数据查询语句类型，只能dql select 2](#_Toc10626)

[2.4. 编码字符串内容 2](#_Toc2422)

[2.5. 拆分操作ast 2](#_Toc6609)

[2.6. Update 条件 一点要有具体id并且是自己的数据，只限一条 2](#_Toc7629)

[2.7. update 和 delete 不提供批量更新和删除， 2](#_Toc24988)

[3. 有限数据 3](#_Toc6679)

[3.1. 使用视图隐藏敏感数据 密码等 3](#_Toc19298)

[3.2. 适当的登录权限id检查 3](#_Toc13310)

[3.3. 登陆后隐藏user id参数 3](#_Toc7840)

[3.4. 只允许读取自己的数据检查，所以数据必须要有userid后端隐藏提供 3](#_Toc25478)

[3.5. 限制数据库类型白名单 3](#_Toc28643)

[3.6. 数据表黑白名单 3](#_Toc15699)

[3.7. 条件查询只能and not。。禁止or条件， 3](#_Toc12891)

[3.8. 多条件必须拆分开，方便参数检查参数绑定，防止注入操作 3](#_Toc23662)

[3.9. 参数绑定可以避免SQL注入 3](#_Toc7967)

[4. 资源性能限制 3](#_Toc16125)

[4.1. 没有翻页参数的可以拒绝 或者强制少量数据默认1000 4](#_Toc26501)

[4.2. 运行之前可以expain一下 4](#_Toc21942)

[5. 数据库操作语句类型（DQL、DML、DDL、DCL） 4](#_Toc4918)

[5.1. 1. 数据查询语言DQL 4](#_Toc17450)

[5.2. 2 .数据操纵语言DML 更新 4](#_Toc12264)

[5.3. 3. 数据定义语言DDL 建表语句 5](#_Toc15)

[5.4. 4. 数据控制语言DCL 5](#_Toc26597)

[6. 结构化查询语言包含6个部分： 7](#_Toc12340)

[7. ref 7](#_Toc32197)

## 检查数据类型

# 有限操作DML

## 限制执行函数黑名单机制

白名单

database()等

## 限制执行系统sp

## 限制数据查询语句类型，只能dql select

过滤select into 语句禁止 ，select merger等会影响数据结果的禁止。。

## 编码字符串内容

特殊符号’ -- #等符号检查

## 拆分操作ast

这样方便检查内容。。Or and not 等操作拆分，不要字符串模式容易混淆

## Update 条件 一点要有具体id并且是自己的数据，只限一条

Insert 适当放开

Delete 一点要有具体id并且是自己的数据，只限一条

Where 条件值允许and

隐藏式userid

## update 和 delete 不提供批量更新和删除，

只能根据 objectId（where objectId=xxx）和其他条件来更新或者删除某个文档

# 有限数据

## 使用视图隐藏敏感数据 密码等

## 适当的登录权限id检查

## 登陆后隐藏user id参数

## 只允许读取自己的数据检查，所以数据必须要有userid后端隐藏提供

## 限制数据库类型白名单

防止查询info\_schema 元数据库等

## 数据表黑白名单

## 条件查询只能and not。。禁止or条件，

## 多条件必须拆分开，方便参数检查参数绑定，防止注入操作

## 参数绑定可以避免SQL注入

# 资源性能限制

## 没有翻页参数的可以拒绝 或者强制少量数据默认1000

## 运行之前可以expain一下

# [数据库操作语句类型（DQL、DML、DDL、DCL）](https://www.cnblogs.com/tanjiyuan/p/11049458.html)

[IMG_256](https://www.cnblogs.com/tanjiyuan/p/javascript:void(0);)

数据库操作语句类型（DQL、DML、DDL、DCL）简介

SQL语言共分为四大类：数据查询语言DQL，数据操纵语言DML，数据定义语言DDL，数据控制语言DCL。

## 1. 数据查询语言DQL

数据查询语言DQL基本结构是由SELECT子句，FROM子句，WHERE

子句组成的查询块：

SELECT <字段名表>

FROM <表或视图名>

WHERE <查询条件>

## 2 .数据操纵语言DML 更新

数据操纵语言DML主要有三种形式：

1) 插入：INSERT

2) 更新：UPDATE

3) 删除：DELETE

## 3. 数据定义语言DDL 建表语句

数据定义语言DDL用来创建数据库中的各种对象-----表、视图、

索引、同义词、聚簇等如：

CREATE TABLE/VIEW/INDEX/SYN/CLUSTER

表 | 视图 | 索引 | 同义词 | 簇

说明：DDL操作是隐性提交的！不能rollback

## 4. 数据控制语言DCL

数据控制语言DCL用来授予或回收访问数据库的某种特权，并控制

数据库操纵事务发生的时间及效果，对数据库实行监视等。如：

1) GRANT：授权。

2) ROLLBACK [WORK] TO [SAVEPOINT]：回退到某一点。

回滚---ROLLBACK

回滚命令使数据库状态回到上次最后提交的状态。其格式为：

SQL>ROLLBACK;

EG:

-- 执行表数据闪回（回滚）申明

ALTER TABLE FCPARDATA ENABLE ROW MOVEMENT;

-- 正式数据回滚

FLASHBACK TABLE FCPARDATA TO TIMESTAMP TO\_TIMESTAMP('2019-06-19 08:40:00','YYYY-MM-DD HH24:MI:SS');

3) COMMIT [WORK]：提交。

在数据库的插入、删除和修改操作时，只有当事务在提交到数据库时才算完成。在事务提交前，只有操作数据库的这个人才能有权看到所做的事情，别人只有在最后提交完成后才可以看到。提交数据有三种类型：显式提交、隐式提交及自动提交。下面分别说明这三种类型。

(1) 显式提交

用COMMIT命令直接完成的提交为显式提交。其格式为：

SQL>COMMIT；

(2) 隐式提交

用SQL命令间接完成的提交为隐式提交。这些命令是：

ALTER，AUDIT，COMMENT，CONNECT，CREATE，DISCONNECT，DROP，

EXIT，GRANT，NOAUDIT，QUIT，REVOKE，RENAME。

(3) 自动提交

若把AUTOCOMMIT设置为ON，则在插入、修改、删除语句执行后，

系统将自动进行提交，这就是自动提交。其格式为：

SQL>SET AUTOCOMMIT ON；

# 结构化查询语言包含6个部分：

1、数据查询语言（[DQL](https://baike.baidu.com/item/DQL" \t "https://baike.baidu.com/item/%E7%BB%93%E6%9E%84%E5%8C%96%E6%9F%A5%E8%AF%A2%E8%AF%AD%E8%A8%80/_blank):Data Query Language）：其语句，也称为“数据检索[语句](https://baike.baidu.com/item/%E8%AF%AD%E5%8F%A5" \t "https://baike.baidu.com/item/%E7%BB%93%E6%9E%84%E5%8C%96%E6%9F%A5%E8%AF%A2%E8%AF%AD%E8%A8%80/_blank)”，用以从表中获得数据，确定数据怎样在应用程序给出。保留字[SELECT](https://baike.baidu.com/item/SELECT/10735068" \t "https://baike.baidu.com/item/%E7%BB%93%E6%9E%84%E5%8C%96%E6%9F%A5%E8%AF%A2%E8%AF%AD%E8%A8%80/_blank)是DQL（也是所有SQL）用得最多的动词，其他DQL常用的保留字有WHERE，ORDER BY，GROUP BY和HAVING。这些DQL保留字常与其它类型的SQL语句一起使用。 [4] 

2、[数据操作语言](https://baike.baidu.com/item/%E6%95%B0%E6%8D%AE%E6%93%8D%E4%BD%9C%E8%AF%AD%E8%A8%80" \t "https://baike.baidu.com/item/%E7%BB%93%E6%9E%84%E5%8C%96%E6%9F%A5%E8%AF%A2%E8%AF%AD%E8%A8%80/_blank)（DML：Data Manipulation Language）：其语句包括动词[INSERT](https://baike.baidu.com/item/INSERT" \t "https://baike.baidu.com/item/%E7%BB%93%E6%9E%84%E5%8C%96%E6%9F%A5%E8%AF%A2%E8%AF%AD%E8%A8%80/_blank)、[UPDATE](https://baike.baidu.com/item/UPDATE" \t "https://baike.baidu.com/item/%E7%BB%93%E6%9E%84%E5%8C%96%E6%9F%A5%E8%AF%A2%E8%AF%AD%E8%A8%80/_blank)和[DELETE](https://baike.baidu.com/item/DELETE" \t "https://baike.baidu.com/item/%E7%BB%93%E6%9E%84%E5%8C%96%E6%9F%A5%E8%AF%A2%E8%AF%AD%E8%A8%80/_blank)。它们分别用于添加、修改和删除。 [4]

3、事务控制语言（TCL）：它的语句能确保被DML语句影响的表的所有行及时得以更新。包括COMMIT（提交）命令、SAVEPOINT（保存点）命令、ROLLBACK（回滚）命令。

4、[数据控制语言](https://baike.baidu.com/item/%E6%95%B0%E6%8D%AE%E6%8E%A7%E5%88%B6%E8%AF%AD%E8%A8%80" \t "https://baike.baidu.com/item/%E7%BB%93%E6%9E%84%E5%8C%96%E6%9F%A5%E8%AF%A2%E8%AF%AD%E8%A8%80/_blank)（DCL）：它的语句通过GRANT或REVOKE实现权限控制，确定单个用户和用户组对[数据库对象](https://baike.baidu.com/item/%E6%95%B0%E6%8D%AE%E5%BA%93%E5%AF%B9%E8%B1%A1" \t "https://baike.baidu.com/item/%E7%BB%93%E6%9E%84%E5%8C%96%E6%9F%A5%E8%AF%A2%E8%AF%AD%E8%A8%80/_blank)的访问。某些RDBMS可用GRANT或REVOKE控制对[表单](https://baike.baidu.com/item/%E8%A1%A8%E5%8D%95" \t "https://baike.baidu.com/item/%E7%BB%93%E6%9E%84%E5%8C%96%E6%9F%A5%E8%AF%A2%E8%AF%AD%E8%A8%80/_blank)个列的访问。 [4]

5、数据定义语言（[DDL](https://baike.baidu.com/item/DDL/21997" \t "https://baike.baidu.com/item/%E7%BB%93%E6%9E%84%E5%8C%96%E6%9F%A5%E8%AF%A2%E8%AF%AD%E8%A8%80/_blank)）：其语句包括动词CREATE,ALTER和DROP。在数据库中创建新表或修改、删除表（CREAT TABLE 或 DROP TABLE）；为表加入索引等。 [4]

6、指针控制语言（CCL）：它的语句，像DECLARE CURSOR，FETCH INTO和UPDATE WHERE CURRENT用于对一个或多个表单独行的操作。 [4]

# ref

SQL注入——入门篇 - 姑苏城外的江枫\_博客 - CSDN博客.html