浙江大学

数据库系统实验报告

作业名称：SQL 安全性

姓　　名：谢集

学　　号：3220103501

电子邮箱：1436572990@qq.com

联系电话：13567793981

指导老师：孙建伶

2024 年 4 月 7 日

实验 4　SQL 安全性

一、实验目的

1. 熟悉通过 SQL 进行数据安全性控制的方法。

二、实验环境

操作系统：Windows11 22H2。

数据库管理系统：MySQL

三、实验流程

1、表权限管理

打开命令行，输入 mysql -u sanaka -p。输入密码，完成 Lab1 中所创建账号的登录。继续使用 Lab3 中关于部门管理的数据库，包含两个表：

1、部门（departments）

- d_id: 部门的 ID，我将它设为主键。
- name: 部门的名字，我令它不能为 NULL 或空字符串。

2、雇员（employee）

- e_id: 雇员的 ID，我将它设为主键。
- name: 雇员的名字，我令它不能为 NULL 或空字符串。
- d_id: 雇员所属部门的 ID，我将它设为外键，引用部门表格中的信息。
- sex: 雇员的性别，我在它上面设置 check，检查其是否属于’F’或者’M’。

创建代码如下：

```
create table departments (
    d_id int primary key,
    name varchar(255) not null,
    check (name != '')
);

create table employees (
    e_id int primary key,
    name varchar(255) not null,
    sex varchar(1) not null,
    d_id int,
    foreign key (d_id) references departments(d_id)
        on delete set null
        on update cascade,
    check (name != ''),
    check (sex in ('F', 'M'))
);
```

使用命令 `create user 'Lab4manager'@'%' identified by 'sanaka';` 创建一个对所有主机开放权限（%）的用户 Lab4manager，密码为 *sanaka*。然后我们使用这个用户登录：

```
C:\Users\xieji>mysql -u Lab4manager -p
Enter password: ******
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 12
Server version: 8.0.36 MySQL Community Server - GPL

Copyright (c) 2000, 2024, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
```

但是我们无法使用数据库 Lab3，这是因为我们还没有权限访问 sanaka 账户创建的数据库。

```
mysql> use Lab3;
ERROR 1044 (42000): Access denied for user 'Lab4manager'@'%' to database 'lab3'
```

我们登录回 sanaka 账户，使用 grant 命令赋予 Lab4manager 权限。

```
mysql> grant select on Lab3.employees to 'Lab4manager'@'%';
Query OK, 0 rows affected (0.01 sec)

mysql> show grants for 'Lab4manager'@'%';
+-----------------------------------------------------------+
| Grants for Lab4manager@%                                  |
+-----------------------------------------------------------+
| GRANT USAGE ON *.* TO `Lab4manager`@`%`                   |
| GRANT SELECT ON `lab3`.`employees` TO `Lab4manager`@`%`   |
+-----------------------------------------------------------+
2 rows in set (0.00 sec)
```

我们还可以通过看表格 mysql.table_priv 来看所有的权限：

```
mysql> select * from mysql.tables_priv;
+-----------+-------+---------------+------------+-----------------+---------------------+------------+-------------+
| Host      | Db    | User          | Table_name | Grantor         | Timestamp           | Table_priv | Column_priv |
+-----------+-------+---------------+------------+-----------------+---------------------+------------+-------------+
| %         | lab3  | Lab4manager   | employees  | sanaka@localhost | 2024-04-07 17:33:40 | Select     |             |
| localhost | mysql | mysql.session | user       | boot@           | 2024-02-27 09:08:02 | Select     |             |
| localhost | sys   | mysql.sys     | sys_config | root@localhost  | 2024-02-27 09:08:02 | Select     |             |
+-----------+-------+---------------+------------+-----------------+---------------------+------------+-------------+
3 rows in set (0.00 sec)
```

再次登录 Lab4manager 账号，看自己的权限如何：

```
mysql> select * from employees;
+------+------+-----+------+
| e_id | name | sex | d_id |
+------+------+-----+------+
|    1 | xj   | M   |    1 |
|    2 | pxy  | F   |    1 |
|    3 | cdj  | M   |    2 |
|    4 | yzy  | M   |    2 |
+------+------+-----+------+
4 rows in set (0.00 sec)

mysql> select * from departments;
ERROR 1142 (42000): SELECT command denied to user 'Lab4manager'@'localhost' for table 'departments'
```

可以发现现在我们的账号拥有了 select employees 表格的权限，但仍然没有 select departments 表格的权限。我们使用 revoke 命令：revoke select on Lab3.employees from 'Lab4manager'@'%'; 就可以收回权限。

2、表创建权限

使用 sanaka 用户赋予表创建权限：grant create on Lab3.* to 'Lab4manager'@'%'; 然后我们使用 Lab4manager 用户建表：

```
mysql> create table test(A int);
Query OK, 0 rows affected (0.02 sec)

mysql> show tables;
+----------------+
| Tables_in_lab3 |
+----------------+
| departments    |
| employees      |
| test           |
+----------------+
3 rows in set (0.02 sec)

mysql> insert into test(A) value(123);
ERROR 1142 (42000): INSERT command denied to user 'Lab4manager'@'localhost' for table 'test'
```

但可以发现，我们仍然没有 insert 的权限。

3、视图查询权限

```
mysql> create view view1 as select name from employees;
Query OK, 0 rows affected (0.02 sec)

mysql> grant select on Lab3.view1 to 'Lab4manager'@'%';
Query OK, 0 rows affected (0.01 sec)
```

创建视图，使用 grant 语句赋予查询其的权限。登录 Lab4manager 查看如下；

```
mysql> select * from view1;
+------+
| name |
+------+
| xj   |
| pxy  |
| cdj  |
| yzy  |
+------+
4 rows in set (0.00 sec)
```

四、遇到的问题及解决方法

在登录新用户的时候，我不知道密码是什么，后来我才意识到 identified 后面就是密码，这暴露了我的基础较为薄弱，需要巩固加强。

五、总结

通过本次实验，我通过实践学习掌握了 MySQL 的数据安全控制方法，包括用户权限管理、表权限细节、以及视图权限的设置与查询。这一过程不仅增强了我对 SQL 安全控制的理解，还提高了我的问题解决能力，并强化了数据安全在数据库管理中的重要性。这次实验不仅提升了我的技术技能，也加深了我对于实施高安全标准在数据库设计和管理中的认识，为我的未来工作奠定了坚实的基础。