

## Praktikum Keamanan Basis Data

Nama : Belinda Panjaitan

NIM : 4332101022

Kelas : RKS 3A – Pagi

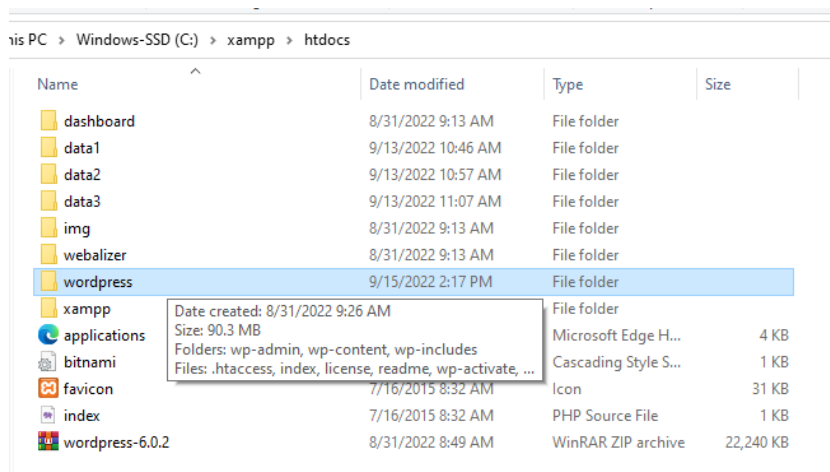
### Install Wordpress & Xampp di Windows

Download & install Wordpress & Xampp.

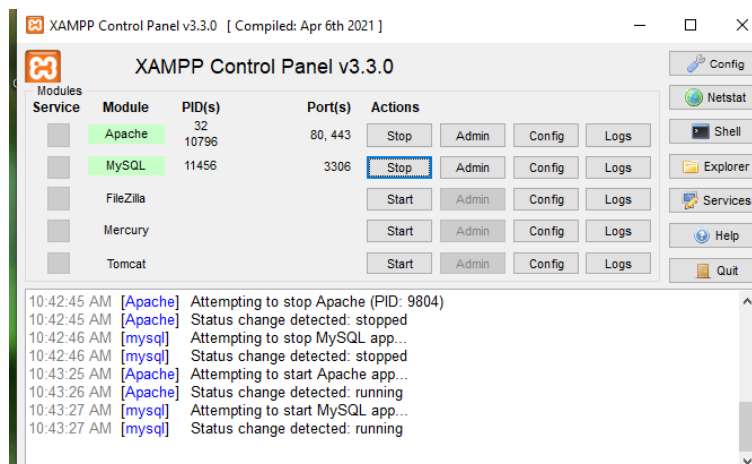
Xampp : <https://www.apachefriends.org/download.html>

Wordpress : <https://wordpress.org/download/>

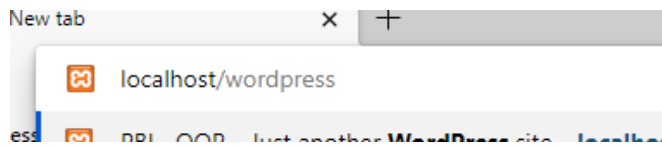
Extract file wordpress ke folder xampp/htdocs



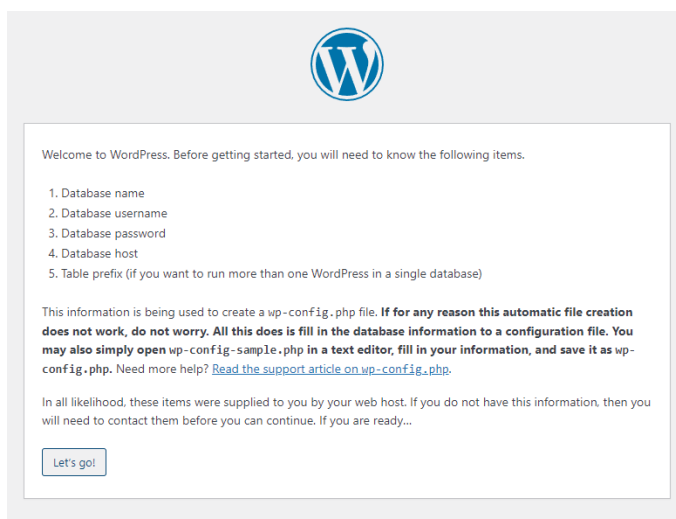
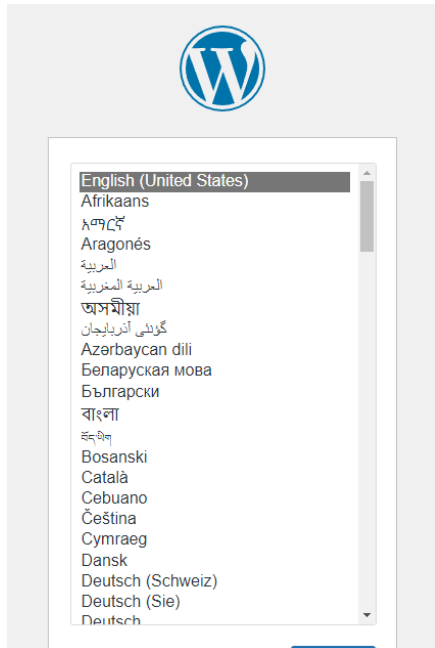
Jalankan xampp sebagai administrator dan start service Apache & MySQL




Selanjutnya membuat database di phpmyadmin. Buka browser dan ketik localhost/phpmyadmin, setelah laman terbuka klik menu Database lalu isi nama database dan klik create.



Kemudian buka wordpress di browser dengan perintah *http://localhost/wordpress*



Lengkapi data yang dibutuhkan seperti di bawah ini, lalu klik Install Wordpress.



Below you should enter your database connection details. If you are not sure about these, contact your host.


Database Name	<input type="text" value="data2"/>	The name of the database you want to use with WordPress.
Username	<input type="text" value="root"/>	Your database username.
Password	<input type="password"/>	Your database password.
Database Host	<input type="text" value="localhost"/>	You should be able to get this info from your web host, if localhost does not work.
Table Prefix	<input type="text" value="wp_"/>	If you want to run multiple WordPress installations in a single database, change this.

### Information needed

Please provide the following information. Do not worry, you can always change these settings later.

Site Title	<input type="text" value="basis data 2"/>
Username	<input type="text" value="data2"/> <small>Usernames can have only alphanumeric characters, spaces, underscores, hyphens, periods, and the @ symbol.</small>
Password	<input type="password" value="data2"/> <input type="button" value="Hide"/> <b>Very weak</b> <b>Important:</b> You will need this password to log in. Please store it in a secure location.
Confirm Password	<input checked="" type="checkbox"/> Confirm use of weak password
Your Email	<input type="text" value="belindanovelaa@gmail.com"/> <small>Double-check your email address before continuing.</small>
Search engine visibility	<input type="checkbox"/> Discourage search engines from indexing this site <small>It is up to search engines to honor this request.</small>

Tampilan yang akan muncul setelah install wordpress. Klik Log In untuk memulai pengaturan wordpress.



**Success!**

WordPress has been installed. Thank you, and enjoy!

Username	data2
Password	Your chosen password.

Note : pastikan mengingat username dan password yang telah dibuat, karena akan digunakan setiap login ke wordpress.

## Install WordPress dengan Database dan Web Server Terpisah

Untuk menghubungkan wordpress dengan web server dan database terpisah, dapat menggunakan 2 mesin virtual. Untuk memudahkan identifikasi server berbeda, diberi nama berbeda.



Untuk panduan cara menginstall mesin virtual dapat diakses pada

<https://adinusa.id/content/post/blogs/panduan-install-ubuntu-server-di-virtualbox/>

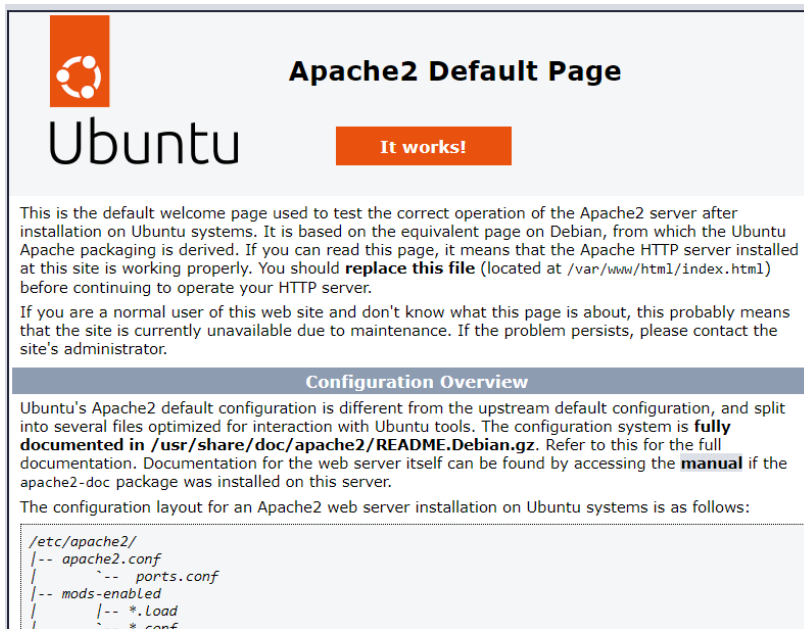
Setelah melakukan instalasi lanjut dengan setup VM Server & VM Database. Start kedua mesin virtual kemudian lakukan update dan upgrade dengan command:

```
belinda@belinda:~$ sudo apt update && apt upgrade
```

Selanjutnya install web server apache2. Status web server active atau tidak akan terlihat.

```
belinda@belinda:~$ sudo apt install apache2
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
apache2 is already the newest version (2.4.52-1ubuntu4.1).
The following packages were automatically installed and are no longer required:
  libevent-pthreads-2.1-7 libmecab2 libprotobuf-lite23 mecab-ipadic mecab-ipadic-
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
belinda@belinda:~$ systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor pre
   Active: active (running) since Thu 2022-09-15 22:46:40 UTC; 3min 59s ago
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 2190 ExecStart=/usr/sbin/apachectl start (code=exited, status=0
```

Untuk memastikan apakah server sudah berjalan, dapat juga dengan membuka browser dan mengetik ip server.



Lalu install PHP dan MySQL-client.

```
belinda@belinda:~$ sudo apt install php php-mysql
```

```
belinda@belinda:~$ sudo apt install mysql-client
```

Lakukan hal yang sama pada server kedua. Pada saat penginstalan mysql, lakukan perintah *sudo apt install mysql-server*.

```
sudo apt install mysql-server_
```

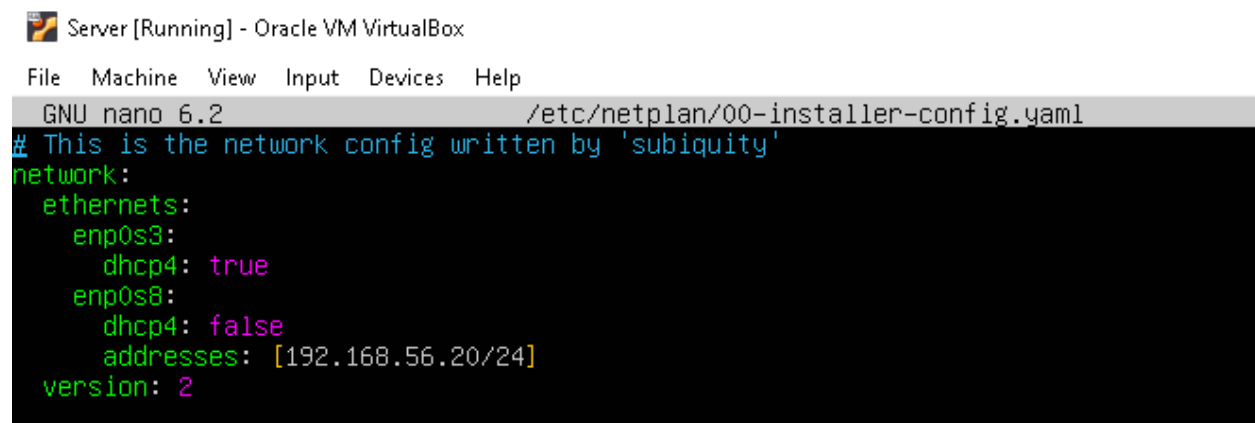
Note : untuk instalasi lebih lanjut dapat dilihat pada

<https://www.digitalocean.com/community/tutorials/how-to-install-mysql-on-ubuntu-22-04>

## Menghubungkan Server dengan Database

Setup IP ke-2 VM, gunakan 2 adapter yaitu, HostOnly % NAT di kedua VM.

Untuk konfigurasi ip ke static bisa menggunakan command: *sudo nano /etc/netplan/00-installer-config.yaml*



Dilakukan agar ip tidak berubah-ubah sehingga untuk mengaksesnya akan lebih mudah. Untuk menyimpannya, tekan ctrl+x lalu tekan y kemudian enter. Lakukan pengecekan dengan command: *sudo netplan apply* untuk mengetahui system dapat berjalan atau tidak.

Lakukan hal yang sama untuk VM ke-2.

Selanjutnya masuk ke mysql dengan akses root, lalu membuat user & database mysql. untuk keluar dari database, dapat dengan mengetik *exit*, dan restart mysql agar perintah yang telah dibuat dapat berjalan dengan baik dengan command: *restart mysql*.

```
mysql> CREATE DATABASE wordpress;
Query OK, 1 row affected (0.14 sec)

mysql> CREATE USER 'Admin'@'192.168.56.20' IDENTIFIED BY 'password';
Query OK, 0 rows affected (0.07 sec)

mysql> GRANT ALL PRIVILEGES ON wordpress.* TO 'Admin'@'192.168.56.20';
Query OK, 0 rows affected (0.02 sec)

mysql> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.87 sec)

mysql> exit
Bye
wordpress@database:~$ sudo systemctl restart mysql
```

Setting bind-address database agar dapat terhubung ke server, dengan command: *sudo nano /etc/mysql/mysql.conf.d/mysqld.cnf*

```
~$ sudo nano /etc/mysql/mysql.conf.d/mysqld.cnf
```

Untuk memastikan apakah web server dan mysql database terhubung, pada web server dapat dengan command: *sudo mysql -u nama database -h ip database -p*

```
wordpress@server:~$ sudo mysql -u Admin -h 192.168.56.30 -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 9
Server version: 8.0.30-0ubuntu0.22.04.1 (Ubuntu)

Copyright (c) 2000, 2022, 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.

mysql> _
```

Jika tampilannya seperti yang di atas, maka vm server dan database sudah terhubung.

**Instalasi Wordpress pada Web server**

Untuk instalasi pada wordpress dapat mengikuti tutorial pada link berikut :

<https://www.digitalocean.com/community/tutorials/install-wordpress-on-ubuntu>

### Menambah lebih dari satu wordpress di 1 VM

Download wordpress lalu extract file di wordpress.

```
wordpress@server:~$ cd /tmp && wget https://wordpress.org/latest.tar.gz
wordpress@server:/tmp$ tar -xvf latest.tar.gz
```

Dan copy file yang di extract ke /var/www/html.

```
wordpress@server:/tmp$ cp -R wordpress /var/www/html/
```

Untuk menambah wordpress ke-2 dan ke-3 ataupun seterusnya, copy Kembali file extract wordpress tadi ke folder baru di /var/www/html/(nama-folder-baru).

```
wordpress@server:/tmp$ sudo cp -R wordpress /var/www/html/wordpress2
wordpress@server:/tmp$ sudo cp -R wordpress /var/www/html/wordpress3
wordpress@server:/tmp$
```

Beberapa command untuk mengubah kepemilikan direktori 'wordpress'.

```
wordpress@server:/tmp$ sudo chown -R www-data:www-data /var/www/html/wordpress/
wordpress@server:/tmp$ sudo chown -R www-data:www-data /var/www/html/wordpress2/
wordpress@server:/tmp$ sudo chown -R www-data:www-data /var/www/html/wordpress3/
wordpress@server:/tmp$
```

Ganti file permissions dari folder wordpress.

```
wordpress@server:/tmp$ sudo chmod -R 755 /var/www/html/wordpress/
wordpress@server:/tmp$ sudo chmod -R 755 /var/www/html/wordpress2/
wordpress@server:/tmp$ sudo chmod -R 755 /var/www/html/wordpress3/
wordpress@server:/tmp$
```

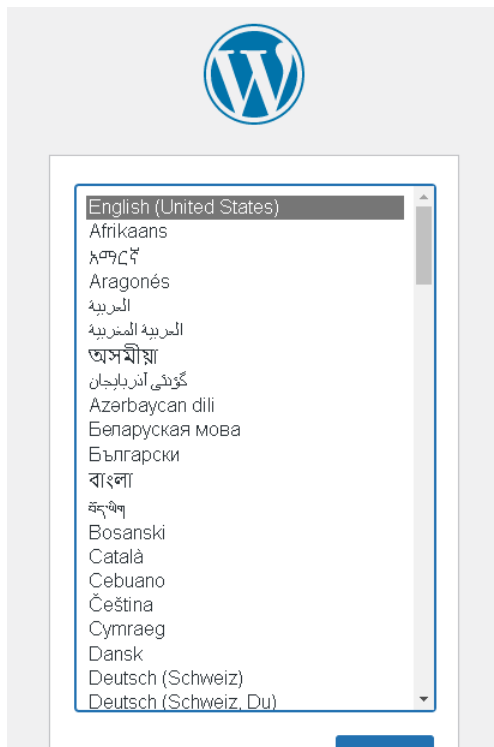
Buat direktori 'uploads'.

```
wordpress@server:/tmp$ sudo mkdir /var/www/html/wordpress/wp-content/uploads
wordpress@server:/tmp$ sudo mkdir /var/www/html/wordpress2/wp-content/uploads
wordpress@server:/tmp$ sudo mkdir /var/www/html/wordpress3/wp-content/uploads
wordpress@server:/tmp$
```

Ganti file permissions dari direktori 'uploads'

```
wordpress@server:/tmp$ sudo chown -R www-data:www-data /var/www/html/wordpress/wp-content/uploads/
wordpress@server:/tmp$ sudo chown -R www-data:www-data /var/www/html/wordpress2/wp-content/uploads/
wordpress@server:/tmp$ sudo chown -R www-data:www-data /var/www/html/wordpress3/wp-content/uploads/
wordpress@server:/tmp$
```

Coba buka browser dan masukkan url ip address server **ip-server/folder-wordpress**. Contoh :  
"ip-server/wordpress" atau "ip-server/wordpress2".



Tampilan yang akan terlihat.

Selanjutnya setting wordpress dengan memasukkan data yang dibutuhkan seperti nama database, user, password sesuai dengan yang telah kita buat.

Information needed

Please provide the following information. Do not worry, you can always change these settings later.

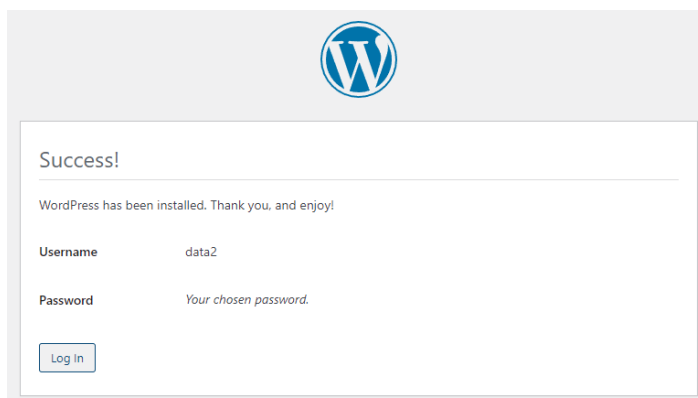
Site Title

Username   
Usernames can have only alphanumeric characters, spaces, underscores, hyphens, periods, and the @ symbol.

Password  [Hide](#)  
Very weak

**Important:** You will need this password to log in. Please store it in a secure location.

Confirm Password ☒ Confirm use of weak password





Lakukan Langkah yang sama untuk web wordpress ke-2 dan selanjutnya.

---

## Query UNION, SELECT, WAIT.

### Union

UNION in SQL is used to join two tables in the form of a new row down where the fields that are SELECTed between one table and another must be the same. Or simply i.e. to the place rows from query with each other and the values are distinct/unique.

```
mysql> SELECT nama_kolom FROM table1  
-> UNION  
-> SELECT nama_kolom FROM table2;
```

```
mysql> SELECT ID FROM wp_users  
-> UNION  
-> SELECT meta_key FROM wp_usermeta;  
  
+-----+  
| ID |  
+-----+  
| 1 |  
| nickname |  
| first_name |  
| last_name |  
| description |  
| rich_editing |  
| syntax_highlighting |  
| comment_shortcuts |  
| admin_color |  
| use_ssl |  
| show_admin_bar_front |  
| locale |  
| wp_capabilities |  
| wp_user_level |  
| dismissed_wp_pointers |  
| show_welcome_panel |  
| wp_dashboard_quick_press_last_post_id |  
| community-events-location |  
+-----+  
18 rows in set (0.02 sec)
```

### Select

The use of SELECT is to display tables in the database.

```
mysql> SELECT * FROM wp_terms;  
  
+-----+-----+-----+-----+  
| term_id | name | slug | term_group |  
+-----+-----+-----+-----+  
| 1 | Uncategorized | uncategorized | 0 |  
+-----+-----+-----+-----+  
1 row in set (0.53 sec)
```

### Wait

In the database, the WAIT function is not available so we use SLEEP for this command. SLEEP() is used to delay execution of the current script for a certain number of seconds.

```
mysql> -- SELECT * FROM wp_terms;  
mysql> SELECT * FROM wp_terms;  
  
+-----+-----+-----+-----+  
| term_id | name | slug | term_group |  
+-----+-----+-----+-----+  
| 1 | Uncategorized | uncategorized | 0 |  
| 2 | Menu 1 | menu-1 | 0 |  
| 3 | twentytwentytwo | twentytwentytwo | 0 |  
| 4 | header | header | 0 |  
| 5 | zeever | zeever | 0 |  
| 6 | footer | footer | 0 |  
| 7 | twentytwenty | twentytwenty | 0 |  
| 8 | startupzy | startupzy | 0 |  
| 9 | hello-elementor | hello-elementor | 0 |  
+-----+-----+-----+-----+  
9 rows in set (0.00 sec)
```

```
mysql> /*SELECT all the columns of all the records in the wp_terms table:*/SELECT * FROM wp_terms;
+-----+-----+-----+-----+
| term_id | name       | slug       | term_group |
+-----+-----+-----+-----+
| 1       | Uncategorized | uncategorized | 0          |
+-----+-----+-----+-----+
1 row in set (0.00 sec)
```

## Grant Privileges/Access Control List

Access Control List atau ACL, adalah daftar izin pengguna yang mengontrol akses ke sumber daya sistem. ACL menentukan pengguna atau proses sistem mana yang diizinkan untuk memiliki akses ke sumber daya sistem. Setiap entri ACL menentukan subjek dan operasi yang diizinkan.

Database adalah tempat penyimpanan virtual bagi sejumlah data penting untuk pembuatan website dan aplikasi web. Database MySQL menyimpan informasi akun user, seperti username, password, alamat email, dan informasi yang nantinya digunakan.

MySQL adalah salah satu sistem manajemen database yang populer dan paling banyak digunakan. Hal ini dikarenakan kemudahan penggunaan yang ditawarkan serta besarnya dukungan komunitas. Facebook dan Twitter adalah contoh platform yang memaksimalkan penggunaan MySQL.

## Membuat Hak Akses Tertentu untuk User MySQL

Pada saat membuat nama database dan nama tabel, pisahkan kedua nama tersebut dengan tanda titik (.) dan tidak perlu ditambahkan spasi. Dengan demikian, root user akan memperoleh finegrain control terhadap data tertentu. Ganti value PERMISSION\_TYPE dengan tipe akses yang ingin diberikan ke akun user baru.

Berikut perintah yang paling sering digunakan di MySQL :

- CREATE – memperbolehkan user untuk membuat database atau table.
- SELECT– memperbolehkan user untuk mengambil data.
- INSERT– memperbolehkan user untuk memodifikasi entri yang ada di tabel.
- DELETE– memperbolehkan user untuk menghapus entri tabel.
- DROP– memperbolehkan user untuk menghapus semua tabel database.

## Menampilkan Tipe Hak Akses yang Telah Diberikan Kepada User MySQL

Untuk mengecek kembali hak akses apa saja yang sudah dibagikan ke user MySQL, gunakan perintah SHOW GRANTS: *SHOW GRANTS FOR 'user\_name'@'localhost';*

Pada penggunaan MySQL, akan langsung diberikan username dan password. Dengan adanya informasi login ini, user akan memperoleh akses root atau kendali penuh atas semua database dan tabel.

Seiring dengan berjalannya waktu dan proyek online yang makin berkembang, pastinya administrator berencana untuk memberikan akses database ke user lain. Namun, dalam hal ini administrator tidak ingin mengizinkan user tersebut memegang kendali penuh.

Misalnya, administrator meminta bantuan developer untuk mengelola database. Akan tetapi, tidak ingin developer punya hak untuk menghapus atau memodifikasi informasi yang bersifat

sensitif. Maka dari itu, tipe informasi login yang sebaiknya diberikan adalah yang bersifat non-root user. Nantinya administrator bisa melacak apa saja yang boleh dan tidak boleh dilakukan oleh developer terhadap data tersebut.

### MySQL melakukan dua tahap ACL:

- Tahap 1 – MySQL memeriksa identitas profil dengan membandingkan profil dengan host dan nama pengguna yang tersimpan. Nama pengguna MySQL dan host klien menentukan identitas pemilik.
- Tahap 2 – Setelah Tahap 1, MySQL memeriksa hak istimewa di database MySQL saat melakukan operasi atau mengirim permintaan melalui koneksi yang dimiliki.

```
mysql> GRANT hak_akses ON nama_database TO 'nama_user'@'lokasi_user';_

mysql> SHOW DATABASES;
+-----+
| Database |
+-----+
| information_schema |
| performance_schema |
| website |
| wordpress |
+-----+
4 rows in set (0.01 sec)

mysql> USE website;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> SHOW TABLES;
+-----+
| Tables_in_website |
+-----+
| user |
+-----+
1 row in set (0.00 sec)

mysql> SELECT * FROM user;
Empty set (0.03 sec)

mysql> DROP TABLE user;
ERROR 1142 (42000): DROP command denied to user 'Admin'@'192.168.56.20' for table 'user'
mysql> _
```

### Jenis-Jenis Hak Akses berdasarkan Cakupan Akses Level.

#### Hak Akses Global(\*.\*)

Hak akses ini berarti user dapat memiliki hak akses untuk seluruh database yang terdapat di dalam MySQL.

```
mysql> GRANT SELECT ON *.* TO 'user'@'localhost';
```

penulisan \*.\* , sehingga user tersebut dapat mengakses seluruh table pada seluruh database.

#### Hak Akses Level Database (nama\_database.\*)

Hak akses ini berarti user dapat memiliki hak akses penuh untuk sebuah database.

```
mysql> GRANT SELECT ON *.* TO 'user'@'localhost';
mysql> GRANT SELECT ON website.* TO 'user'@'localhost';
```

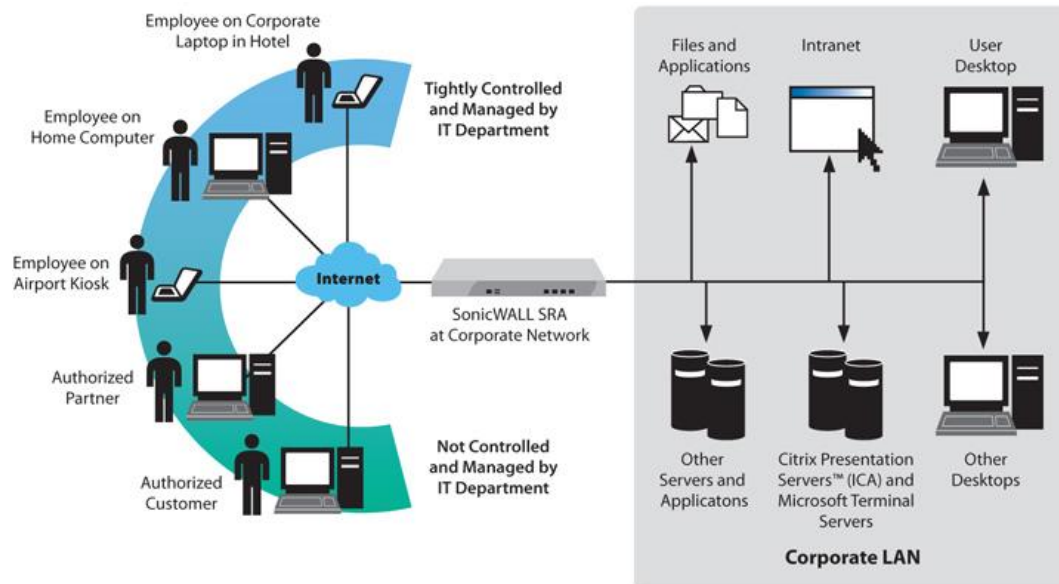
#### Hak Akses Level Kolom (nama\_kolom)

Hak akses ini adalah hak akses paling kecil yang dapat diberikan kepada sebuah user. Dengan

hak akses level kolom, user hanya memiliki akses untuk beberapa kolom pada sebuah table.

```
mysql> GRANT SELECT (nama-kolom) ON (nama-database).(nama-table)_TO 'user'@'localhost';
```

## Fundamental Access Control



Access control adalah proteksi layer pertama terhadap aset aset perusahaan atau organisasi, umumnya access control menggunakan beberapa layer teknologi. Namun secara teori ada yang dinamakan ada object access control dan subyek access control. Object adalah sebuah bentuk pasif dari aset perusahaan sedangkan subject adalah bentuk active dari perusahaan, contoh object adalah jaringan perusahaan, database perusahaan, email dll, sedangkan contoh subject adalah user atau aplikasi lain yang melakukan akses ke object tersebut.

Authentifikasi merupakan proses verifikasi untuk subject subject tersebut, autentifikasi bersifat rahasia, sedangkan identifikasi adalah proses umum, identifikasi bisa berupa account atau nama yang digunakan sebagai ID agar bisa dikenali orang lain. Proses lain didalam access control adalah proses Authorisasi yang berisi penempatan hak serta kewenangan subjek dalam melakukan tugasnya.

Dari sisi teknologi, autorizasi sekarang ini menggunakan beberapa jenis , antara lain adalah biometric, password, token devices, memory & smartcard, cryptographic keys, meskipun bermacam macam tetapi tujuannya ya sama saja. Strong Authentifikasi dikenal dengan Two Factor Authentification , terdiri dari 2 (dua) faktor misalnya password + token, password + pin dll, jadi memiliki 2 (dua) layer proteksi.

Teknologi yang paling tinggi adalah dengan biometric, didalam biometric dikenal ada yang namanya CER (Cross Over Error Rate), CER digunakan untuk mengukur akurasi dari biometric, semakin rendah nilai CER nya semakin tinggi akurasinya. Beberapa biometric yang kita kenal antara lain dengan fingerprint (sidik jari), hand geometry (yang diukur adalah punggung tangan, panjang jari jari, jarak antara jari jari), hand topology (pengukuran dari samping tangan , yang diukur ketebalan tapak tangan, struktur tulang). Lainnya adalah Iris (yang diukur pola iris mata),

retina (yang diukur pola darah dibelakang iris mata), signature dinamik (pengukuran tanda tangan digital) dan terakhir voice print (pengukuran berdasar pola suara, frekwensi suara, dialek suara).

Source: <https://edysusanto.com/acces-control-fundamental/>

Contoh penggunaan ACL adalah seperti berikut:

```
setfacl -m u:user:rw /path/to/file # add permission for user
setfacl -m g:group:rw /path/to/file # add permission for a group
setfacl -Rm u:user:rw /path/to/dir # recursive
setfacl -x u:user /path/to/file # remove a spesific entry
setfacl -b /path/to/file # remove a spesific entry for all user
getfacl /path/to/file # get ACL information in a file
```