Atitit sql注入的防范

目录

[1.1. 检查数据类型 1](#_Toc4418)

[1.2. 使用视图隐藏敏感数据 密码等 1](#_Toc4454)

[1.3. 没有翻页参数的可以拒绝 或者强制少量数据默认1000 1](#_Toc25900)

[1.4. 运行之前可以expain一下 1](#_Toc12279)

[1.5. 限制数据查询语句类型，只能dql select 1](#_Toc29998)

[1.6. 限制数据库类型白名单 1](#_Toc3312)

[1.7. 数据表黑白名单 2](#_Toc18149)

[1.8. 限制执行函数黑名单机制 2](#_Toc12038)

[1.9. 限制执行系统sp 2](#_Toc10132)

[1.10. 适当的登录权限id检查 2](#_Toc4681)

[1.11. 只允许读取自己的数据检查 2](#_Toc24444)

[2. 有限操作DML 2](#_Toc28833)

[3. 数据库操作语句类型（DQL、DML、DDL、DCL） 2](#_Toc12518)

[3.1. 1. 数据查询语言DQL 2](#_Toc15147)

[3.2. 2 .数据操纵语言DML 更新 3](#_Toc2190)

[3.3. 3. 数据定义语言DDL 建表语句 3](#_Toc13183)

[3.4. 4. 数据控制语言DCL 3](#_Toc12878)

## 检查数据类型

## 使用视图隐藏敏感数据 密码等

## 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

## 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。。

## 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

## 限制执行函数黑名单机制

白名单

database()等

## 限制执行系统sp

## 适当的登录权限id检查

## 只允许读取自己的数据检查

# 有限操作DML

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

# [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；

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