8. 사용자 계정 및 권한

데이터베이스 보호

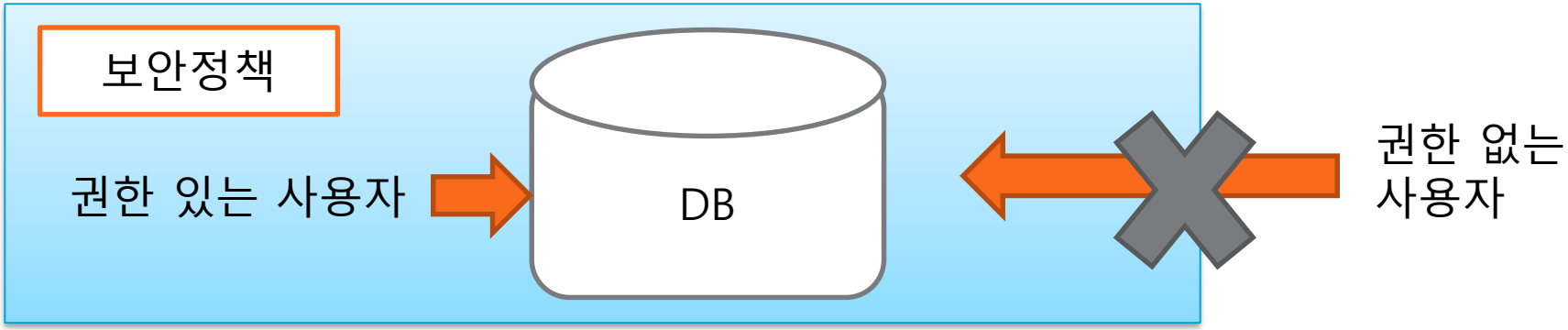
가상 뉴스

00고등학교의 홈페이지 데이터베이스가 해킹되어 학생들의 정보가 유출되었다고 합니다.

학생들의 개인정보 유출로 많은 피해가 예상됩니다.

:

힘들게 설계한 데이터베이스가 외부로 유출된다면 엄청난 피해 예상



데이터베이스 사용자 권한 설정

- 데이터베이스는 **여러 사용자들이 공유**하여 사용한다.
- 각 사용자에게 데이터베이스를 다룰 수 있는 모든 권한을 주면 데이터베이스의 보호에 문제가 발생한다.
- 따라서 **데이터베이스관리자(DBA)**는 각 사용자(계정)에게 작업을 위해 필요한 데이터베이스, 테이블에 대한 **최소한의 권한을 설정**해 주어야 한다.

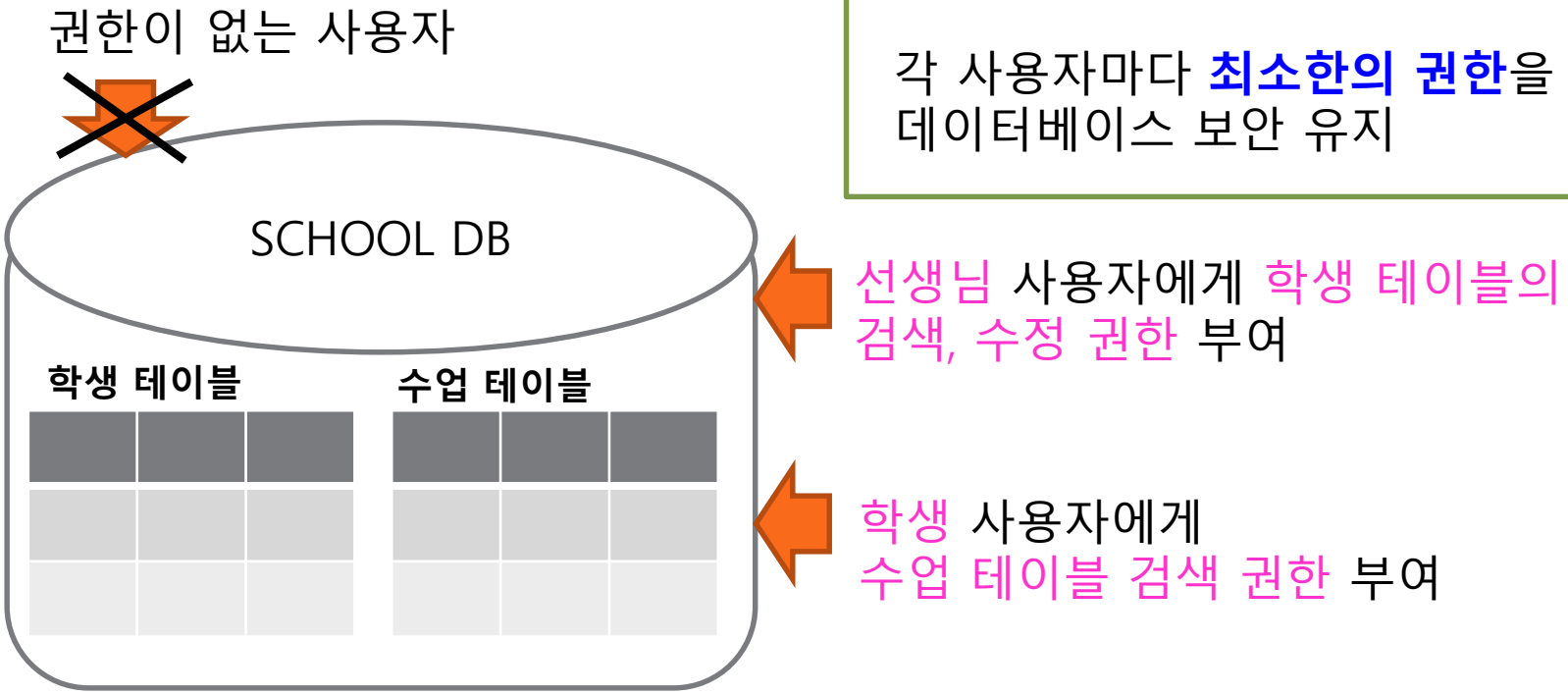
데이터베이스 권한

DBA(DataBase Administrator) : 데이터베이스를 관리 하는 역할

데이터베이스 보안

모두가 데이터베이스에 접근, 수정 등이 가능하다면 보안상 큰 문제

각 사용자마다 **최소한의 권한**을 주어 데이터베이스 보안 유지



데이터베이스 계정 및 권한 정보 검색

- **mysql 데이터베이스**의 **user 테이블이** 계정과 권한 정보를 가지고 있다.
- **user 테이블**의 컬럼(필드) 정보를 확인한다.

MariaDB[mysql]>desc user; // user 테이블에 어떤 항목(필드)이 있는지 보여줌

```
MariaDB [mysql]> desc user;
+------------------------+-----------------------+------+-----+----------+-------+
| Field                  | Type                  | Null | Key | Default  | Extra |
+------------------------+-----------------------+------+-----+----------+-------+
| Host                   | char(60)              | NO   |     |          |       |
| User                   | char(80)              | NO   |     |          |       |
| Password               | longtext              | YES  |     | NULL     |       |
| Select_priv            | varchar(1)            | YES  |     | NULL     |       |
| Insert_priv            | varchar(1)            | YES  |     | NULL     |       |
| Update_priv            | varchar(1)            | YES  |     | NULL     |       |
| Delete_priv            | varchar(1)            | YES  |     | NULL     |       |
| Create_priv            | varchar(1)            | YES  |     | NULL     |       |
| Drop_priv              | varchar(1)            | YES  |     | NULL     |       |
| Reload_priv            | varchar(1)            | YES  |     | NULL     |       |
| Shutdown_priv          | varchar(1)            | YES  |     | NULL     |       |
| Process_priv           | varchar(1)            | YES  |     | NULL     |       |
| File_priv              | varchar(1)            | YES  |     | NULL     |       |
| Grant_priv             | varchar(1)            | YES  |     | NULL     |       |
| References_priv        | varchar(1)            | YES  |     | NULL     |       |
| Index_priv             | varchar(1)            | YES  |     | NULL     |       |
| Alter_priv             | varchar(1)            | YES  |     | NULL     |       |
| Show_db_priv           | varchar(1)            | YES  |     | NULL     |       |
| Super_priv             | varchar(1)            | YES  |     | NULL     |       |
| Create_tmp_table_priv  | varchar(1)            | YES  |     | NULL     |       |
| Lock_tables_priv       | varchar(1)            | YES  |     | NULL     |       |
```

데이터베이스 계정 및 권한 정보 검색

- mysql 데이터베이스의 user 테이블을 통해 정의된 계정이 있는지 확인한다.

MariaDB>select host, user from user;

```
MariaDB [mysql]> select host, user from user;
+-----------+-------+
| Host      | User  |
+-----------+-------+
| 127.0.0.1 | root  |
| ::1       | root  |
| heesugi   | root  |
| localhost | root  |
| localhost | test1 |
+-----------+-------+
5 rows in set (0.034 sec)
```

SELECT host, user from user;

사용자 계정 만들기 – CREATE USER

CREATE USER '아이디'@'호스트' **IDENTIFIED BY** '비밀번호';

'stu1'@'localhost' 계정 생성 //localhost만 접속 가능(DB가 있는 컴에서만)

//* 인 경우 모든 컴퓨터에서 접속 가능

◆ 계정에 대한 정보는 **mysql** DB의 **user** 테이블에 있음.

```
MariaDB [mysql]> create user 'stu1'@'localhost' identified by 'pass1111';
Query OK, 0 rows affected (0.002 sec)
```

```
MariaDB [mysql]> select host, user ,password from user;
+-----------+-------+-------------------------------------------+
| Host      | User  | Password                                  |
+-----------+-------+-------------------------------------------+
| localhost | root  | *A4B6157319038724E3560894F7F932C8886EBFCF |
| heesugi   | root  | *A4B6157319038724E3560894F7F932C8886EBFCF |
| 127.0.0.1 | root  | *A4B6157319038724E3560894F7F932C8886EBFCF |
| ::1       | root  | *A4B6157319038724E3560894F7F932C8886EBFCF |
| localhost | test1 | *A4B6157319038724E3560894F7F932C8886EBFCF |
| localhost | stu1  | *5D65F9BBA3717C3C9846AFD2DD067B7A98A6308F |
+-----------+-------+-------------------------------------------+
6 rows in set (0.001 sec)
```

아이디 : stu1
비밀번호 : pass1111
현재 컴에서만 접속 가능
으로 사용자계정 생성함

Select문으로 계정이 만들어졌는지 확인한다.

'' 주의 해서 만들기. '아이디@호스트'로 하면 '' 안이 모두 아이디가 됨.

사용자 계정의 권한 확인하기

SHOW GRANTS [FOR 사용자]

현재 사용자에게 부여된 권한을 확인하기

```
MariaDB [mysql]> SHOW GRANTS;
+-----------------------------------------------------------------------------------------------------------------------------------------------------+
| Grants for root@localhost                                                                                                                           |
+-----------------------------------------------------------------------------------------------------------------------------------------------------+
| GRANT ALL PRIVILEGES ON *.* TO 'root'@'localhost' IDENTIFIED BY PASSWORD '*A4B6157319038724E3560894F7F932C8886EBFCF' WITH GRANT OPTION              |
| GRANT PROXY ON ''@'%' TO 'root'@'localhost' WITH GRANT OPTION                                                                                       |
+-----------------------------------------------------------------------------------------------------------------------------------------------------+
2 rows in set (0.002 sec)
```

다른 사용자에게 부여된 권한을 확인하기

```
MariaDB [mysql]> SHOW GRANTS FOR stu1@localhost;
+-----------------------------------------------------------------------------------------------------------------------------------------------------+
| Grants for stu1@localhost                                                                                                                           |
+-----------------------------------------------------------------------------------------------------------------------------------------------------+
| GRANT USAGE ON *.* TO 'stu1'@'localhost' IDENTIFIED BY PASSWORD '*5D65F9BBA3717C3C9846AFD2DD067B7A98A6308F'                                         |
| GRANT SELECT ON `test`.* TO 'stu1'@'localhost'                                                                                                      |
+-----------------------------------------------------------------------------------------------------------------------------------------------------+
2 rows in set (0.001 sec)
```

사용자 계정에 권한 설정 - GRANT

특정 객체에 대한 **CRUD(Create/Retrieve/Update/Delete)** 권한 설정

GRANT 권한[권한 리스트] ***ON*** *객체(DB명.table명)* **TO** 계정

- 객체와 권한의 종류

권한	객체
all [privileges]	Database Table View Index 등
select, update, insert, delete, create, alter, drop, Index 등	

어떤 사용자가 어떤 객체에 대해 어떤 권한을 가지는지 정의 하는 게 매우 중요

➡ 계정 하나하나에 권한을 주는 일은 쉽지 않다.

⬇

역할을 정의(그룹으로 묶음)하여 권한을 부여하기도 한다.

사용자 계정에 권한 설정

Grant all on *.* to 'stu1'@'localhost';

- stu1에게 모든 DB, 모든table에 대해 모든 권한 부여.
  단, stu1은 **localhost에서만 접속** 가능

Grant all on com_1.* to 'stu1'@'localhost';

- stu1에게 com_1 데이터베이스의 모든 테이블에 대해 모든 권한 부여
  단, stu1은 **localhost에서만 접속** 가능

Grant SELECT, INSERT on SCHOOL.STUDENT to 'stu2'@'*'

- stu2에게 SCHOOL 데이터베이스의 STUDENT 테이블에 대해
  SELECT, INSERT 권한을 부여. 단, stu2는 어떤 컴퓨터에서도 접속 가능

Grant update on SCHOOL.CIRCLE to 'stu2'@'localhost';

- stu2에게 SCHOOL 데이터베이스의 CIRCLE 테이블에 대해 UPDATE 권한을
  부여. 단, **stu2는 localhost에서만 접속** 가능

사용자 계정에 대한 권한 삭제 - REVOKE

특정 객체에 대한 권한 삭제

REVOKE 권한[권한 리스트] ***ON*** *객체(DB명.table명)* **FROM** 계정

Revoke all on *.* from 'stu1'@'localhost';

- **stu1의 모든 DB와 모든테이블**의 **모든 권한**을 삭제, stu1은 **로컬 컴**에서만 접속

Revoke SELECT, INSERT on SCHOOL.STUDENT from 'stu2'@'*'

- **stu2의 SCHOOL 데이터베이스의 STUDENT 테이블**의 **SELECT, INSERT 권한**을 삭제. 이때 stu2는 **어떤 컴퓨터**에서도 접속 가능

Revoke update on SCHOOL.CIRCLE from 'stu2'@'localhost';

- **stu2**계정의 **SCHOOL데이터베이스의 CIRCLE테이블**의 **update 권한**을 삭제 stu2은 **로컬 컴**에서만 접속

사용자 계정 삭제하기

DROP USER *'stu1'@'localhost'* **;**

```
MariaDB [mysql]> drop user 'stu1'@'localhost';
Query OK, 0 rows affected (0.002 sec)
```

```
MariaDB [mysql]> select host, user from user;
+-----------+-------+
| Host      | User  |
+-----------+-------+
| 127.0.0.1 | root  |
| ::1       | root  |
| heesugi   | root  |
| localhost | root  |
| localhost | test1 |
+-----------+-------+
5 rows in set (0.001 sec)
```