

Laporan Keamanan Basis Data
Wordpress Multi Database & MySQL ACL



Disusun Oleh :
M. Arghian Taufahena
4332101007

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

M. Arghian Taufahena

4332101007

RKS 3A Pagi

Keamanan Basis Data | Wordpress Multi Database

1. Database Server

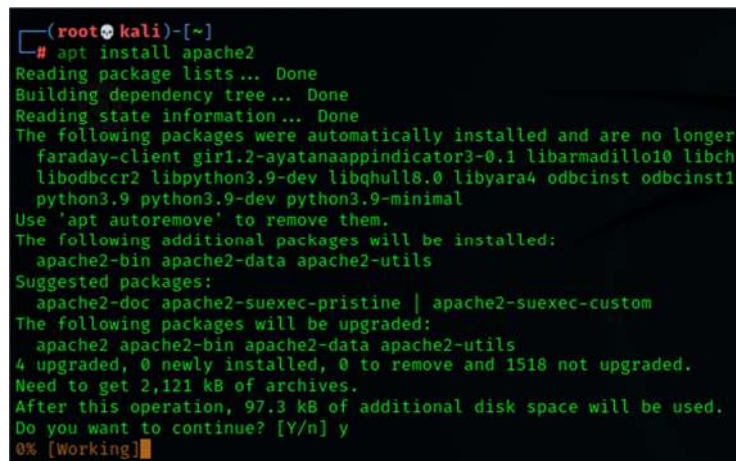
Untuk server database saya menggunakan os ubuntu server yang sudah saya install pada mesin virtual. Database server disini bertujuan untuk menyimpan ketiga web database yang berbeda dengan user privilege yang berbeda pula.

a. Set Up Layanan Server

Sebelum itu pertama kita akan set up server database dengan menginstall beberapa service (disini saya menggunakan server dummy, hanya untuk menginstall service database server yang diperlukan, karena sebelumnya untuk Ubuntu database server saya tidak sempat untuk mengambil screenshot.) ;

1. Apache2

Apache2 disini berfungsi sebagai penghubung server dengan website yang akan kita tampilkan nantinya. Gunakan perintah *apt install apache2* untuk menginstall.



```
(root@kali)-[~]
# apt install apache2
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer
required:
  faraday-client gir1.2-ayatanaappindicator3-0.1 libarmadillo10 libch
  libodbccr2 libpython3.9-dev libqhull8.0 libyara4 odbcinst odbcinst1
  python3.9 python3.9-dev python3.9-minimal
Use 'apt autoremove' to remove them.
The following additional packages will be installed:
  apache2-bin apache2-data apache2-utils
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom
The following packages will be upgraded:
  apache2 apache2-bin apache2-data apache2-utils
4 upgraded, 0 newly installed, 0 to remove and 1518 not upgraded.
Need to get 2,121 kB of archives.
After this operation, 97.3 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
0% [Working]
```

2. MySql

Selanjutnya adalah mysql, mysql disini berfungsi sebagai service untuk database wordpress kita nantinya. Gunakan perintah *apt install mariadb-server mariadb-client*

```
(root@kali)-[~]
# apt install mariadb-server mariadb-client
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer
required:
  faraday-client girl1.2-ayatanaappindicator3-0.1 libarmadillo10 libch
  libodbc2 libpython3.9-dev libqhull8.0 libyara4 odbcinst odbcinst1
  python3.9 python3.9-dev python3.9-minimal
Use 'apt autoremove' to remove them.
The following additional packages will be installed:
  default-mysql-server libdaxctl1 libndctl6 libpmem1 mariadb-client-1
Suggested packages:
  mailx mariadb-test netcat-openbsd
The following packages will be REMOVED:
  mariadb-client-10.5 mariadb-client-core-10.5 mariadb-server-10.5 ma
The following NEW packages will be installed:
  libdaxctl1 libndctl6 libpmem1 mariadb-client mariadb-client-10.6 ma
The following packages will be upgraded:
  default-mysql-server mariadb-common
2 upgraded, 9 newly installed, 4 to remove and 1516 not upgraded.
Need to get 13.7 MB of archives.
After this operation, 4,417 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://kali.darklab.sh/kali kali-rolling/main amd64 mariadb-com
```

3. PHP

Selanjutnya PHP, berfungsi sebagai service atau web browser, ketika ada permintaan dari browser ke web server, PHP akan menghubungi MySQL server untuk mencari data yang dibutuhkan di database. Gunakan perintah *apt install php php-mysql* untuk menginstall.

```
(root@kali)-[~]
# apt install php php-mysql
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are r
  faraday-client girl1.2-ayatanaappindicator3-0.1 libarmadillo
  libodbc2 libpython3.9-dev libqhull8.0 libyara4 odbcinst o
  python3-pyhp python3.9 python3.9-dev python3.9-minimal
Use 'apt autoremove' to remove them.
The following additional packages will be installed:
  libapache2-mod-php8.1 php8.1 php8.1-cli php8.1-common php8.
Suggested packages:
  php-pear
The following NEW packages will be installed:
  libapache2-mod-php8.1 php8.1 php8.1-cli php8.1-common php8.
The following packages will be upgraded:
  php php-mysql
2 upgraded, 7 newly installed, 0 to remove and 1514 not upgra
Need to get 4,857 kB of archives.
After this operation, 21.6 MB of additional disk space will b
Do you want to continue? [Y/n] y
Get:2 http://http.kali.org/kali kali-rolling/main amd64 php8.
Get:6 http://archive-4.kali.org/kali kali-rolling/main amd64
Get:7 http://http.kali.org/kali kali-rolling/main amd64 php a
13% [Waiting for headers]
```

b. Set Up Database Server

Setelah selesai penginstallan semua service yang dibutuhkan, selanjutnya saya akan membuat ketiga database web nya, dengan cara :

- Masuk ke mysql root (`mysql -u root -p`)
- Membuat database (`Create database nama_database;`)
- Membuat user dengan untuk database sebelumnya (`create user 'nama'@'ip host yang akan diberikan akses untuk remote user' identified by 'password';`)
- Beri semua hak akses pada akun yang telah kita buat (`grant all privileges on nama_database.* to 'user'@'ip host';`)
- Refresh privileges (`flush privileges;`)

Berikut database wp_sucxsz dengan user sucxsz yang sudah saya buat, dan bisa di remote pada atau di akses di mysql atau wordpress web server nantinya. Dengan ketentuan ip web server harus sama dengan ip host yang sudah saya masukkan untuk user sucxsz.

```
MariaDB [(none)]> create database wp_sucxsz;
Query OK, 1 row affected (1.541 sec)

MariaDB [(none)]> create user 'sucxsz'@'192.168.20.6' identified by 'gamma';
Query OK, 0 rows affected (0.438 sec)

MariaDB [(none)]> grant all privileges on wp_sucxsz.* to 'sucxsz'@'192.168.20.6';
'> ';
ERROR 1133 (28000): Can't find any matching row in the user table
MariaDB [(none)]> grant all privileges on wp_sucxsz.* to 'sucxsz'@'192.168.20.6';
Query OK, 0 rows affected (0.099 sec)

MariaDB [(none)]> flush privileges;
Query OK, 0 rows affected (0.102 sec)

MariaDB [(none)]> _
```

Selanjutnya kita akan konfigurasi mysql server untuk menambahkan ip address server. Dengan cara buka dan edit file yang ada pada direktori **/etc/mysql/mariadb.conf.d/50-server.conf**. disini saya menggunakan nano sebagai layanan file editing konfigurasi. Masukkan ip server pada bagian bind-address, ini akan berguna sebagai host layanan yang akan kita berikan oleh server kita.

```
GNU nano 6.2 /etc/mysql/mariadb.conf.d/50-server.cnf
#
# These groups are read by MariaDB server.
# Use it for options that only the server (but not clients) should see
#
# This is read by the standalone daemon and embedded servers
[server]
#
# This is only for the MySQL standalone daemon
[mysqld]
#
# * Basic Settings
#
#user                    = mysql
#pid-file                = /run/mysqld/mysqld.pid
#basedir                = /usr
#port                   = 3306
#datadir                = /var/lib/mysql
#tmpdir                 = /tmp
#
# Broken reverse DNS slows down connections considerably and name resolve is
# safe to skip if there are no "host by domain name" access grants
#skip-name-resolve
#
# Instead of skip-networking the default is now to listen only on
# localhost which is more compatible and is not less secure.
#bind-address            = 192.168.20.5
#
# * Fine Tuning
#
[ Read 115 lines ]
G Help      W Write Out  W Where Is  C Cut       E Execute   C Location  M-U Undo
X Exit      R Read File  R Replace  U Paste     J Justify   G Go To Line M-E Redo
```

Setelah semua ini dilakukan, tinggal lanjut ke web server, untuk melakukan installasi dan konfigurasi wordpress dan menghubungkan ke database server.

2. Wordpress Web Server

Untuk Webserver disini saya menggunakan os debian 9 server mode GUI. Yang sudah saya install pada mesin virtual yang sama dengan database server. Webserver ini bertujuan untuk melakukan penginstallan dan konfigurasi web wordpress yang akan terhubung ke dalam ketiga database yang telah saya buat sebelumnya.

a. Remote Mysql

Disini pertama tama saya ingin uji coba untuk me remote salah satu user database mysql yang sudah saya buat sebelumnya, dengan cara,
Masuk ke terminal dan Login mysql dengan perintah (*mysql -u user -h ip host -p*)
User dan host disini saya menggunakan user sucxsz dengan ip 192.168.20.5 (ip databaseserver).

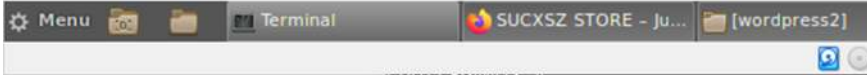
```
root@sucxsz:~# mysql -u sucxsz -h 192.168.20.5 -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 119
Server version: 10.6.7-MariaDB-2ubuntu1.1 Ubuntu 22.04

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

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

MariaDB [(none)]> show databases;
+-----+
| Database |
+-----+
| information_schema |
| wp_sucxsz |
+-----+
2 rows in set (0.07 sec)

MariaDB [(none)]>
```



Dapat dilihat disini sudah bisa remote database sesuai ketentuan akun yang sudah dibuat, yaitu user sucxsz dapat hak akses pada databases wp_sucxsz.

b. Install Wordpress CMS

Untuk penginstalan wordpress pada webserver, disini saya menggunakan beberapa perintah yaitu :

- Mengunduh file wordpress pada domain wordpress.org/latest.tar.gz yang ditempatkan pada direktori /tmp (`cd /tmp && wget https://wordpress.org/latest.tar.gz`)

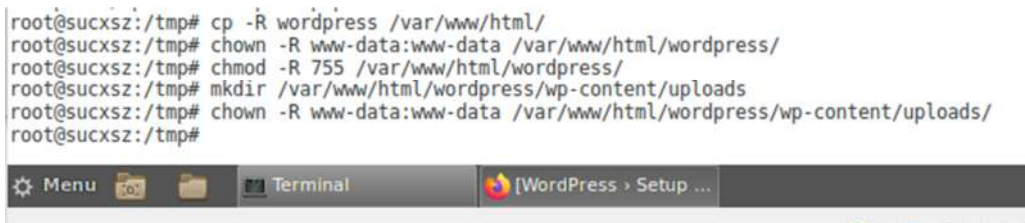
```
root@sucxsz:~# cd /tmp && wget https://wordpress.org/latest.tar.gz
--2022-09-22 00:57:48-- https://wordpress.org/latest.tar.gz
Resolving wordpress.org (wordpress.org)... 198.143.164.252
Connecting to wordpress.org (wordpress.org)|198.143.164.252|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 21172479 (20M) [application/octet-stream]
Saving to: 'latest.tar.gz'

latest.tar.gz          5%[=>]
```



- Selanjutnya copy file atau folder wordpress ke direktori html (`cp -R wordpress /var/www/html/`)
- Ubah permission dir wordpress (`chown -R`) dan (`chmod -R 755`)
- Buat direktori uploads di dalam /wordpress/wp-content/ (`mkdir`)
- Kembali ubah permission dir uploads seperti wordpress (`chown -R`)

```
root@sucxsz:/tmp# cp -R wordpress /var/www/html/
root@sucxsz:/tmp# chown -R www-data:www-data /var/www/html/wordpress/
root@sucxsz:/tmp# chmod -R 755 /var/www/html/wordpress/
root@sucxsz:/tmp# mkdir /var/www/html/wordpress/wp-content/uploads
root@sucxsz:/tmp# chown -R www-data:www-data /var/www/html/wordpress/wp-content/uploads/
root@sucxsz:/tmp#
```

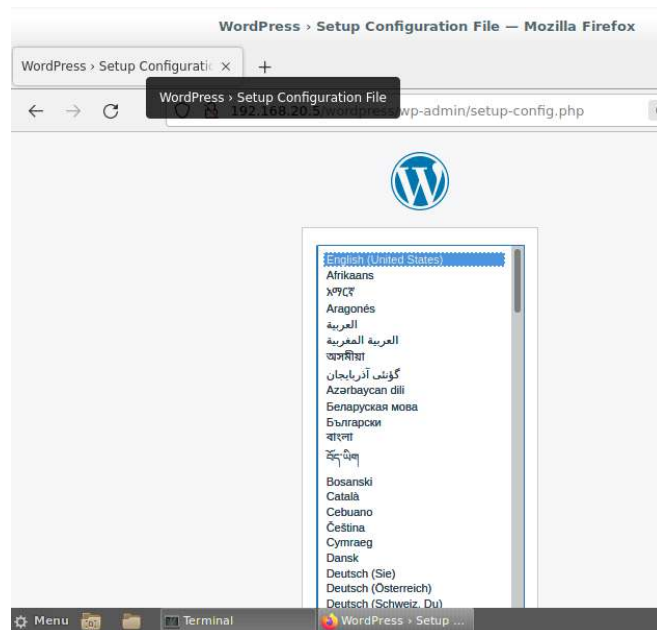


- Penjelasan Command
 - o `cp -R` yang berfungsi untuk menyalin sebuah direktori
 - o `chown -R` yang berfungsi untuk mengganti owner atau kepemilikan folder, disini `www-data:www-data` agar jika ada hacker yang mendapat eksploit ke file, maka hacker tersebut hanya dapat masuk sebagai `www-data`.
 - o `Chmod -R` yang berfungsi mengubah permission sebuah file atau hak akses, disini `755` hanya bisa mengakses file untuk melihat dan mengeksekusi.

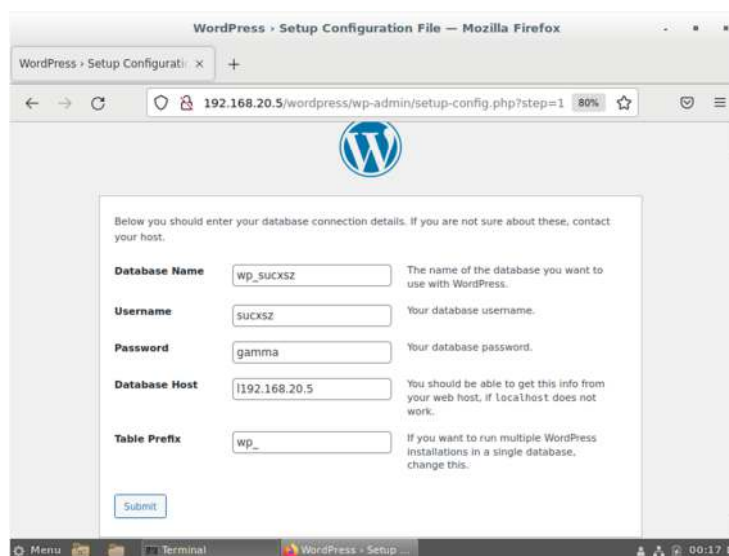
c. Konfigurasi Wordpress

Untuk konfigurasi atau membuat website wordpress, kita gunakan browser untuk membuatnya, buka ip address web server pada kolom domain, disertai direktori wordpress. **192.168.20.6/wordpress.**

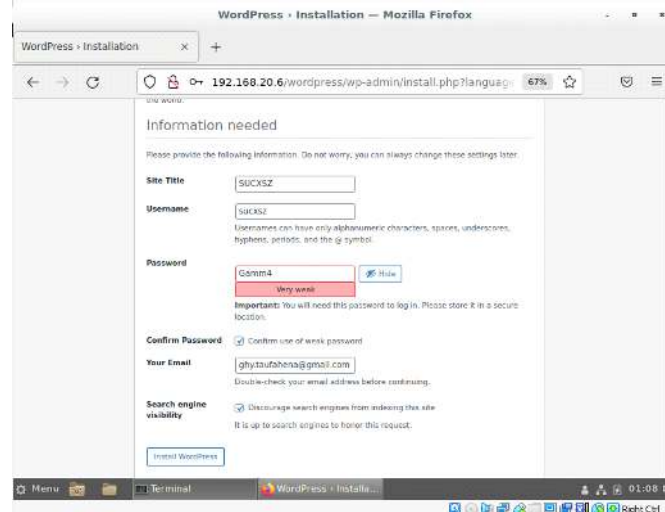
Pertama kita disuruh memilih bahasa yang akan kita gunakan



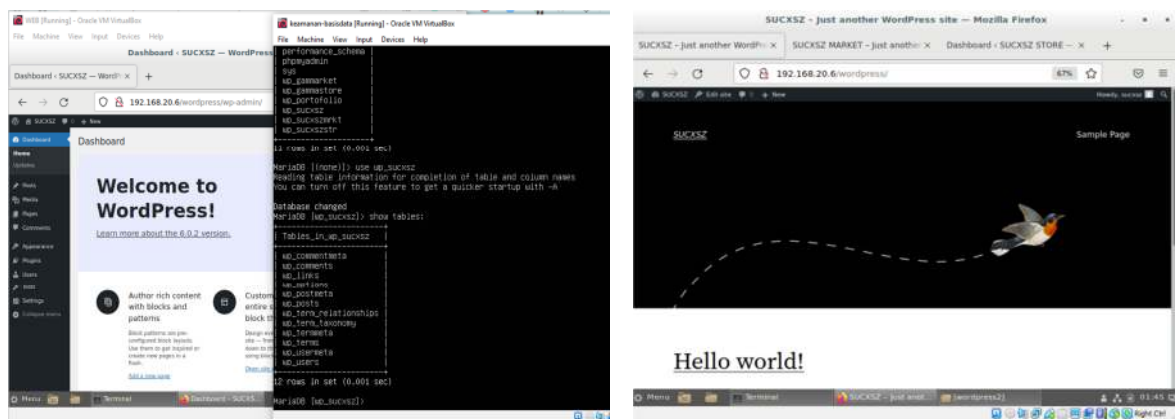
Selanjutnya kita akan memilih database yang akan kita gunakan sesuai dengan database yang ada di database server. Untuk website pertama, saya gunakan database wp_sucxsz. Dan juga gunakan username, password dan host ip (database server) yang sesuai dengan database nya. Untuk table prefix tetap diisi dengan wp_ saja.



Selanjutnya kita isi beberapa kolom yang akan digunakan untuk wordpress, disini terdapat judul situs, username, password dan email. Diisi saja sesuai keinginan kita membuat website dan akun nya.



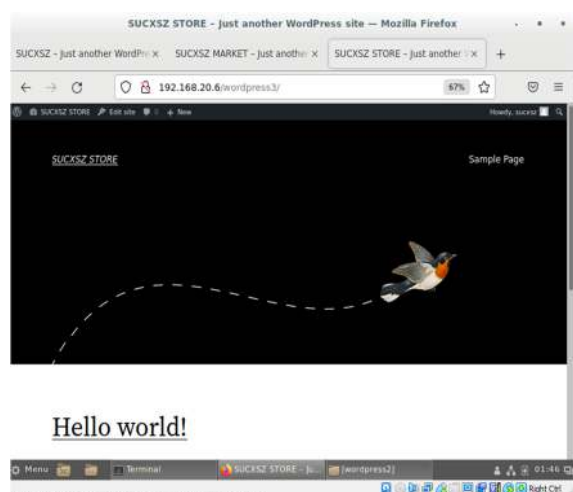
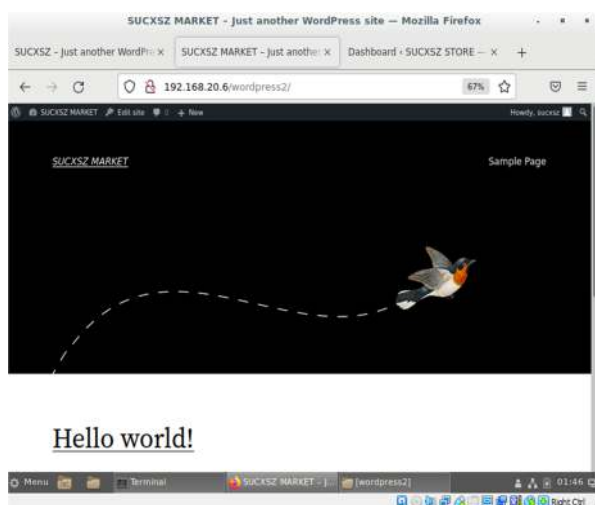
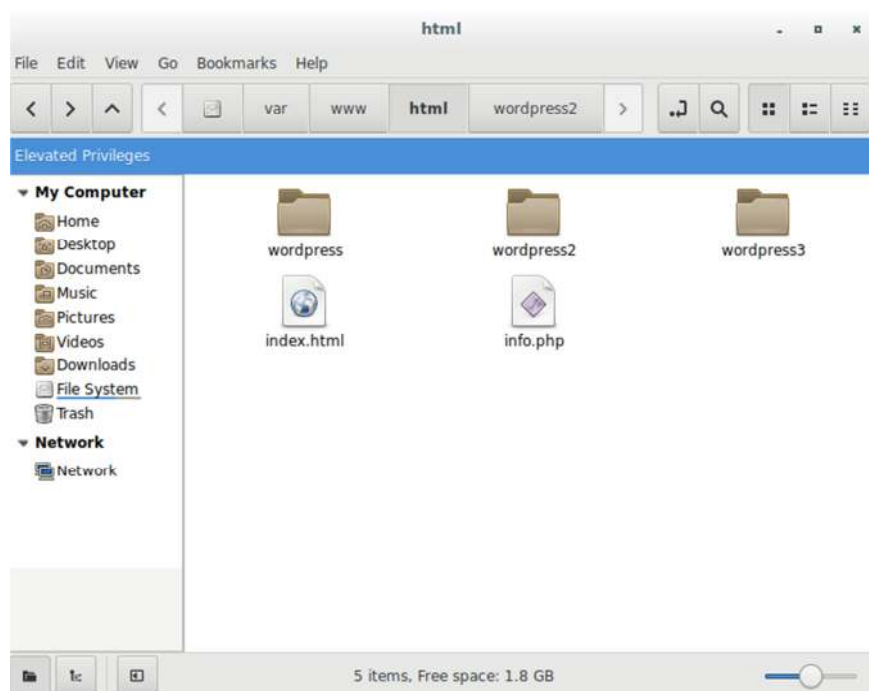
Setelah semua proses selesai, maka wordpress pertama sudah jadi. Dan lanjut untuk membuat web wordpress kedua dengan sisa 2 database yang masih kosong. Caranya tidak berbeda dengan sebelumnya, hanya saja ada sedikit perubahan pada direktori wordpress nya.



Untuk membuat dua wordpress lainya adalah dengan cara menduplikat file wordpress yang sebelumnya telah ada. contoh disini saya buat2 duplikat file wordpress dengan tambahan angka 2 dan 3 sebagai penanda.

Tidak hanya duplikat direktori, salah satu file yang ada dalam wordpress harus kita hapus terlebih dahulu, yaitu file **wp-config.php**. kenapa dihapus ? karena file config ini sudah menyimpan konfigurasi dari wordpress pertama yang kita buat, jadi kita perlu membuat file config baru. Untuk membuatnya gampang, wordpress akan otomatis menyuruh kita membuat file **wp-config.php**, apabila di file wordpress yang digunakan tidak ada pada saat penginstallan atau pembuatan web berlangsung.

Dan untuk membuat website kedua ini kita hanya perlu mengganti direktori pada domain awal, yaitu **192.168.20.6/wordpress2**



Terakhir, saya akan mencoba melihat isi dalam database ketiga, yang harusnya didalamnya sudah terisi oleh database dari wordpress website ketiga saya. Disini saya akan menggunakan remote akses mysql user ke 3.

```
root@sucxsz:~# mysql -u sucxsz3 -h 192.168.20.5 -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 120
Server version: 10.6.7-MariaDB-2ubuntu1.1 Ubuntu 22.04


Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

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

MariaDB [(none)]> show databases;
+-----+
| Database |
+-----+
| information_schema |
| wp_sucxszstr |
+-----+
2 rows in set (0.00 sec)

MariaDB [(none)]> use wp_sucxszstr
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

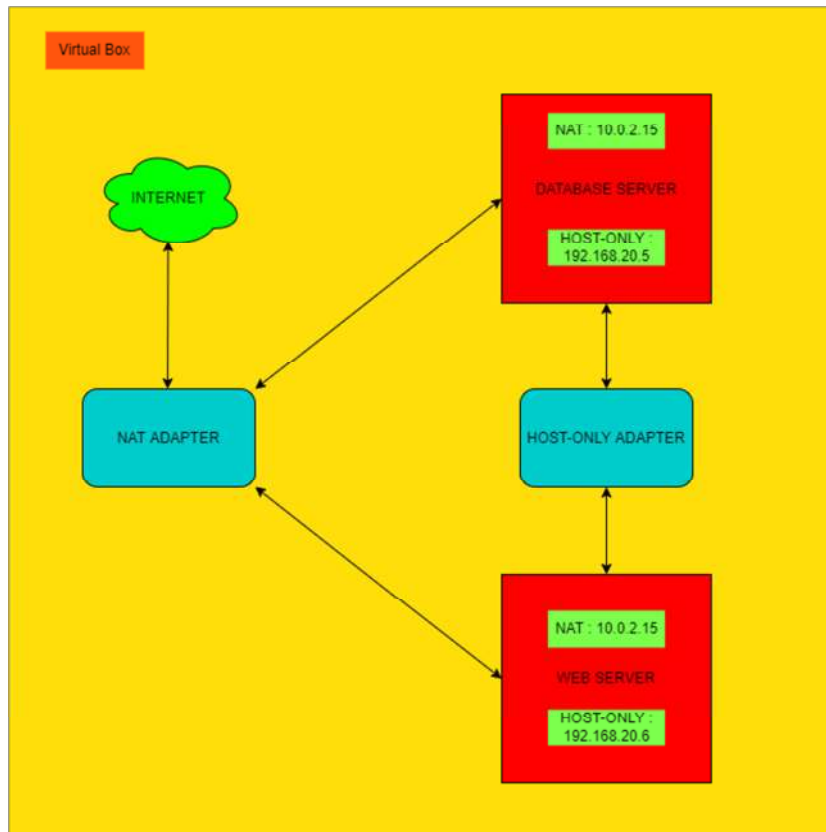
Database changed
MariaDB [wp_sucxszstr]> show tables;
+-----+
| Tables_in_wp_sucxszstr |
+-----+
| wp_commentmeta |
| wp_comments |
| wp_links |
| wp_options |
| wp_postmeta |
| wp_posts |
| wp_term_relationships |
| wp_term_taxonomy |
+-----+
```



Nah, sudah dapat dilihat bahwa database ke 3 saya sudah terisi dengan database wordpress ke 3.

3. Topologi

Topologi jaringan yang saya gunakan untuk menjalankan kedua server adalah sebagai berikut :

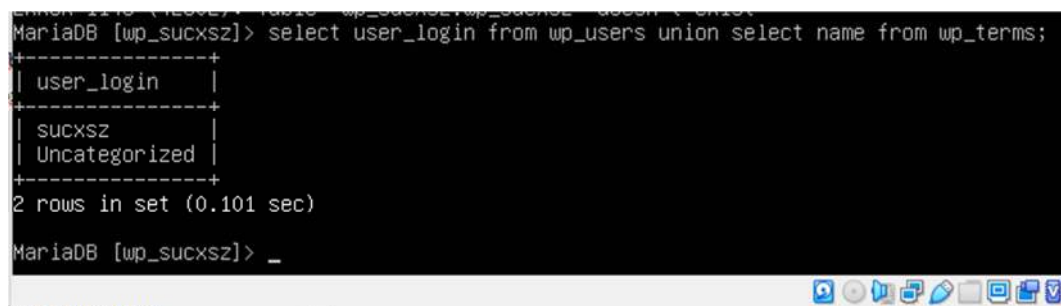


4. Mysql UNION, SELECT, SLEEP & --

a. UNION

Fungsi MySQL UNION adalah Operator MySQL yang digunakan untuk menggabungkan kumpulan hasil dari 2 atau lebih pernyataan SELECT. Ini menghapus duplikat baris antara berbagai pernyataan SELECT. Setiap pernyataan SELECT di dalam operator UNION harus memiliki jumlah field yang sama pada set hasil dengan tipe data yang sama.

Contoh : *select nama_kolom from nama_tabel UNION select nama_kolom from tabel2.*



```

MariaDB [wp_sucxsz] > select user_login from wp_users union select name from wp_terms;
+-----+
| user_login |
+-----+
| sucxsz    |
| Uncategorized |
+-----+
2 rows in set (0.101 sec)

MariaDB [wp_sucxsz] > _
```

Disini saya menggunakan kolom `user_login` dari table `wp_users` dan kolom `name` dari table `wp_terms`

b. SELECT

Select digunakan untuk memilih data dari sebuah tabel atau beberapa tabel. Data yang dipilih menggunakan select dapat dalam satu kondisi atau beberapa kondisi yang mengkombinasikan select dengan operator lain.

CONTOH : SELECT * FROM nama_tabel

```

MariaDB [wp_sucxsz]> select user_pass from wp_users;
+-----+
| user_pass |
+-----+
| $P$BUjkBSZ4g9eVkjtoE2EJUDwjbpcvYz/ |
+-----+
1 row in set (0.000 sec)

MariaDB [wp_sucxsz]> _

```

Disini saya menggunakan kolom user_pass pada table wp_users.

c. SLEEP

Sleep digunakan menunggu batas waktu berakhir. Pada contoh di bawah saya mau menampilkan semua record dari table wp_users kemudian saya gunakan sleep(5) maka akan membutuhkan waktu 5 detik untuk menampilkan semua recordnya.

CONTOH : Select *, SLEEP from nama_tabel

```
Database changed
MariaDB [wp_sucxsz]> show tables;
+-----+
| Tables_in_wp_sucxsz |
+-----+
| wp_commentmeta      |
| wp_comments         |
| wp_links            |
| wp_options          |
| wp_postmeta         |
| wp_posts            |
| wp_term_relationships|
| wp_term_taxonomy    |
| wp_termmeta         |
| wp_terms            |
| wp_usermeta         |
| wp_users            |
+-----+
12 rows in set (0.00 sec)

MariaDB [wp_sucxsz]> select *, sleep(7) from wp_posts;
```

A screenshot of a terminal window with a dark background. The prompt is MariaDB [wp_sucxsz]. The first command executed is 'show tables;', which returns a list of 12 tables in the wp_sucxsz database, enclosed in a box-like format with dashed borders. The second command is 'select *, sleep(7) from wp_posts;'. The terminal shows the start of the result grid with dashed lines, but it is mostly empty, suggesting the query was interrupted or the output is truncated. At the bottom, there is a macOS-style taskbar with icons for Menu, Finder, Terminal, and other applications. The active window title is '[wordpress2]'. The system clock shows 10:19.

d. SQL Comments (--)

Perintah `--` pada sql digunakan untuk menambahkan komentar dengan pernyataan dengan contoh kode .

CONTOH : `select* all records from nama table; -- dari table nama table`

```
MariaDB [wp_sucxszmkt]> select* -- selects all records
-> from wp_users; -- dari table wp_users
+-----+-----+-----+-----+-----+-----+
| ID | user_login | user_pass | user_nicename | user_email | u
ser_url | user_registered | user_activation_key | user_status | display_na
me |
+-----+-----+-----+-----+-----+-----+
| 1 | sucxsz | $P$B0puEXtMfDw2DUaiz8VjTKAu9H3PYp. | sucxsz | ghy.taufahena@gmail.com | h
ttp://192.168.20.6/wordpress2 | 2022-09-22 05:41:00 | | 0 | sucxsz
+-----+-----+-----+-----+-----+-----+
1 row in set (0.000 sec)

MariaDB [wp_sucxszmkt]>
```

5. Mysql ACL

MySQL menggunakan keamanan berdasarkan Akses Control List (ACL) untuk semua koneksi, kueri, dan operasi lain yang dapat dilakukan pengguna. Ada juga dukungan untuk koneksi terenkripsi SSL antara klien dan server MySQL.

ACL biasa digunakan untuk manajemen user dan control akses ,

Contoh disini, perintah **Show Grants** untuk melihat privilege sebuah user dan **Revoke** untuk menghapus hak akses yang tidak diperlukan.

```
MariaDB [(none)]> show grants for 'sucxsz'@'192.168.20.6';
+-----+
| Grants for sucxsz@192.168.20.6 |
+-----+
| GRANT USAGE ON *.* TO `sucxsz`@`192.168.20.6` IDENTIFIED BY PASSWORD '*3DDB6F1DCB51287BC6DFA27177D
DD805ACAE1224' |
| GRANT ALL PRIVILEGES ON `wp_sucxsz`.* TO `sucxsz`@`192.168.20.6` |
+-----+
2 rows in set (0.106 sec)

MariaDB [(none)]> _
```


Investasikan dalam firewall. Ini melindungi Anda dari setidaknya 50% dari semua jenis eksploitasi dalam perangkat lunak apa pun. Letakkan MySQL di belakang firewall atau di zona demiliterisasi (DMZ).

MySQL menggunakan port 3306 secara default. Port ini seharusnya tidak dapat diakses dari host yang tidak dipercaya. Sebagai cara sederhana untuk memeriksa apakah port MySQL Anda terbuka, coba perintah berikut dari beberapa mesin jarak jauh,.

Contohnya disini saya menggunakan perintah telnet untuk mengetahui apakah port 3306 dari MySQL dapat diakses dari pihak luar , dengan perintah *telnet ip_server 3306*

```
(rootkali)-[/home/kali]
# telnet 192.168.20.5 3306
Trying 192.168.20.5 ...
Connected to 192.168.20.5.
Escape character is '^]'.
HHost '192.168.20.10' is not allowed to connect to this MariaDB server
Connection closed by foreign host.

(rootkali)-[/home/kali]
# █
```

