# Keamanan Basis Data



4332101031 - Ariana Losong

# PROGRAM STUDI TEKNIK INFORMATIKA JURUSAN REKAYASA KEAMANAN SIBER POLITEKNIK NEGERI BATAM TAHUN 2022

## Keamanan Basis Data

Nama: Ariana Losong

Kelas: RKS 3B Reguler

NIM: 4332101031

### 1. Fundamental Access Control

Akses control merupakan hal penting yang perlu dikonfigurasi demi menjaga keamanan data. Fundamental Access Control pada Mysql dapat berupa user root yang memberikan aksess terhadap database tertentu kepada user biasa.

Berikut Langkah konfigurasi pemberian hak akses.

Untuk memberikan hak akses keseluruhan menggunakan perintah GRANT ALL ON databasename.\* TO user@ipaddress;

```
MariaDB [world]> GRANT ALL ON world. * to ari@192.168.56.105;
Query OK, 0 rows affected (0.021 sec)
MariaDB [world]> _
```

Maka disini user ari telah mendapatkan seluruh akses control. Kemudian jalankan perintah show databases; untu memeriksa apakah hak akses pada database world telah berhasil.

Pada kondisi ini, hak akses yang didapatkan user ari merupakan keseluruhan akses seperti membaca, menambah, mengubah, menghapus, dan sebagainya yang ingin dilakukan terhadap data dalam database.

# 2. Mandatory Access Control

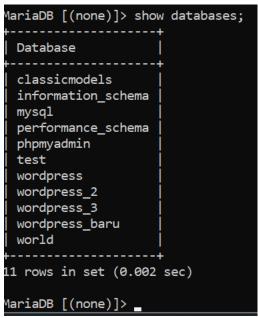
Mandatory access control merupakan metode untuk mengontrol pengguna atau suatu proses yang memiliki akses ke sumber daya dalam sebuah sistem.

Contoh MAC adalah user root yang memegang kendali penuh terhadap suatu data sehingga user tidak dapat sembarang mengakses data yang hak aksesnya dilarang oleh user root. Hanya user root yang dapat mengubah kebijakannya. Contoh:

```
MariaDB [(none)]> GRANT SELECT ON world. * to ari@192.168.56.105; Query OK, 0 rows affected (0.014 sec)

MariaDB [(none)]> show databases;
```

Hak akses yang diberikan hanya dapat untuk melaihat database. Untuk melihat apakah sudah berhasil, ketik perintah *show databases*;



Kemudian jalankan beberapa perintah untuk memeriksa hak akses yang telah diberikan

(perintah select)

# 3. Discreationary Access Control

Discreationary access control (DAC) merupakan prinsip membatasi akses ke objek berdasarkan identitas subjek. Control akses ini diimplementasikan menggunakan daftar kontrol akses. Administrator keamanan menentukan profil untuk setiap objek (sumber daya atau grup sumber daya), dan memperbarui daftar kontrol akses untuk profil tersebut. Jenis kontrol ini bersifat diskresioner dalam arti bahwa subjek dapat memanipulasinya, karena pemilik sumber daya, selain administrator keamanan, dapat mengidentifikasi siapa yang dapat mengakses sumber daya dan dengan otoritas apa.

Dalam database, DAC dapat diimplementasikan dan berhubungan dengan CRUD, yakni:

- Create, untuk membuat tabel baru
- Read, untuk membaca tabel dari sebuah database
- Update, untuk mengubah isi tabel
- Delete, untuk menghapus isi tabel

Contoh implementasi, user ari akan diberi akses create dan read dengan perintah grant create, insert, select on world. \* to ari@192.168.56.105;

```
MariaDB [world]> GRANT CREATE, INSERT, SELECT ON world.* TO ari@192.168.56.105;
Query OK, 0 rows affected (0.003 sec)
```

Lakukan perintah untuk memeriksa apakah akses yang diberikan telah berhasil

```
MariaDB [world]> SELECT * from city limit 3;
                                             Population
  ID
       Name
                  CountryCode
                                 District
       Kabul
                   AFG
                                  Kabol
                                                 1780000
                   AFG
   2
       Qandahar
                                 Qandahar
                                                  237500
                  AFG
                                 Herat
                                                  186800
       Herat
  rows in set (0.001 sec)
```

```
MariaDB [world]> CREATE TABLE data (no int(5) not null, nama varchar(200) not null);
Query OK, 0 rows affected (0.047 sec)
```