CHAPTER 5
IMPLEMENTATION AND TESTING

5.1 Implementation

Linux Installation

1. According to illustration 5.1 the first step is select the language to install linux. And then create a partition for the linux operating system that will be installed. The partition that will be used in the installation of linux is the swap partition and partition/.
2. According to illustration 5.2 The next step is select the location to determine the timezone in linux. And then select the keyboard layout is used.
3. According to illustration 5.3 the next step is to create a username and password to login to a linux operating system that has been installed. After that the linux installation process will start.
4. According to illustration 5.4 After the installation process is complete restart the computer that has been installed linux. After that login with username and passsword that have been created.

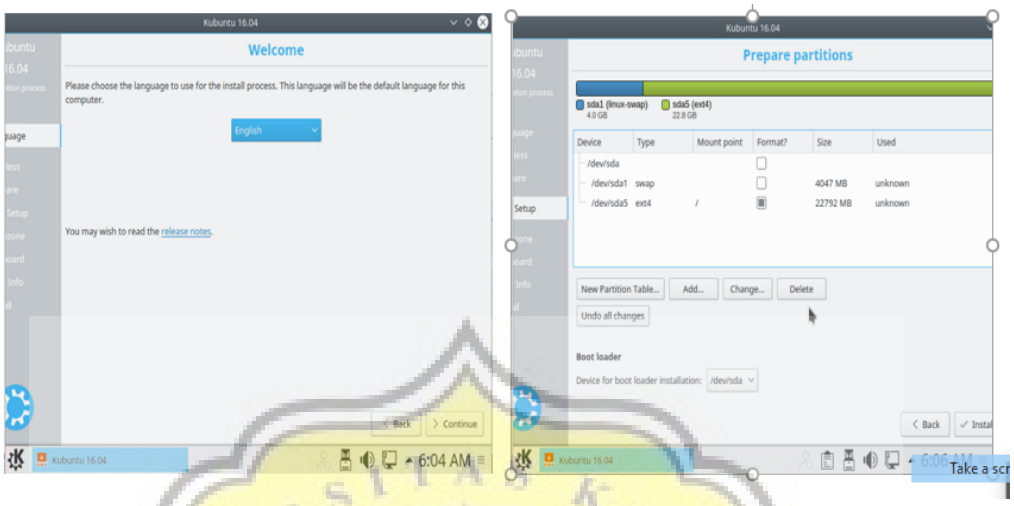

Illustration 5.1 Display To Select The Language To Install Linux And Create Patition.

Illustration 5.2 Display To Select Timezone And Keyboard Layout.

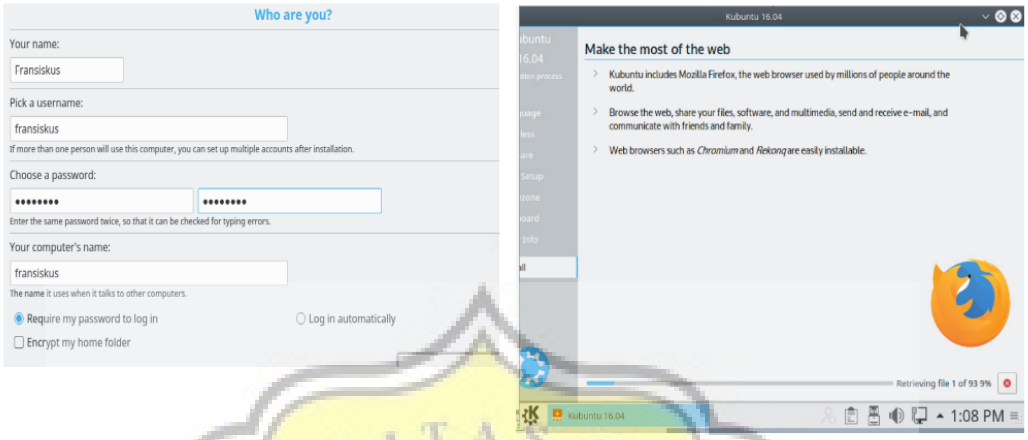

Illustration 5.3 Display To Create User And Password And Installation Process

Illustration 5.4 Linux Installation Is Complete.

ISP Config Installation

1. Open the terminal and sign in as user root.

   sudo su

2. The next step was to reconfigure the dpkg and select no to use the dash as the default system shell in the bin/sh directory.

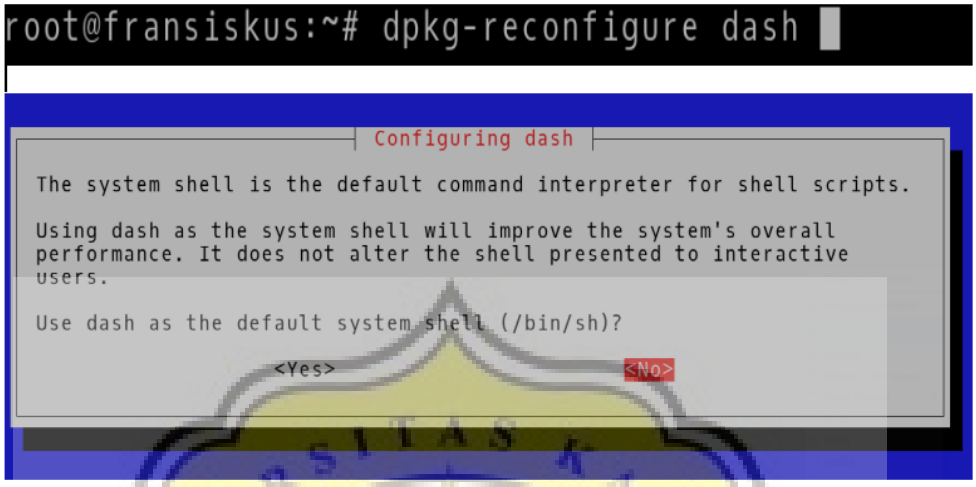

Illustration 5.5 Reconfigure Dpkg.

3. Disable apparmor.

   service apparmor stop

   update-rc.d -f apparmor remove

   And Remove Apparmor

   apt-get remove apparmor apparmor-utils

   Apparmor is a linux security system that can interfere with the installation in the isp config. Apparmor is equal to Selinux which is owned by redhat linux.

4. Installing network time protocol.

   apt-get -y install ntp ntpdate

   To set on a system clock with an NTP through internet network when running the server.

5. install e-mail server, MariaDB server, dan Rootkit Hunter.

   apt-get install rkhunter openssl getmail4 binutils dovecot-imapd dovecot-pop3d dovecot-mysql dovecot-sieve dovecot-lmtpd sudo postfix postfix-mysql postfix-doc mariadb-client mariadb-server

6. Configure the type of email to use and enter the system's email name. Type of email used is internet site because this type of email can be accessed through web broswer via a computer network. While the name of the email system is the hostname entered is already created when installing linux.

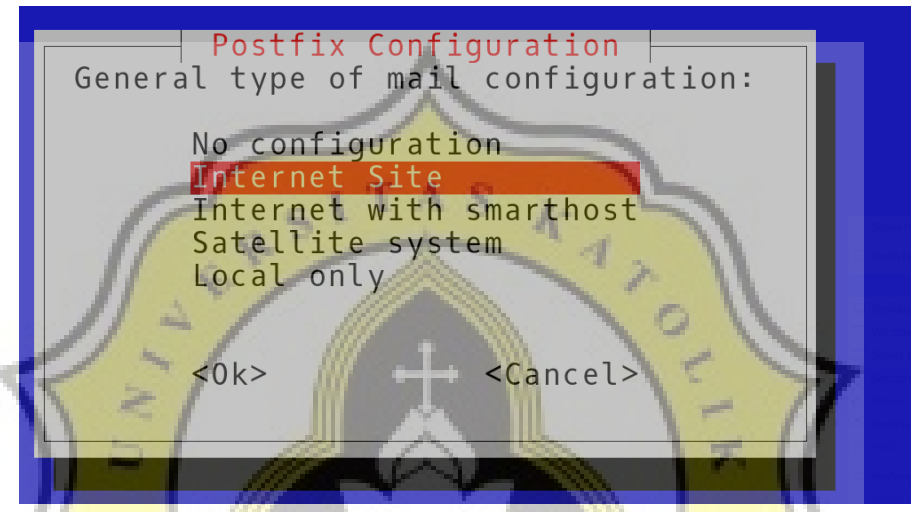

Illustration 5.6 Display To Choose The Type Of E-mail To Be Used.

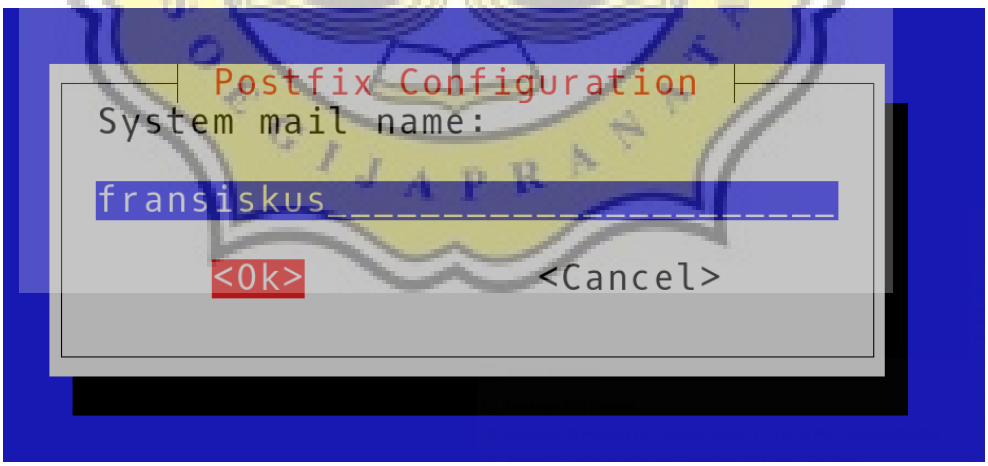

Illustration 5.7 Input System Mail Name.

7. Then edit the configuration file postfix in the directory/etc/postfix/master.cf.

nano /etc/postfix/master.cf

This configuration is used to enable the SMTP port used to send the e-mail. Uncomment on:

submission inet n - - - - smtpd

-o syslog_name=postfix/submission

-o smtpd_tls_security_level=encrypt

-o smtpd_sasl_auth_enable=yes

smtps inet n - - - - smtpd

-o syslog_name=postfix/smtps

-o smtpd_tls_wrappermode=yes

-o smtpd_sasl_auth_enable=yes

SASL itself useful for the security of the user when login using Roundcube. Then change the at-o smtpd_client_restrictions becomes

-o smtpd_client_restrictions = permit_sassl_authenticated, rejects.

This aim as a restriction permission to login to the account email server t hat has created and match the right username and password used to log what is appropriate or not.

8. After the configuration above, the next step is to restart the postfix to run postfix configuration.

   service postfix restart

9. Before installing mysql server to do is edit the mysql configuration file.

   nano /etc/postfix/master.cf

   Uncomment on :

   bind address = 127.0.0.1

   this aim so that mysql can be accessed online viai ISP Config.

10. Then install the mysql server and the mysql server configuration use:

    mysql_secure_installation

    The configuration of the mysql server in the form of filling the root password that will be used to login to the mysql server, remove the anonymous user so that people who do not have a user account cannot login, root login remotely in order to disallow mysql can be accessed by way of connect to the server and run mysqlnya a command to access the database, delete the test database, and reload privilege table now. All this configuration is used in order for the existing database in mysql be safe

    Enter current password for root (enter for none): <-- press enter

    Set root password? [Y/n] y

    New password: <-- 12345

    Re-enter new password: <-- 12345

    Remove anonymous users? [Y/n] <-- y

    Disallow root login remotely? [Y/n] <-- y

    Reload privilege tables now? [Y/n] <-- y

11. Then Restart Mysql server service

    service mysql restart

12. The next step is installing spamasssin and clamcav with:

    apt-get install spamassassin clamav clamav-daemon zoo unzip bzip2 arj nomarch lzop cabextract apt-listchanges libnet-ldap-perl libauthen-sasl-perl clamav-docs daemon libio-string-perl libio-socket-ssl-perl libnet-ident-perl zip libnet-dns-perl postgrey

13. Disable spamassasin.

    service spamassassin stop

update-rc.d -f spamassassin remove

Because the ISP config will call spamassasin when needed.

14. Install PHP Myadmin, apache web server, and PHP 7.0.

    apt-get install apache2 apache2-doc apache2-utils libapache2-mod-php php7.0 php7.0-common php7.0-gd php7.0-mysql php7.0-imap phpmyadmin php7.0-cli php7.0-cgi libapache2-mod-fcgid apache2-suexec-pristine php-pear php-auth php7.0-mcrypt mcrypt imagemagick libruby libapache2-mod-python php7.0-curl php7.0-intl php7.0-pspell php7.0-recode php7.0-sqlite3 php7.0-tidy php7.0-xmlrpc php7.0-xsl memcached php-memcache php-imagick php-gettext php7.0-zip php7.0-mbstring

15. PHP Myadmin Configuration. Configuration of choosing a web server that will be used for PHP Myadmin, and set the password mysql application in PHP Myadmin. The created password will be used to login to the Myadmin PHP page by using the root user. The web server to be used by PHP Myadmin uses apache 2.

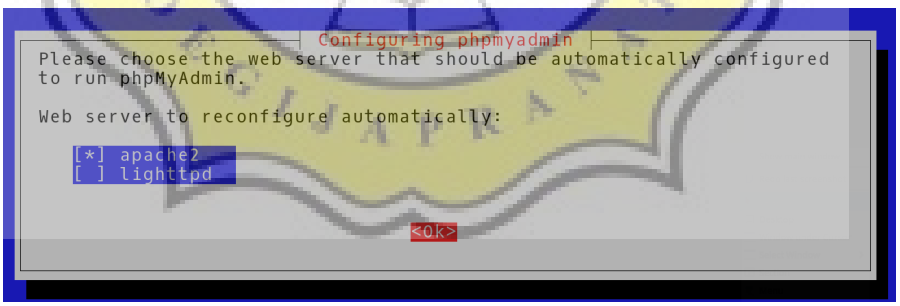

Illustration 5.8 The display For Select Webserver.

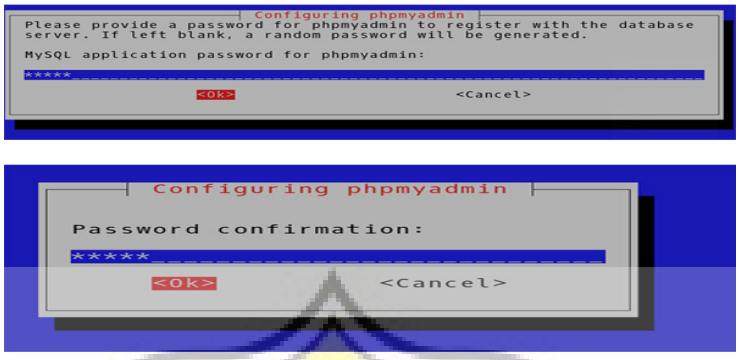

Illustration 5.9 Input PHP MyAdmin Password.

16. Then run the suexec rewrite ssl actions file include cgi in the Apache 2 directory.

    a2enmod suexec rewrite ssl actions include cgi

    The purpose of running this configuration is to write the certificate to be used by the ISP config as its security system.

17. After that run the configuration file also dav_fs auth_digest dav headers that are in the directory of apache2.

    a2enmod dav_fs dav auth_digest headers

    The purpose of running this Setup is so that the user can manage website files on the server.

18. Add a new configuration file with the name httproxy. conf in directory/etc/apache2/conf-available/.

    nano /etc/apache2/conf-available/httpoxy.conf

    The contents of the file are httproxy RequestHeader unset the Proxy early.

    RequestHeader unset Proxy early

Because with the httproxy.conf configuration file will overcome the attack by exploiting the deployment via HTTP Proxy that can change the url. then execute the config file httpoxy.

a2enconf httpoxy

19. Restart Service Apache2.

    service apache2 restart

20. Edit the mimetypes file in /etc/ directory.

    nano /etc/mime.types

    And uncomment on application / x-ruby rb.

    #application/x-ruby

    This configuration is intended to allow the ISP config to grant permissions for each user logged in to the ISP config page.

21. Restart Apache2 service.

    service apache2 restart

22. Install PHP Opcode Cache & PHP-FPM.

    apt-get install php7.0-opcache php-apcu libapache2-mod-fastcgi php7.0-fpm

23. Then run the configuration file actions fastcgi alias.

    a2enmod actions fastcgi alias

    This configuratio is required to make the process of opening the website faster.

24. Restart apache2 service.

    service apache2 restart

25. Install let's encrypt.

apt-get -y install letsencrypt

This software is useful to encrypt the SSL certificate that has been created and will be used for ISP config.

26. Install PureFTPd & Quota.

    apt-get install pure-ftpd-common pure-ftpd-mysql quota quotatool

27. Then edit the pure-ftpd-common configuration file in /etc/default/ directory.

    nano /etc/default/pure-ftpd-common

    And change virtualchroot to true.

    VIRTUALCHROOT=true

    This configuration is required for each user who will have their own directory which is like a directory / which can later be accessed by filezilla.

28. Then change the number on TLS in the / etc / pure-ftpd / conf / TLS directory to .

    echo 1 > /etc/pure-ftpd/conf/TLS

    The configuration is intended to enable TLS as an encryption which will then be used to login to the FTP user that has been created with the ISP config.

29. The next step is to create a parent directory.

    mkdir -p /etc/ssl/private/

    To save SSL keys that will be created later.

30. Then create an SSL certificate that has a validity period of up to 7300 days.

openssl req -x509 -nodes -days 7300 -newkey rsa:2048 -keyout /etc/ssl/private/pure-ftpd.pem -out /etc/ssl/private/pure-ftpd.pem

Open SSL itself is useful for encrypting the process of sending data from server to client or client to server.

31. Then fill in the SSL certificate by entering the country code, province name, city name, organization name, organization unit name, hostname on server, and e-mail address.

    Country Name (2 letter code) [AU]: <-- ID.

    State or Province Name (full name) [Some-State]: <-- Jawa tengah.

    Locality Name (eg, city) []: <-- Semarang.

    Organization Name (eg, company) [Internet Widgits Pty Ltd]: <-- Quantum

    Organizational Unit Name (eg, section) []: <-- Quantum

    Common Name (eg, YOUR name) []: <-- fransiskus

    Email Address []: <-- transient.exia@gmail.com

32. After that change the permission on pure-ftpd.pem.

    chmod 600 /etc/ssl/private/pure-ftpd.pem

    Chmod used is 600 so the owner can read and write on the file.

33. Restart pureftpd service.

    service pure-ftpd-mysql restart

34. The next step is to edit the configuration file in fstab.

    nano /etc/fstab

    And add configuration to set the quota limit of each user and group in the file system / thing that need to be added is in fstab configuration is

/ext4./dev/sda1 / ext4 defaults, noatime, usrjquota = quota.user, grpjquota = quota.group, jqfmt = vfsv0 0 1 / dev / sda5 none swap sw 0 0s

35. Then remount the / directory.

    mount -o remount /

    And turn on the qouta limit on all users and groups.

    quotaon -avug

36. Install bind dns.

    apt-get install bind9 dnsutils haveged

37. Install vlogger, webalizer and awstats.

    apt-get install vlogger webalizer awstats geoip-database libclass-dbi-mysql-perl

38. Edit the Configuration File in the directory in/etc/cron.d/awstats.

    nano /etc/cron.d/awstats

    then uncomment all configurations within awstats.

    #MAILTO=root

    #*/10 * * * * www-data [-x /usr/share/awstats/tools/update.sh] && /usr/share/awstats/tools/update.sh

    # Generate static reports:

    #10 03 * * * www-data [-x /usr/share/awstats/tools/buildstatic.sh] && /usr/share/awstats/tools/buildstatic.sh

    This configuration is done so that the update.sh and buildstatic.sh files are not backed up. If not tagged then the update.sh file will be backed up every 10 minutes and buildstatic will be backed up every 10 minutes once

and 3 hours once This configuration is also used to enable status in ISP config..

39. Install the software needed to install jailkit.

    apt-get install build-essential autoconf automake1.11 libtool flex bison debhelper binutils

40. Then go to the tmp directory and then download jailkit with wget. http://olivier.sessink.nl/jailkit/jailkit-2.19.tar.gz.

    cd /tmp

    wget http://olivier.sessink.nl/jailkit/jailkit-2.19.tar.gz

41. Extract the downloaded jailkit file and then go to the extracted jailkit folder.

    tar xvfz jailkit-2.19.tar.gz

    cd jailkit-2.19

42. Then execute on the debian / rules binary directory.

    ./debian/rules binary

43. After that return to direktory / tmp.

    cd ..

44. The next step is to install jailkit.

    dpkg -i jailkit_2.19-1_*.deb

    The jailkit itself is used to restrict user accounts to certain files by using chroot.

45. Install fail2ban.

    apt-get install fail2ban

Fail2ban is used to provide a rule like in IP Tables to perform a banned against failure in accessing the website.

46. Then create a new config file named jail.local in / etc / fail2ban / directory.

nano /etc/fail2ban/jail.local

The configuration content of jail.local is :

```
[pureftpd]
enabled                 =true
port                    =ftp
filter                  =pureftpd
logpath                 =var/log/syslog
maxretry                =3

[dovecot-pop3imap]
enabled                 =true
filter                  =dovecot-pop3imap
action                  =iptables-multiport[name=dovecot-
        pop3imap,port="pop3,pop3s,imap,imaps",protocol=tcp]
logpath                 =/var/log/mail.log
maxretry                =5

[postfix-sasl]
enabled                 =true
port                    =smtp
filter                  =postfix-sasl
```

logpath =/var/log/mail.log

maxretry = 3

This configuration is useful for enabling FTP, postfix, and dovecot. And configured it also set the IMAP and POP 3 ports on dovecot. And every file transfer and send email using POP3 and IMAP to be saved through log file.

47. After that create a new configuration file named pureftpd.conf in /etc/fail2ban/filter.d/ directory.

    nano /etc/fail2ban/filter.d/pureftpd.conf

    The contents of the configuration file is :

    [Definition]
    failregex =.*pure-ftpd:(.*@[WARNING Authentication failed for user.*
    ignoreregex =

    Configuration is useful for filtering any existing user such as if user and passsword are not appropriate then it will not be able to login via FTP server.

48. Then create a new configuration file named dovecot-pop3imap.conf in the /etc/fail2ban/filter.d/ directory

    nano /etc/fail2ban/filter.d/dovecot-pop3imap.conf

    The contents of the configuration file is :

    [Definition]

    failregex = (?: pop3-login|imap-login): .*(?:Authentication failure| Aborted login (auth failed|Aborted login (tried to use disabled| Disconnected (auth failed|Aborted login (d+ authentication attempts).*rip=(?PS*),.*

ignoreregex =

Configuration is useful for filtering every user who will login in the mail server as an example if the user and passsword does not match then it will not be able to login in the mail server.

49. The next step is to change the configuration in /etc/fail2ban/filter.d/postfix-sasl.conf to ignoreregex.

    echo "ignoreregex =" >> /etc/fail2ban/filter.d/postfix-sasl.conf

    This configuration is done to add the line ignoreregex is missing on the file postfix-sasl.

50. Restart Fail2ban2 service.

    service fail2ban restart

51. Install Roundcube Web Mail.

    apt-get install roundcube roundcube-core roundcube-mysql roundcube-plugins roundcube-plugins-extra javascript-common libjs-jquery-mousewheel php-net-sieve tinymce

52. Configure Mysql password for roundcube web mail. This configuration is useful for making connections between databases with roundcube web mail.

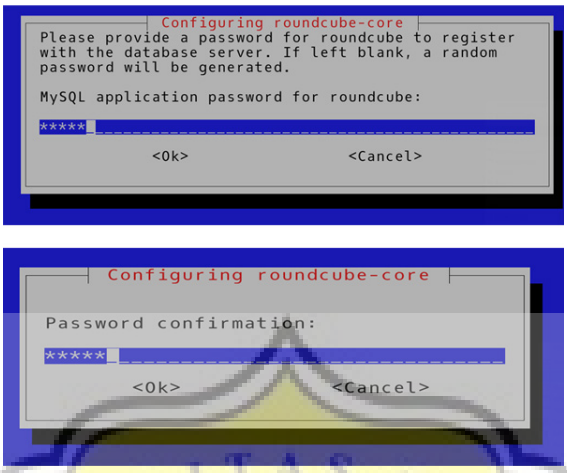

Illustration 5.10 Display To Enter Mysql Password On Roundcube

53. Edit the roundcube.conf configuration file in the / etc / apache2 / conf-enabled / directory.

    nano /etc/apache2/conf-enabled/roundcube.conf

    Uncomment on the third line and add AddType application / x-httpd-php.php in the configuration under the deleted configuration

    Alias /webmail /var/lib/roundcube

    AddType application/x-httpd-php .php

    This configuration aims to roundube web mail can be accessed by web broswer.

54. Edit config.inc.php config file in / etc / roundcube / directory.

    nano /etc/roundcube/config.inc.php

    then fill in $ config ['default_host'] = ''; with localhost

    $config['default_host'] = 'localhost';

    This configuration is useful for roundcube web mail can be accessed via LAN network.

55. Restart Apache2 service.

    service apache2 restart

56. Download file isp config in directory tmp

    wget -O ispconfig.tar.gz https://git.ispconfig.org/ispconfig/ispconfig3/repository/archive.tar.gz?ref=stable-3.1

57. After that the extracted ispconfig file has been downloaded.

    tar xfz ispconfig.tar.gz

58. Then go to the directory / ispconfigs / install.

    cd ispconfig3*/install/

59. After that run ISP config installation file.

    php -q install.php

60. Then fill in the language used to install ispconfig, installation mode, mysql hostname, mysql port, mysq; username, mysql password, database, mysql charset, and fill ssl already created.

    Select language (en,de) [en]: en

    Installation mode (standard,expert) [standard]: standard

    Full qualified hostname (FQDN) of the server, eg server1.domain.tld [fransiskus]: fransiskus

    MySQL server hostname [localhost]: localhost

    MySQL server port [3306]: 3306

    MySQL root username [root]: root

    MySQL root password []: 12345

    MySQL database to create [dbispconfig]: dbispconfig

MySQL charset [utf8]: utf8

Configuring Postgrey

Configuring Postfix

Generating a 4096 bit RSA private key .....++

.....

.....++

writing new private key to 'smtpd.key'

You are about to be asked to enter information that will be incorporated

into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', the field will be left blank.

Country Name (2 letter code) [AU]: ID

State or Province Name (full name) [Some-State]: Jawa Tengah

Locality Name (eg, city) []: Semarang

Organization Name (eg, company) [Internet Widgits Pty Ltd]: Quantum

Organizational Unit Name (eg, section) []: Quantum

Common Name (e.g. server FQDN or YOUR name) []: fransiskus

Email Address []: transient.exia@gmail.com

61. After that fill in the port used to open ispconfignya and also fill in the password to login to ispconfig and re-fill the ssl to be created.

Configuring Getmail

Configuring BIND

Configuring Jailkit

Configuring Pureftpd

Configuring Apache

Configuring vlogger

Configuring Metronome XMPP Server

Configuring Ubuntu Firewall

Configuring Fail2ban

[INFO] service OpenVZ not detected

Configuring Apps vhost

Installing ISPConfig

ISPConfig Port [8080]: 8080

Admin password [admin]: admin

Do you want a secure (SSL) connection to the ISPConfig web interface (y,n) [y]: y

Generating RSA private key, 4096 bit long modulus

.....++

.....

.....++

e is 65537 (0x10001)

You are about to be asked to enter information that will be incorporated

into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', the field will be left blank.

Country Name (2 letter code) [AU]: ID

State or Province Name (full name) [Some-State]: Jawa Tengah

Locality Name (eg, city) []: Semarang

Organization Name (eg, company) [Internet Widgits Pty Ltd]: Quantum

Organizational Unit Name (eg, section) []: Quantum

Common Name (e.g. server FQDN or YOUR name) []: fransiskus

Email Address []: transient.exia@gmail.com

Please enter the following 'extra' attributes

to be sent with your certificate request

A challenge password []: 12345

An optional company name []: quantum

writing RSA key

62. Wait until the installation process is complete.

Configuring DBServer

Installing ISPConfig crontab

no crontab for root

no crontab for getmail

Detect IP addresses

Restarting services ...

Installation completed.

63. After that update user in mysql

    echo "update user set plugin='' where User='root';" | mysql -root -p mysql

    This configuration is required for existing users in the database to be updated.

64. Then sync ispconfig with server

    sync

    This configuration is required for ISP config to be accessible in the web broswer.

65. Then restart the computer

    reboot

66. Open the web broswer with https: // ipaddress: 8080 to make sure ispconfig has been successfully installed.

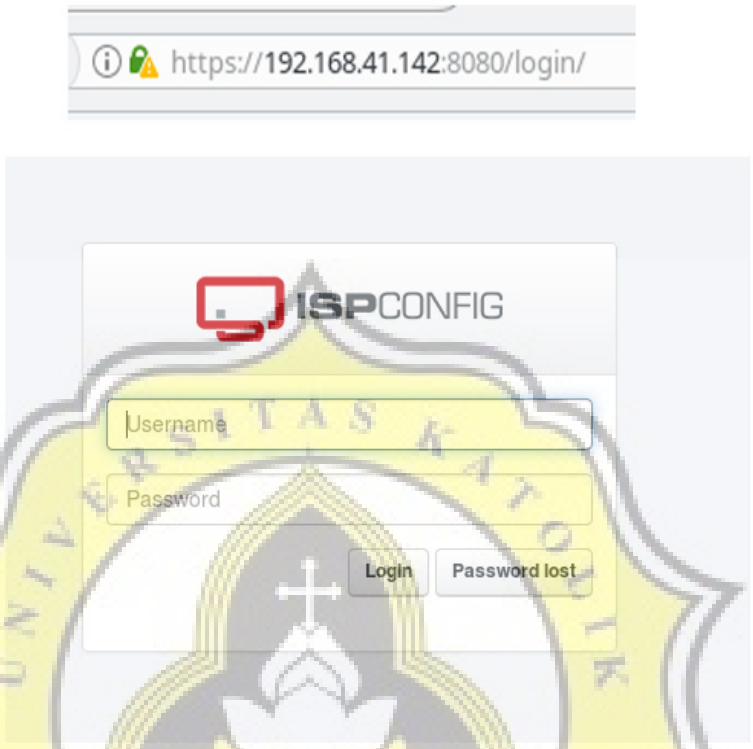

Illustration 5.11 Homepage ISP Config.

Create Clients

1. Login first to the ISP Config page.

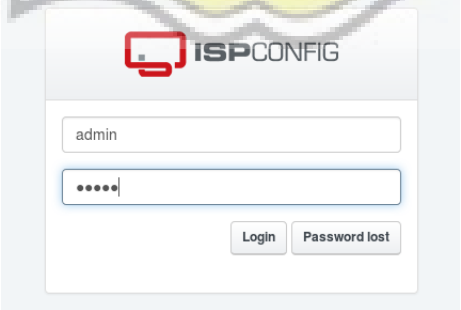

Illustration 5.12 Login To ISP Config.

2. The next step is to click on the clients menu. After that click add new client to add client.

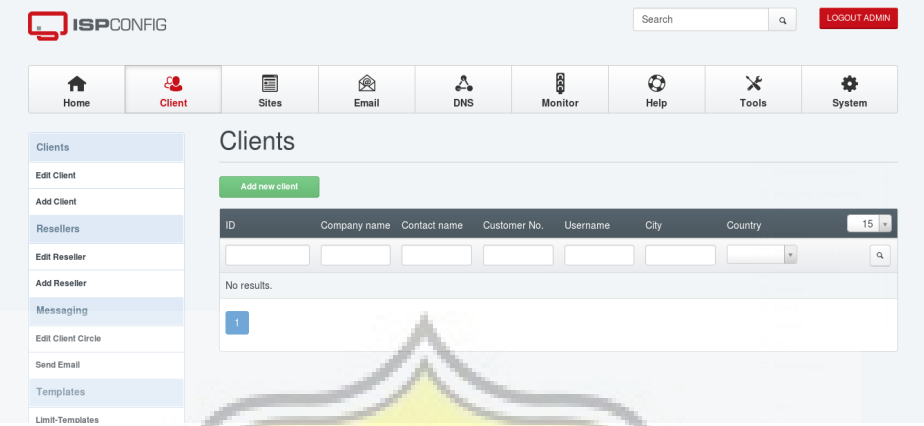

Illustration 5.13 Menu Clients

3. After that fill the client data. The data that needs to be filled is the company name, title, first name on contact, contact name, passsword, and email.

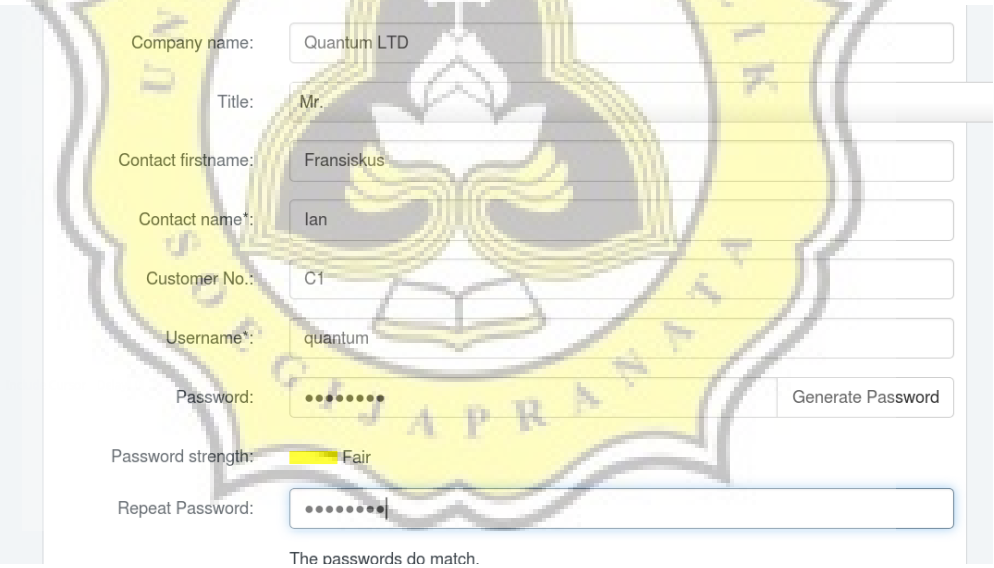

Illustration 5.14 Fill Clients Data.

Illustration 5.15 Fill E-mail Clients.

4. Then click on save to add new client.

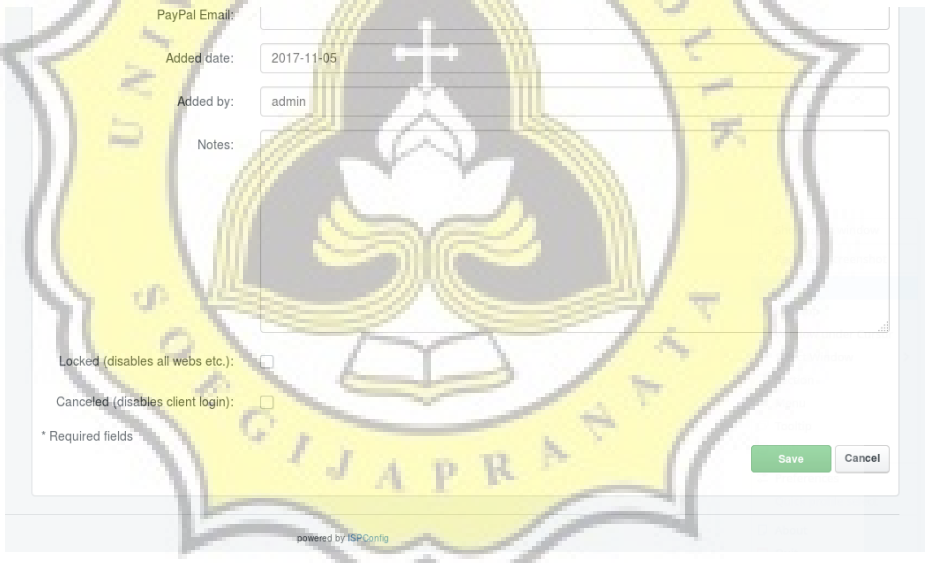

Illustration 5.16 Save Clients.

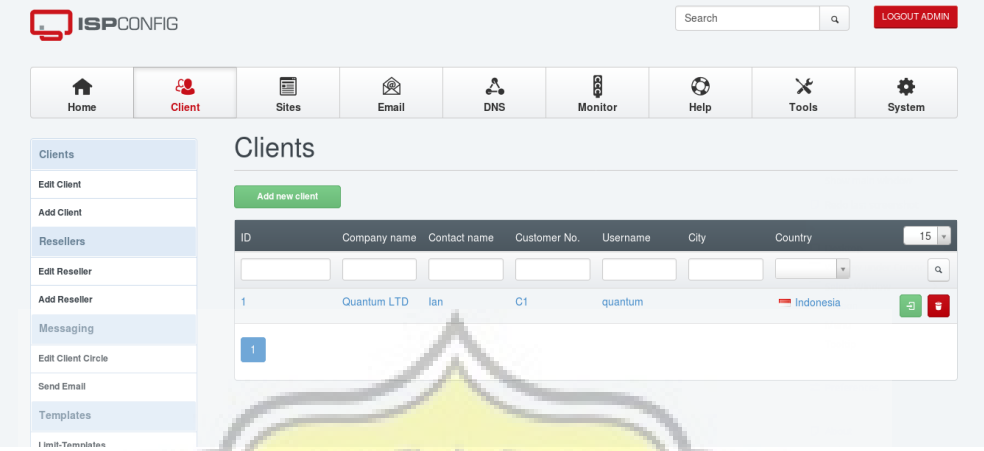

Illustration 5.17 Display After Client Successfully Created.

Create Web Hosting

1. Click on the sites menu then click a new websites.

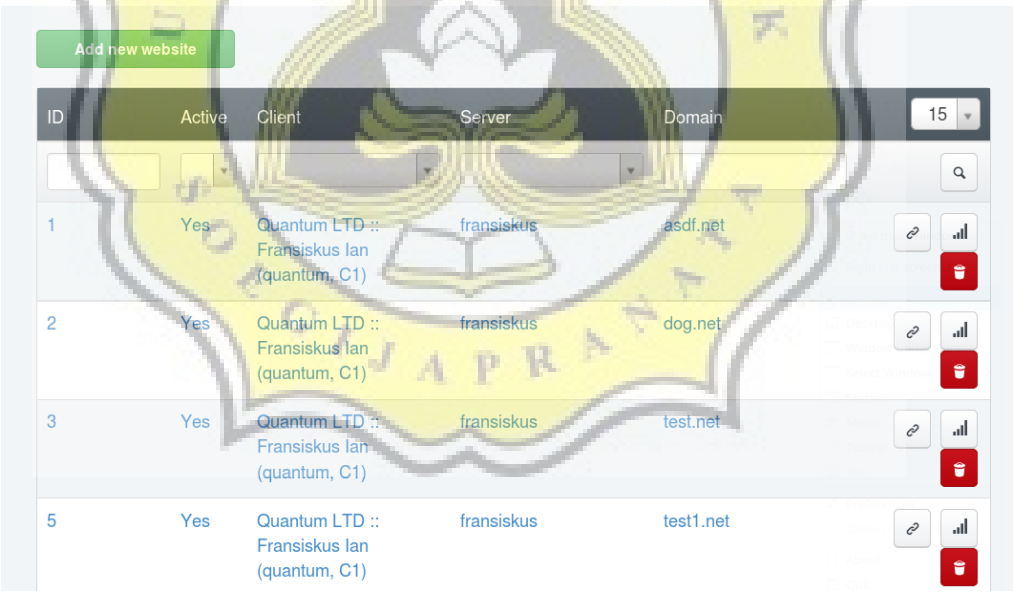

Illustration 5.18 Display To Create A Website.

2. Then select the server used, select the client that has been created, select the ip address used on the server computer, fill in the desired website name then click save to save the name of the website.

Illustration 5.19 Display To Fill Website Name.

3. Click on DNS then click add new DNS zone with wizard. This configuration is required so that the name of websites that have been created can be accessed through web broswer with domain asdf.net.

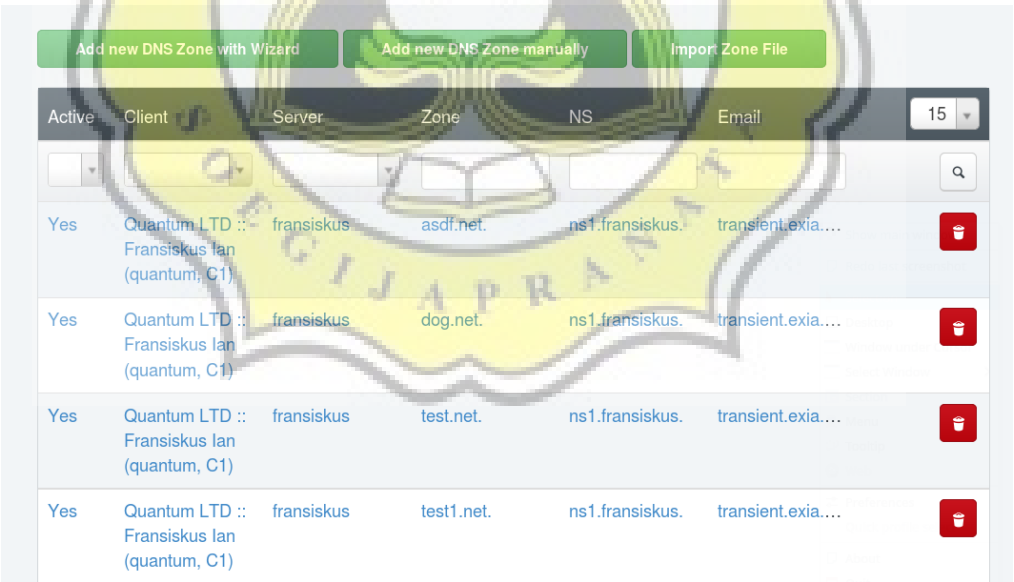

Illustration 5.20 Menu DNS.

4. Then select the server name, select the client used to create the website, the contents of the domain in accordance with the name of the website that has been created, select ip address for the server, fill in NS 1 and NS2 with

ns1.namaserver and ns2.namaserver, and also fill email address user, then click save to save this dns configuration.

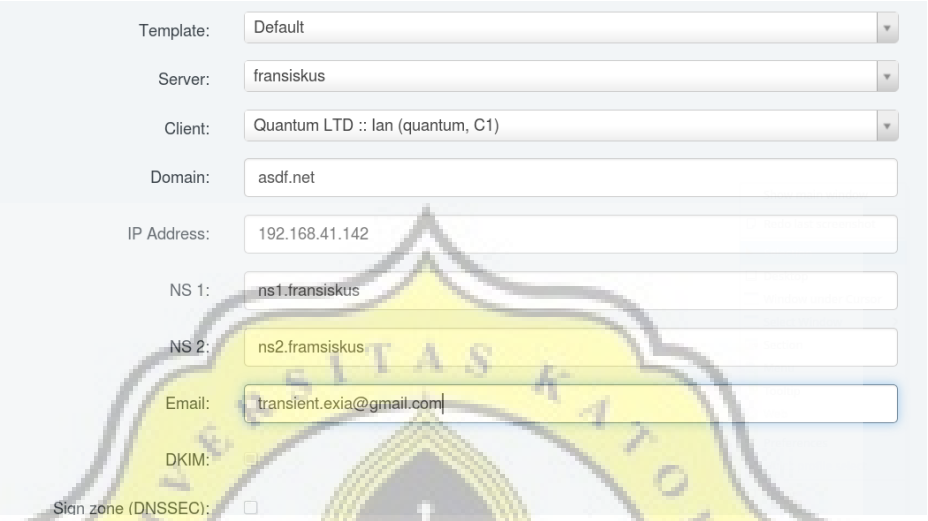

Illustration 5.21 DNS Configuration.

5. Setting the DNS IP belongs to the client computer. Filled in accordance with DNS IP Server to access domains that have been made in the ISP Config.

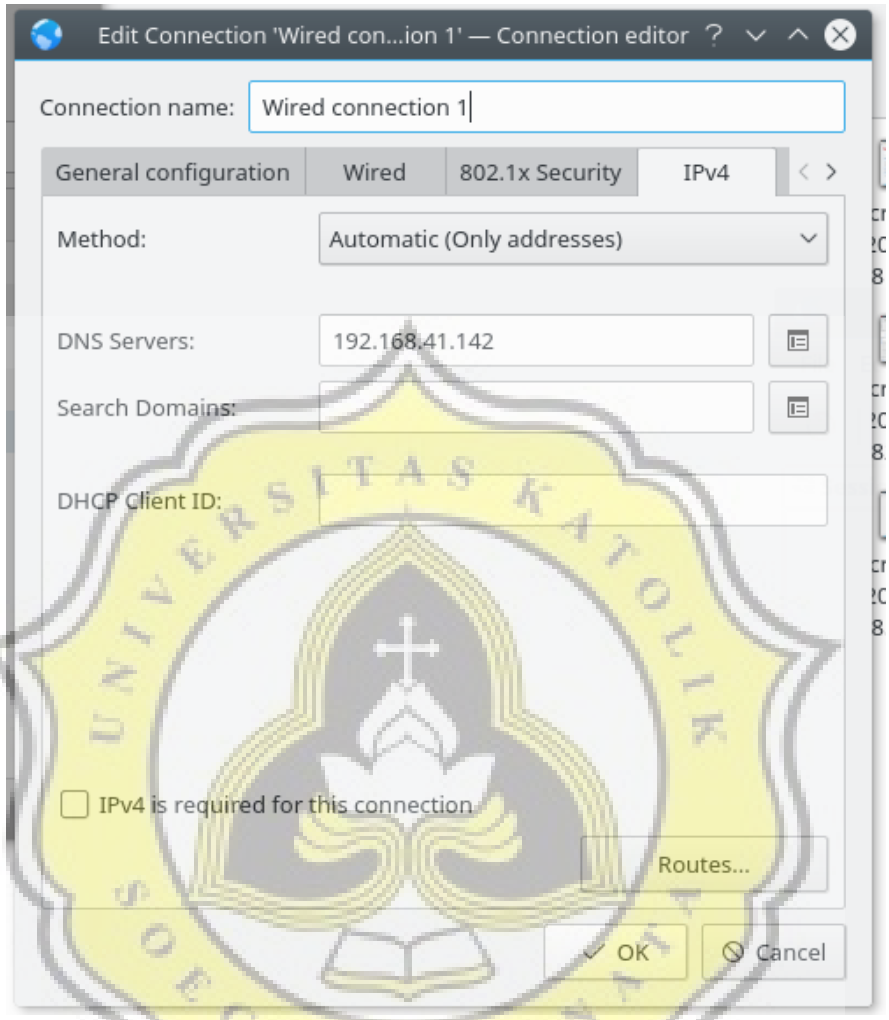

Illustration 5.22 IP DNS Configuration.

6. After that try domain website that has been made in web broswer. If it is successful then it will appear welcome to your website.

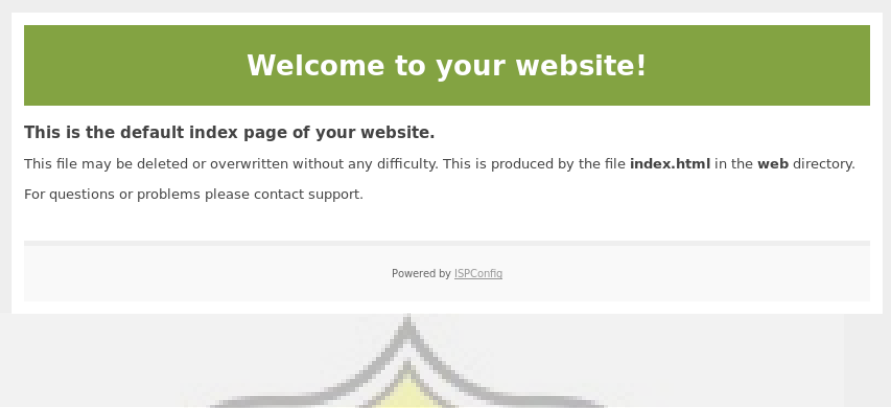

Illustration 5.23 Displays Websites That Have Been Created.

7. The next step is to click back on the menu sites then click on sub menu FTP-accounts, then click add new FTP-User.

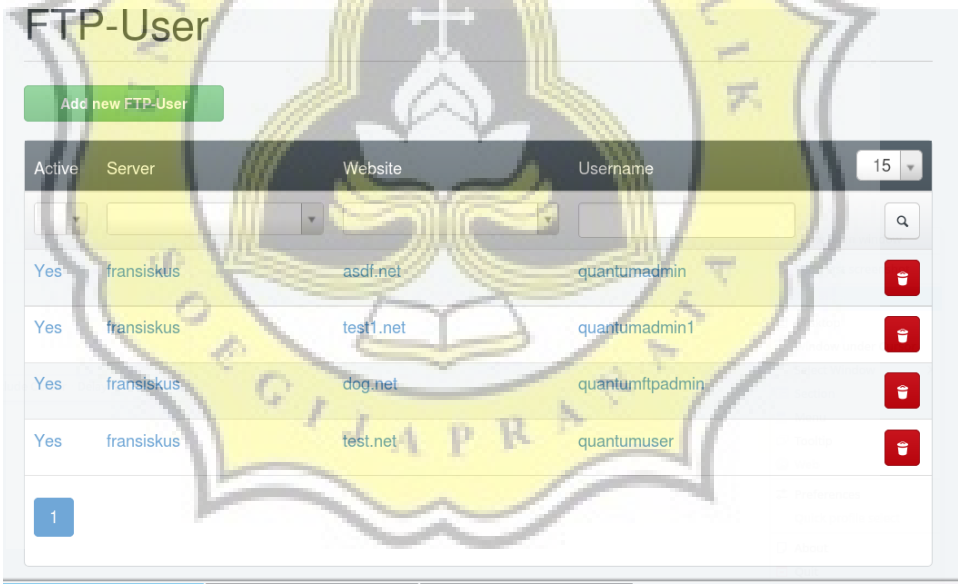

Illustration 5.24 Submenu FTP Accounts.

8. Then select the name of websites that has been created, fill in the username and password that will be used to login, then click save.

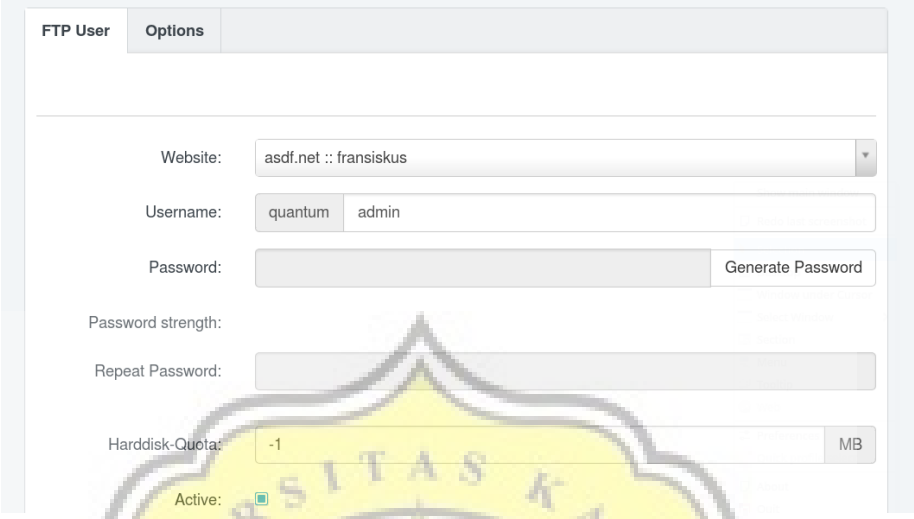

Illustration 5.25 FTP Account Configuration.

9. The next step is to click on the sub menu of the database user and then click add new user to add a user database.

Illustration 5.26 Submenu Database User.

10. Then choose the client that will be used, enter the user name and password database, then click save to save database user that will be used to save database from website which have been prepared.

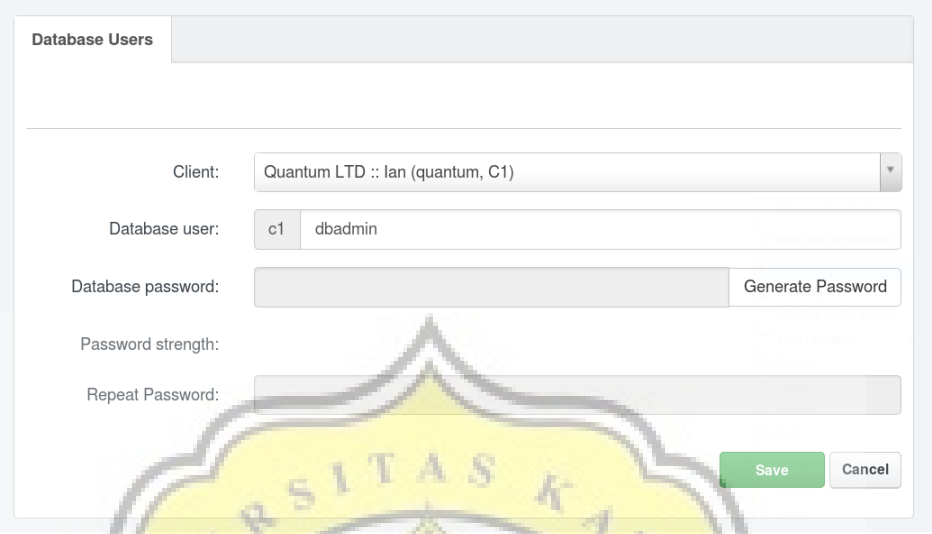

Illustration 5.27 Database User Configuration.

11. After that click on submenu database, then click add new database.

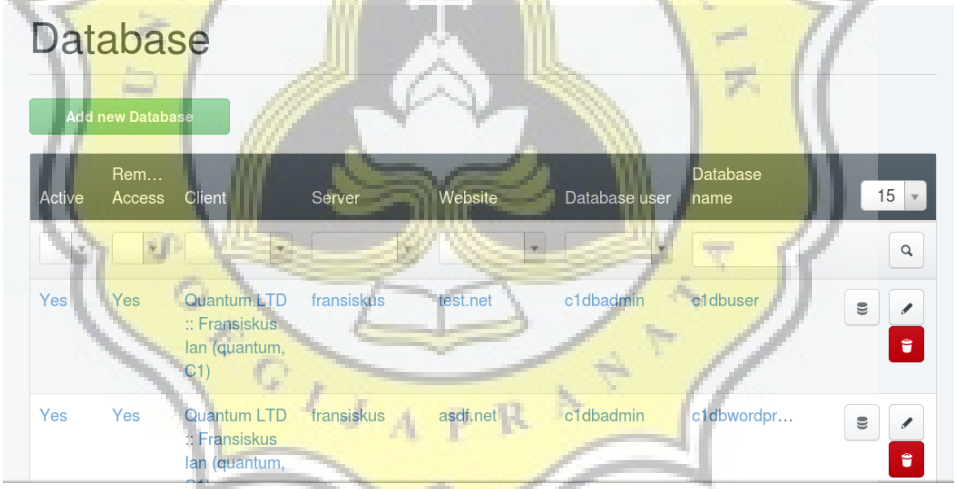

Illustration 5.28 Submenu Database.

12. Then select the name of the server used, select the name of the website to be used, select the database type, fill in the name of the database you want created, select the user database created, put the remote access, then click save. This configuration is required to create a database as a website storage that has been prepared.

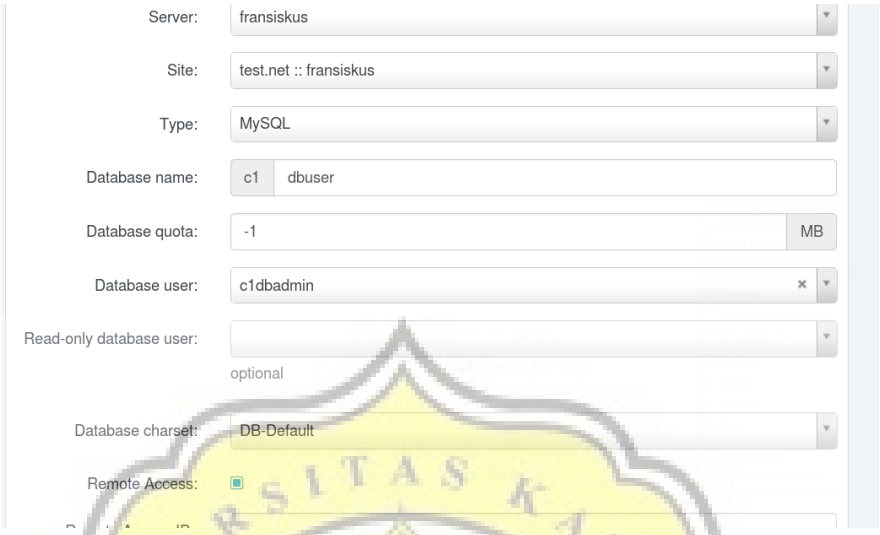

Illustration 5.29 Database Configuration.

13. The next step is to open filezilla to upload website files from client to server.

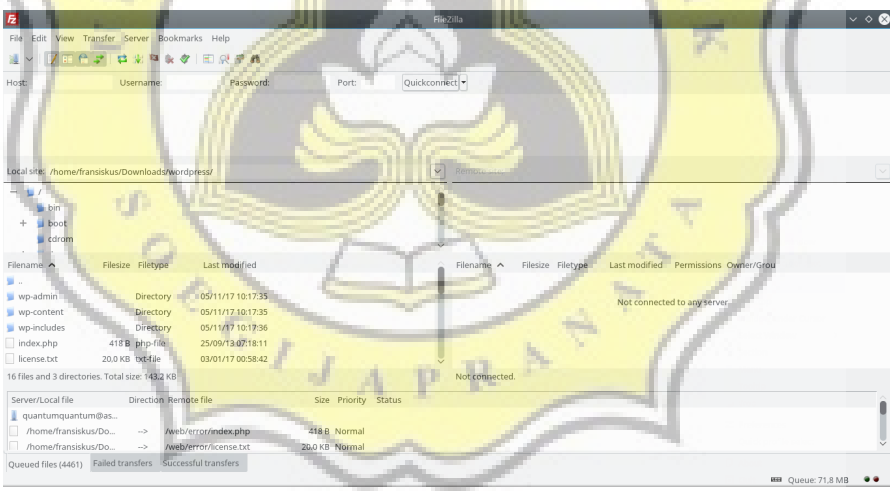

Illustration 5.30 Filezilla.

14. Then fill in the hostname, username and password that have been created. For the hostname to be filled with the website name that has been created After that, click the quick connect to connect to the FTP server that was created in the ISP config.

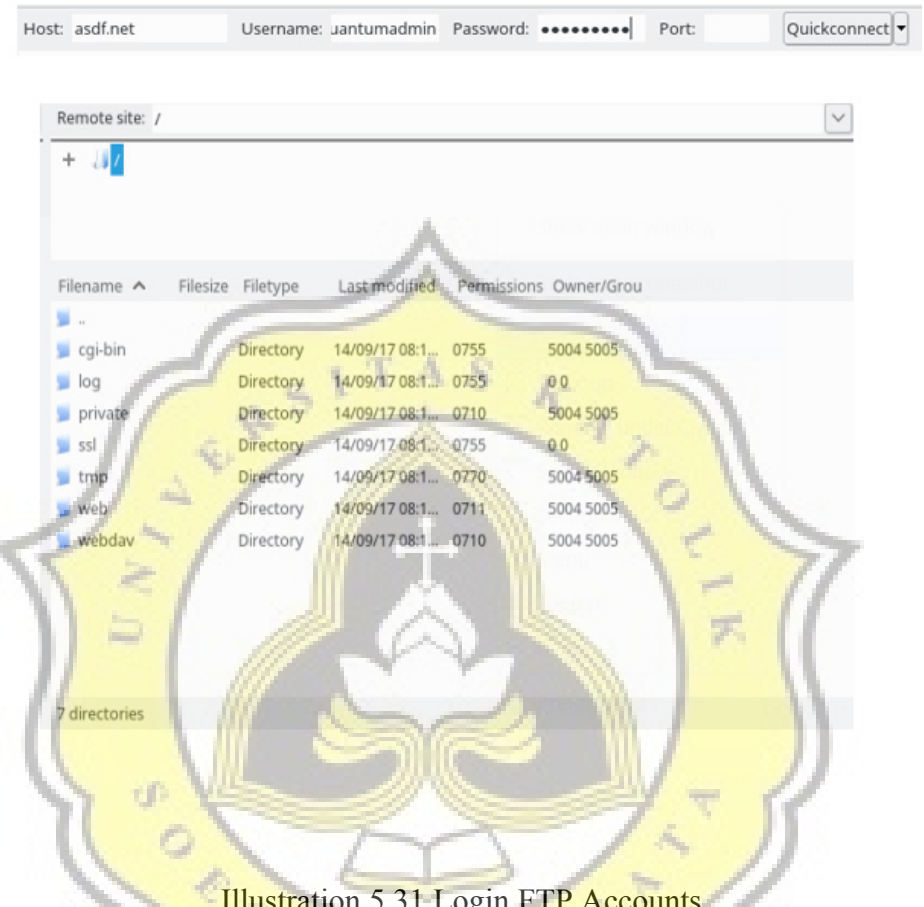

Illustration 5.31 Login FTP Accounts.

15. After successfully connect to the FTP server the next step is to upload the website from the home directory to the directory / web / on the FTP server.

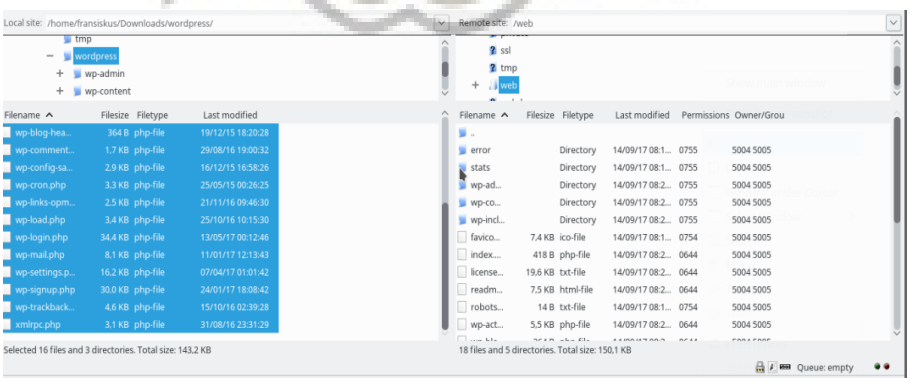

Illustration 5.32 FTP Server Upload Result.

16. The next step is to open a website that has been created as example asdf.net to web broswer, if successful upload file from server to client it will appear result from website already uploaded.

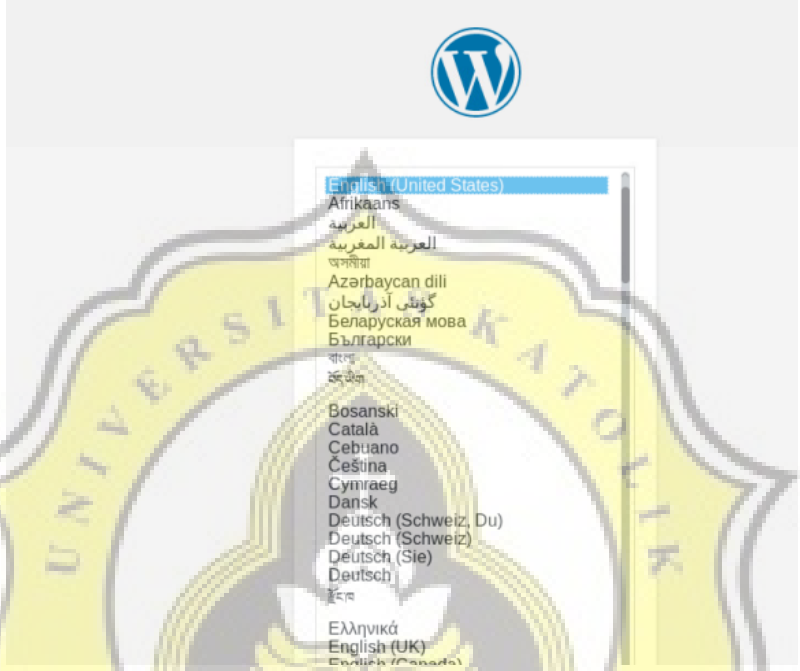

Illustration 5.33 Website Pageviews That Have Been Successfully Uploaded.

Install WordPress on ISP config.

1. Select the language that will be used to install wordpress.

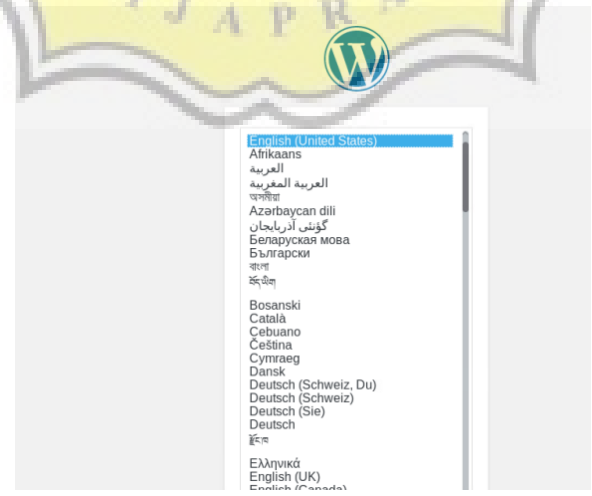

Illustration 5.34 Display To Select Installation Language.

2. Fill in the name of the database that has been created, username and password for the database, the contents of the database host with localhost, then click submit to continue installation.

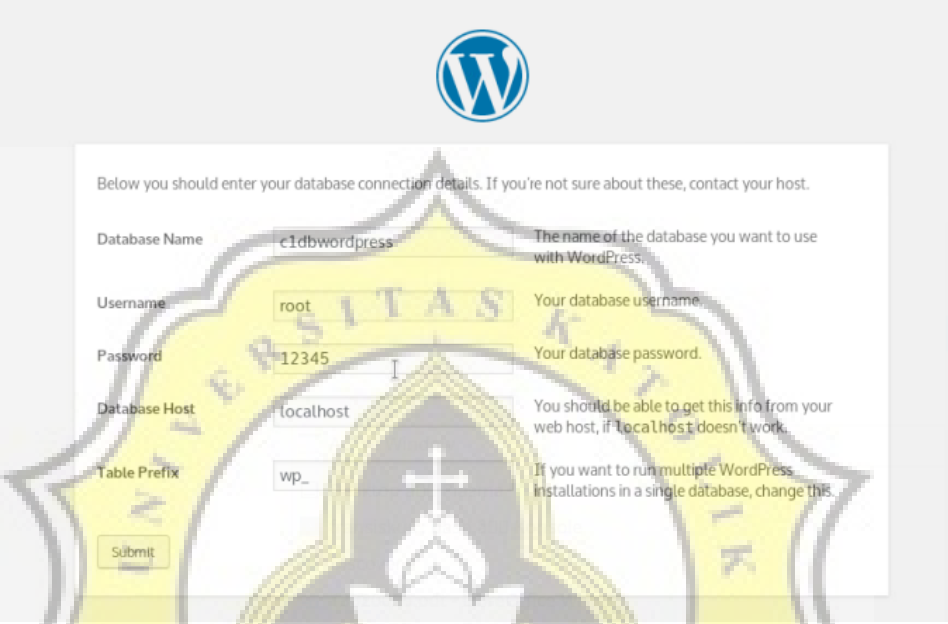

Illustration 5.35 Display To Fill The Database To Be Used.

3. After that the contents of the title wordpress liking, fill in your username and password to login to your wordpress will be installed, enter the email address, then click install wordpress.

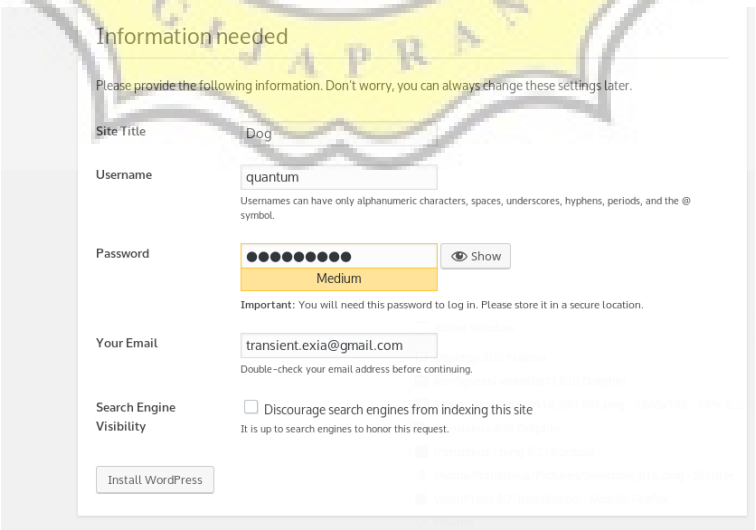

Illustration 5.36 Wordpress Configuration.

4. If the installation was successfully then it will appear the words succes and it appears the username and password information has been created.

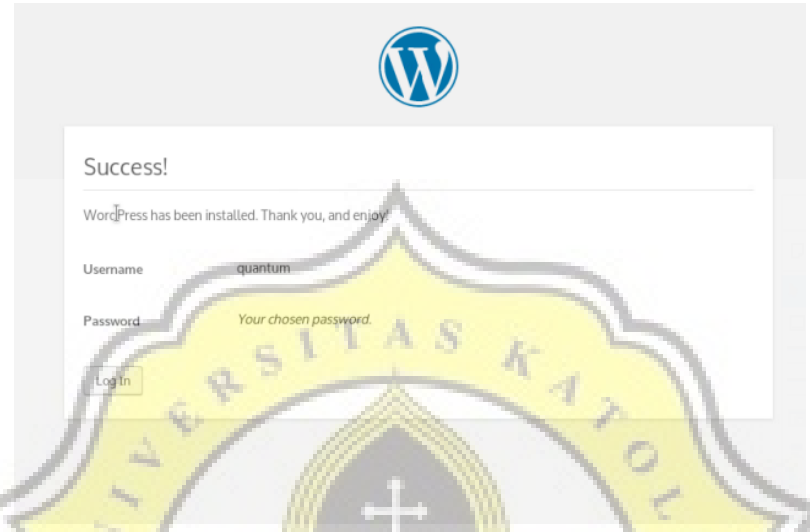

Illustration 5.37 Display After WordPress Installed Successfully.

Illustration 5.38 Wordpress Pages That Are Already Installed.

5.2 Testing

Testing in this project is trying to login to the page wordpress, add postings on wordpress, and display the results of articles that have been inputed.

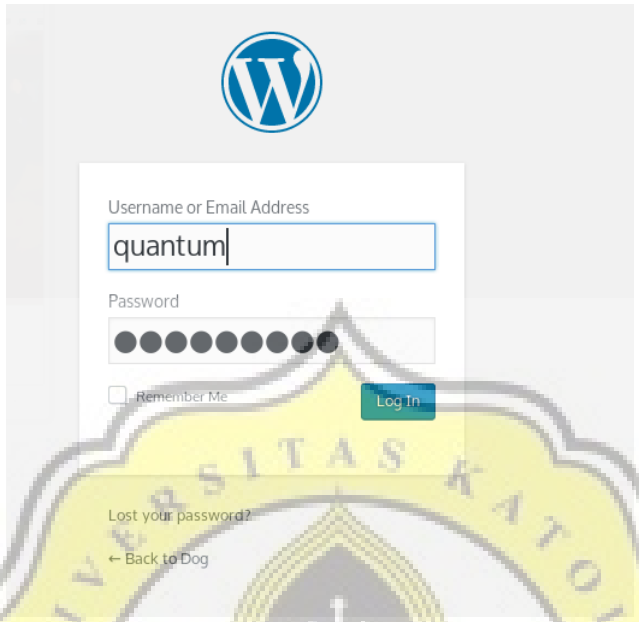

Illustration 5.39 Page To Sign Into WordPress Account.

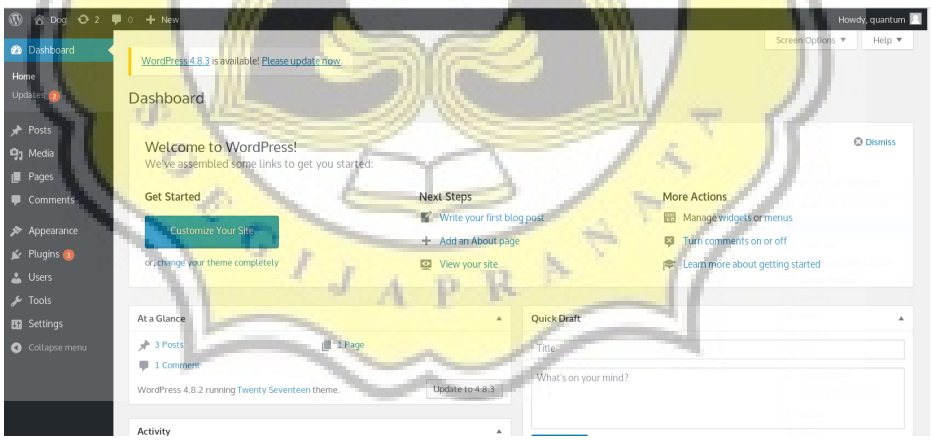

Illustration 5.40 Display After Login.

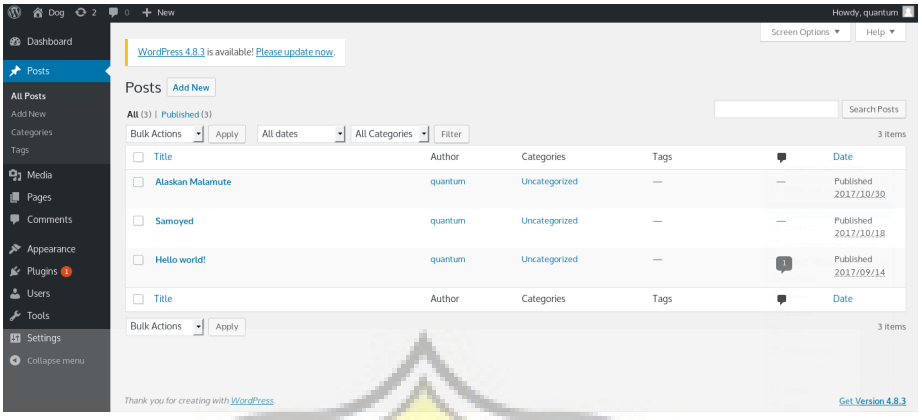

Illustration 5.41 Pages That Contain Articles That Have Been Created.

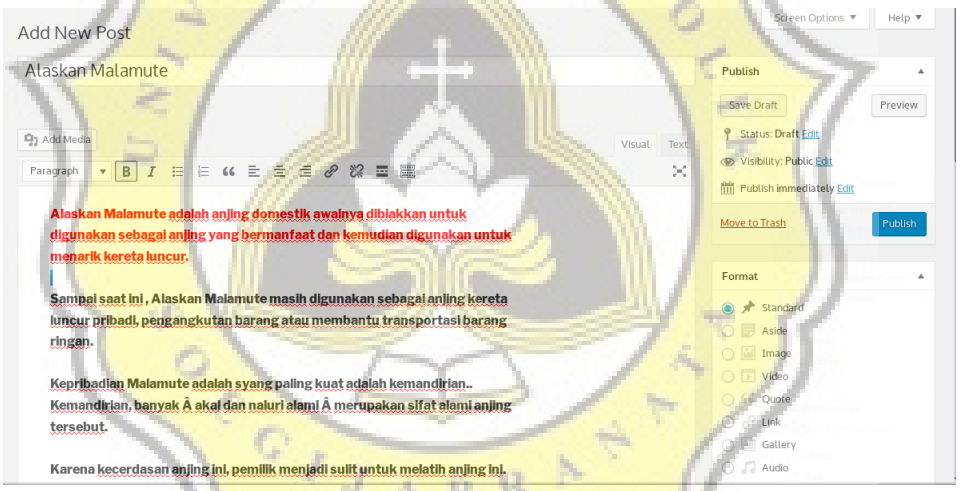

Illustration 5.42 Display To Add New Articles.

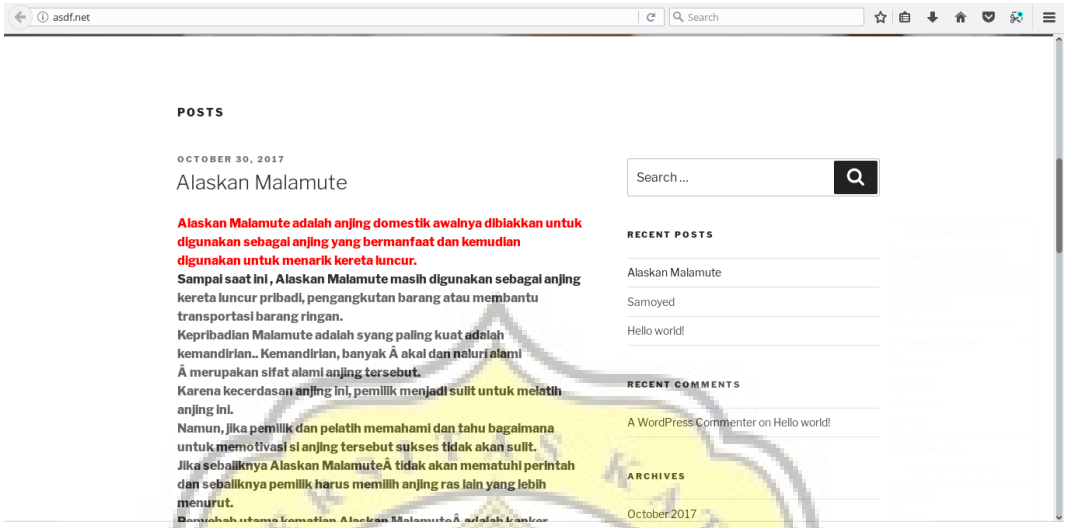

Illustration 5.43 Display Articles In The Wordpress Page.