**Практическая работа №18**

**Пользователи и привилегии**

В этой главе, вы обучитесь работе с привилегиямии пользователями.

SQL используется обычно в средах, которые требуют распознавания пользователей и различия между различными пользователями систем. Вообще говоря, администраторы баз данных, сами создают пользователей и дают им привилегии. С другой стороны, пользователи, которые создают таблицы, сами имеют права на управление этими таблицами.

*Привилегии* — это то, что определяет, может ли указанный пользователь выполнить данную команду. Имеется несколько типов привилегий, соответствующих нескольким типам операций. Привилегии даются и отменяются двумя командами SQL: —**GRANT** (*ДОПУСК*) и **REVOKE** (*ОТМЕНА*). Эта практическая работа покажет вам, как эти команды используются.

**Предоставление привилегий**

Каждый пользователь в SQL базе данных имеет набор привилегий.

Это то, что пользователю разрешается делать (возможно это файл регистрации, который может рассматриваться как минимальная привилегия). Эти привилегии могут изменяться со временем — новые добавляться, старые удаляться. Некоторые из этих привилегий определены в ANSI SQL, но имеются и дополнительные привилегии, которые являются также необходимыми. SQL привилегии, как определено ANSI, не достаточны в большинстве ситуаций реальной жизни. С другой стороны, типы привилегий, которые необходимы, могут видоизменяться с видом системы, которую вы используете, относительно которой ANSI не может дать никаких рекомендаций. Привилегии, которые не являются частью стандарта SQL, могут использовать похожий синтаксис и не полностью совпадающий со стандартом.

Привилегии объекта связаны одновременно и с пользователями, и с таблицами. То есть, привилегия дается определенному пользователю в указанной таблице, или базовой таблице или представлении. Вы должны помнить, что пользователь, создавший таблицу (любого вида), является владельцем этой таблицы. Это означает, что пользователь имеет все привилегии в этой таблице и может передавать привилегии другим пользователям в этой таблице.

Привилегии, которые можно назначить пользователю

|  |  |
| --- | --- |
| SELECT | Пользователь с этой привилегией может выполнять запросы в таблице. |
| INSERT | Пользователь с этой привилегией может выполнять команду INSERT в таблице. |
| UPDATE | Пользователь с этой привилегией может выполнять команду UPDATE на таблице. Вы можете ограничить эту привилегию для определенных столбцов таблицы. |
| DELETE | Пользователь с этой привилегией может выполнять команду DELETE в таблице. |
| REFERENCES | Пользователь с этой привилегией может определить внешний ключ, который использует один или более столбцов этой таблицы, как родительский ключ. Вы можете ограничить эту привилегию для определенных столбцов. |

**Практическая часть:**

**Часть 1 Создание пользователя**

Создадим пользователя с именем newuser:

CREATEUSER 'newuser'@'localhost' IDENTIFIEDBY '12345';

К сожалению, на данном этапе пользователь "newuser" не имеет прав делать что-либо с базами данных.

Таким образом, первое, что нам необходимо сделать, это предоставить пользователю доступ к информации, которая ему потребуется:

GRANT ALL PRIVILEGES ON \* . \* TO 'newuser'@'localhost';

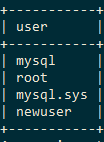
Звездочки в этой команде задают базу и таблицу, соответственно, к которым у пользователя будет доступ. Конкретно эта команда позволяет пользователю читать, редактировать, выполнять любые действия над всеми базами данных и таблицами.

Поле завершения настройки прав доступа новых пользователей, убедитесь, что вы обновили все права доступа:

FLUSH PRIVILEGES;

Проверим, если ли пользователь в системе:

SELECT `user` FROM `mysql` . `user`;



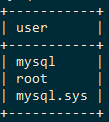
В списке пользователей появился newuser.

Теперь удалим пользователя из MySQL:

DROP USER 'newuser'@'localhost';

Ещё раз проверим список пользователей и убедимся, что пользователь удалён:

SELECT `user` FROM `mysql` . `user`;



**Часть 2 Работа с привилегиями**

Создадим пользователя:

CREATE USER 'newuser'@'localhost' IDENTIFIED BY 'password';

Так как мы уже знаем, что пользователь на данном этапе не имеет прав, то дадим пользователю права на выборку из базы gruber:

GRANT SELECT ON gruber.\* TO 'newuser'@'localhost';

FLUSH PRIVILEGES;

Посмотрим список прав для ‘newuser’

SHOW GRANTS FOR 'newuser'@'localhost';

Если там есть строка –

GRANT SELECT ON `gruber`.\*TO 'newuser'@'localhost'

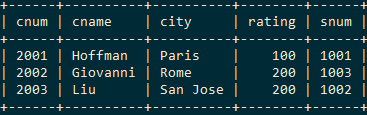
– то всё сделано правильно

Теперь зайдем под новым пользователем и посмотрим можем ли мы делать выборку из баз данных:

mysql -u newuser –p

use gruber;

SELECT \* FROM customers LIMIT 3;



Теперь изменим стоку в таблице:

UPDATE customers SET cname="HOST" WHERE cnum='2001';

MySQLвыдастошибку: UPDATE command denied to user 'newuser'@'localhost' for table 'customers'

Это вполне нормально, потому, что пользователь newuser может делать только выборку из таблицы.

Усложним задачу. Дадим ‘newuser’ право изменять данные в таблице orders базы данных gruber. Для этого нужно вернуться обратно под root :

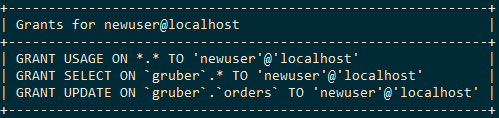
mysql -uroot –p

GRANT UPDATE ON gruber.orders TO 'newuser'@'localhost';

FLUSH PRIVILEGES;

Посмотрим, что получилось:

SHOW GRANTS FOR 'newuser'@'localhost';



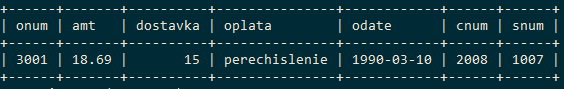
Возвращаемся под пользователя ‘newuser’:

mysql -u newuser –p

use gruber;

Попробуем сделать SELECT для таблицы orders:

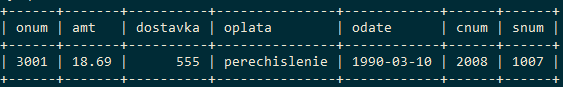
SELECT \* FROM orders LIMIT 1;



SELECT выдаёт результат. Теперь проработаем UPDATE:

UPDATE orders SET dostavka='555' WHERE onum='3001';

SELECT \* FROM orders WHERE onum='3001';



Всё работает. Поле dostavka изменилось с 15 до 555.

Сделаем изменения в таблицу customers:

UPDATE customers SET city='hacked' AND rating='-500' AND cname='NONAME';

MySQL выдаст ошибку:

ERROR 1142 (42000): UPDATE command denied to user 'newuser'@'localhost' for table 'customers'.

Если вы получили эту ошибку, то значит все хорошо.

**Часть 3 Удаление прав пользователям**

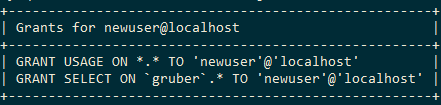
Удалим право на UPDATE таблице orders;

REVOKE UPDATE ON gruber.orders FROM 'newuser'@'localhost';

FLUSH PRIVILEGES;

Посмотрим права пользователя:

SHOW GRANTS FOR 'newuser'@'localhost';



Теперь зайдем и проверим права:

mysql -u newuser–p

use gruber;

UPDATE orders SET dostavka='15' WHERE onum='3001';

Получим ошибку:

ERROR 1142 (42000): UPDATE command denied to user 'newuser'@'localhost' for table 'orders'

Это значит что ‘newuser’ не имеет прав на редактирование и мы правильно удалили права

Удалите самостоятельно пользователя ‘newuser’.

Поздравляем! Вы научились создавать пользователей и давать права.

**Задания:**

1. Создать пользователя под именем ‘gruber\_user’ и паролем ‘12345’
2. Дать права на выборку из таблицы orders и salespeople.
3. Сделать выборку из таблицы salespeople
4. Дать право на вставку значений в таблицу orders
5. Вставить строку в таблицу orders
6. Удалить право делать выборку из таблицы orders
7. Дать пользователю право на обновление таблицы customers
8. Убрать право на обновление таблицы customers;
9. Удалить пользователя ‘gruber\_user’