SYSTEM AND NETWORK ADMINISTRATION

How to set up a website for a company

K.M.Piyumal

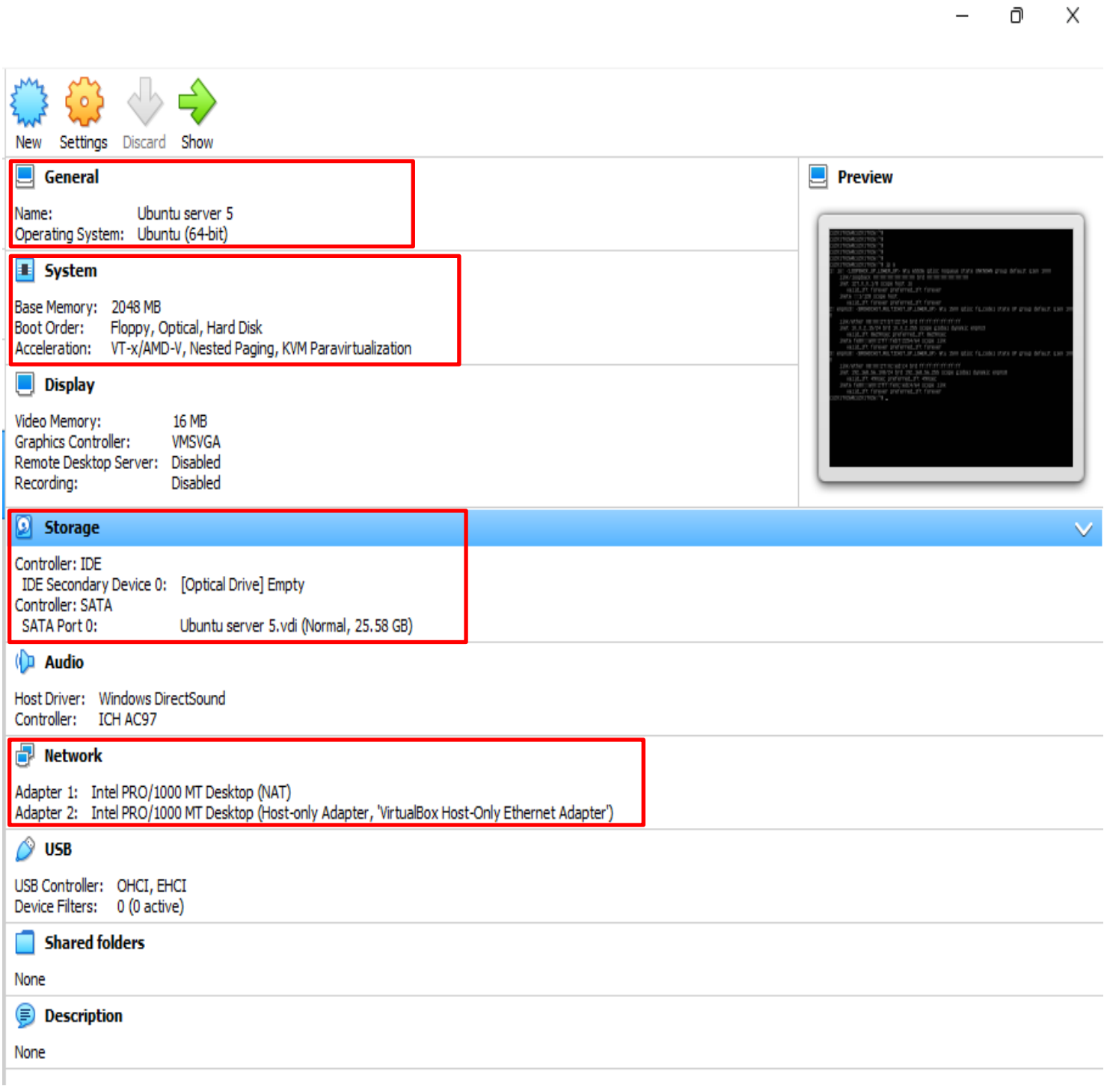
Table of contents

1.Introduction

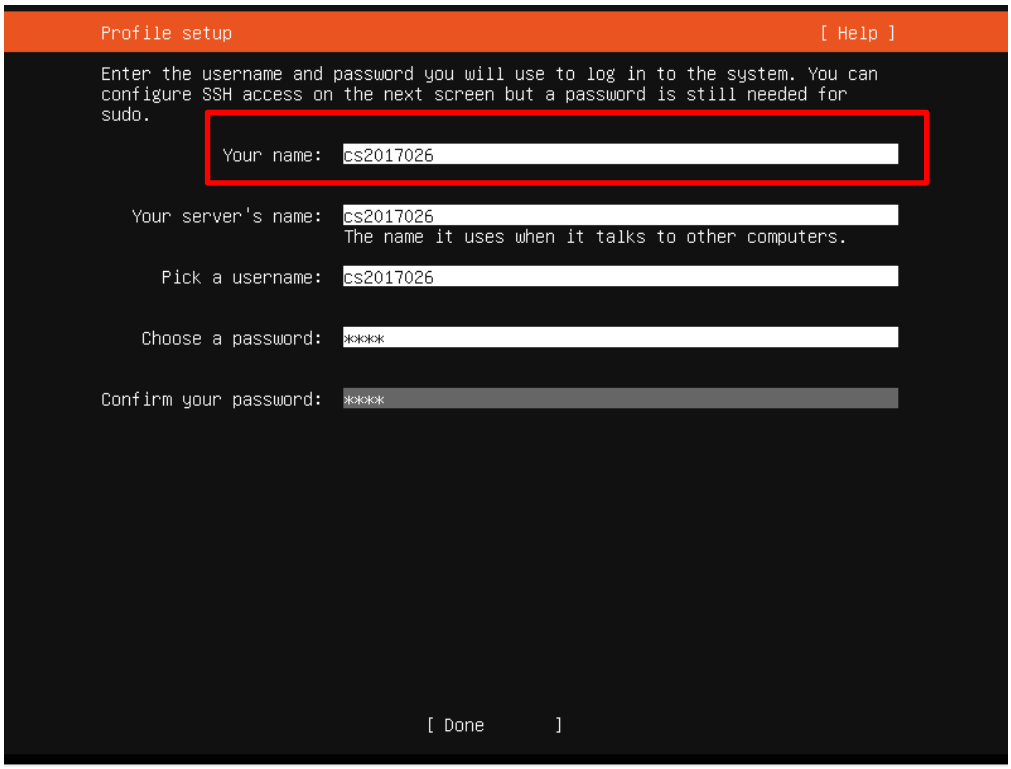
In this tutorial we are mainly discuss about how to set up a website for a company. So, this is quite a sample document about setting up a company website. Mainly there are two methos to set up a website for a company. They are LAMP and LEMP methods. In LAMP method, we use Linux operating system, Apache server, MySQL database and Php to configure the website. In the LEMP method, we use Linux operating system, Nginx server, MariaDB database and PHP to configure the website. So, at first, we configure the LAMP environments and then configure the SSL Certificate with our server and finally install the WordPress Content Management System. Also, Oracle VM VirtualBox is another major resource for our task. So, you can get, how combine these things to create the web server using this report.

1.Basic Configurations

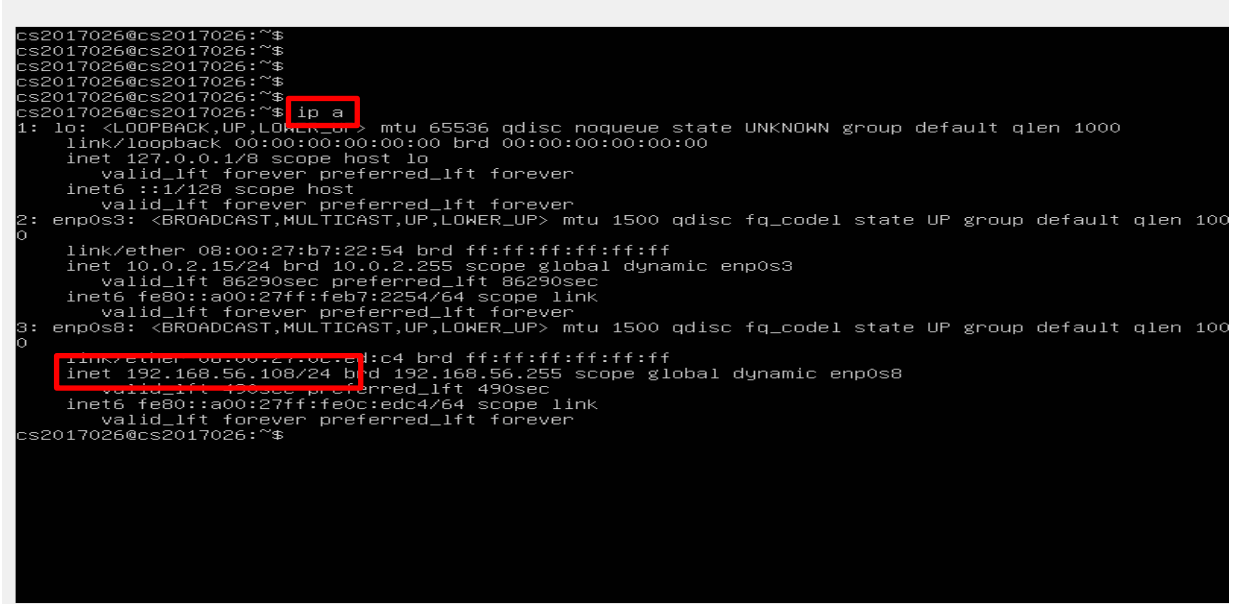
- This tutorial begins with the Oracle VM Virtual machine. So, I used Oracle VM virtual machine to install the linux environment. I used ubuntu server version 20.04.3 as my server machine. The below shows specification of my ubuntu server.



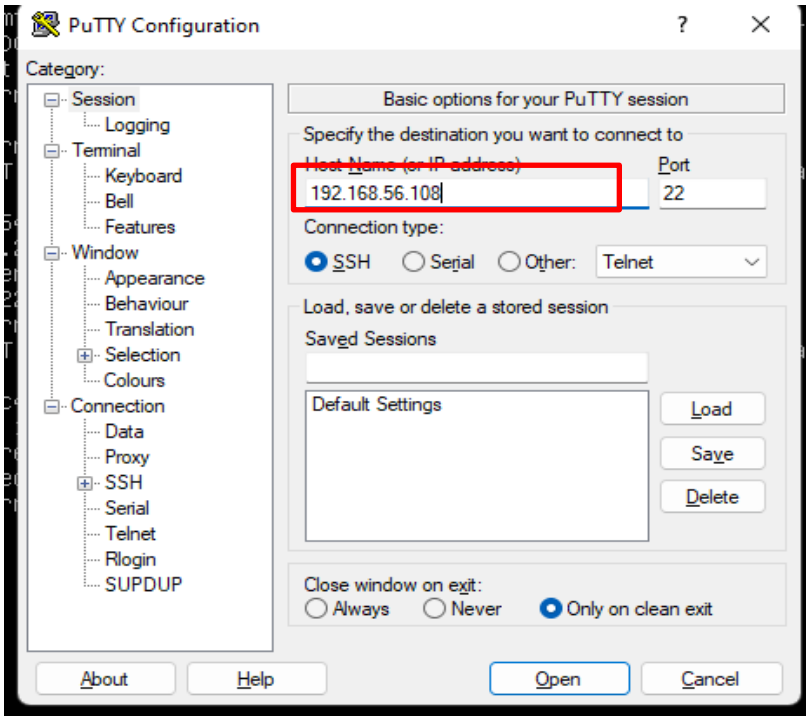
- In this machine I used 2048 MB of base memory, and approximately 25 GB of secondary storage, NAT adapter and host only adapter for configure the networks. After the configuration of ubuntu server, I installed the ubuntu server on Virtual machine. So, in the host name I used my student number. Below figure has shown it.



- After the installation, I gave the credentials to log into the system and then I got the ip address of my virtual machine using the 'ip a' command.



- So, my ip address was 192.168.56.108. Then, I used this ip address to log into the SSH and telnet client called putty. Putty's SSH provides secure, encrypted connection to the remote system. The bellow figure has shown this.



- Then, I logged into the putty using my username and password of ubuntu server. After, I updated the ubuntu server using bellow command.

```
4 updates can be applied immediately.
To see these additional updates run: apt list --upgradable


Last login: Tue Sep 14 13:57:32 2021
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

cs2017026@cs2017026:~$ sudo apt update
[sudo] password for cs2017026:
```

- In this command,

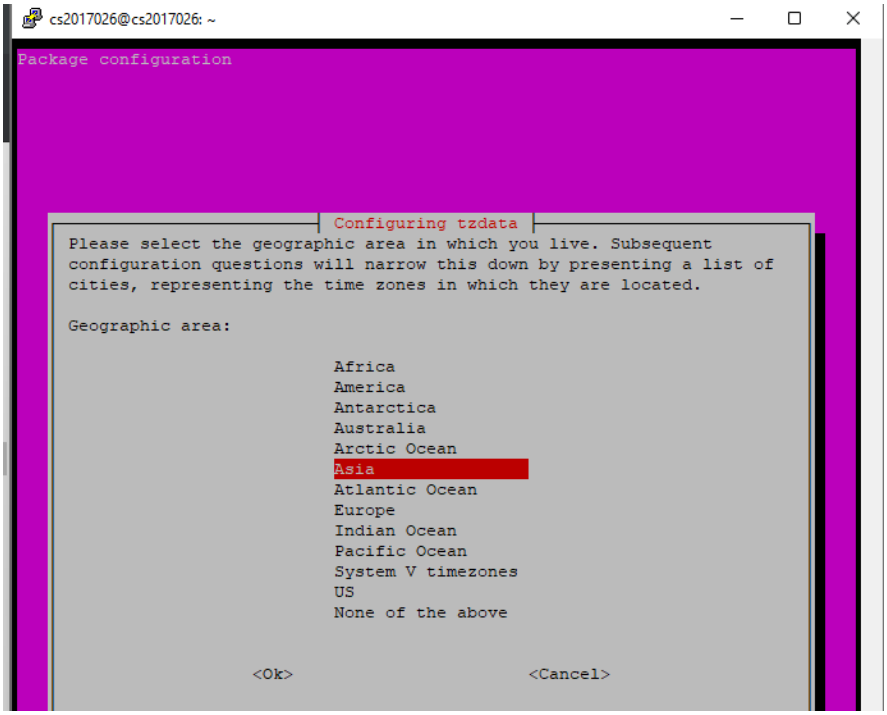
  sudo – Super user(root)
  apt – Advanced Package Tool
  This command is used to update ubuntu machine as super user.

- After, I set the time zone of ubuntu machine. For that, I used the following command.

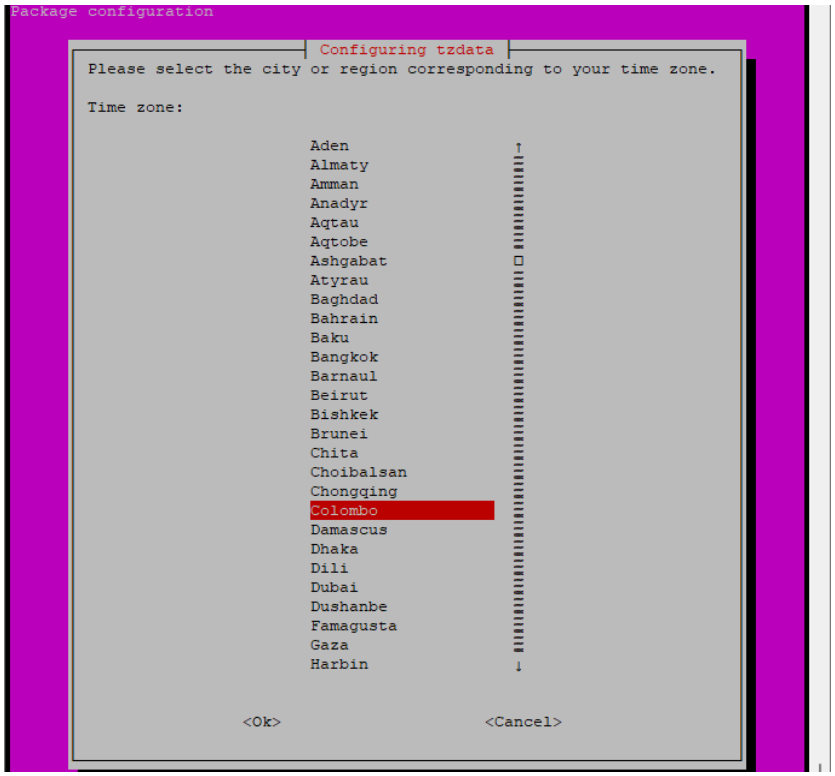
```
cs2017026@cs2017026:~$ sudo dpkg-reconfigure tzdata
[sudo] password for cs2017026:
```

- In this command,

  sudo – super user(root)
  dpkg-reconfigure – This one is used to reconfigure an already installed package.
  tzdata – time zone data.



- After entering the above command, you can see this like interface and choose the Geographic area from this and ok. Then the below figure will come as interface.



- Then select the time zone from this list. So, these are the basic configurations required to do this task.

2.LAMP Configuration

- In this LAMP configuration, first, we have to update and install the Linux environment, Apache server, MySQL database and PHP before the LAMP configuration. First, I updated the linux environment using the below command.

```
cs2017026@cs2017026:~$ sudo apt update
[sudo] password for cs2017026:
Hit:1 http://lk.archive.ubuntu.com/ubuntu focal InRelease
Hit:2 http://lk.archive.ubuntu.com/ubuntu focal-updates InRelease
Get:3 http://lk.archive.ubuntu.com/ubuntu focal-backports InRelease [101 kB]
Hit:4 http://lk.archive.ubuntu.com/ubuntu focal-security InRelease
Fetched 101 kB in 2s (51.3 kB/s)
Reading package lists... Done
Building dependency tree
Reading state information... Done
4 packages can be upgraded. Run 'apt list --upgradable' to see them.
cs2017026@cs2017026:~$ sudo apt upgrade
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
The following packages will be upgraded:
  alsa-ucm-conf open-vm-tools python-apt-common python3-apt
```

- ❖ In these above commands,
  sudo – Super user(root)
  apt - Advanced Package Tool
  These commands are used to update the ubutu environment as a super user.

- ❖ So, update updates the list of available packages and their current versions, but update does not install or upgrade any new packages. upgrade installs newer versions of the packages you have.
- ❖ Then we need to update and install the apache server. This Apache webserver is an open-source web server software which is used to serve the content on the web. So, to do this installation, I used the following command.

```
Processing triggers for systemd (245.4-4ubuntu3.11) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for libc-bin (2.31-0ubuntu9.2) ...
cs2017026@cs2017026:~$ sudo apt install apache2
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  apache2-bin apache2-data apache2-utils libaprl libaprutill
  libaprutill-dbd-sqlite3 libaprutill-ldap libjansson4 liblua5.2-0 ssl-cert
Suggested packages:
```

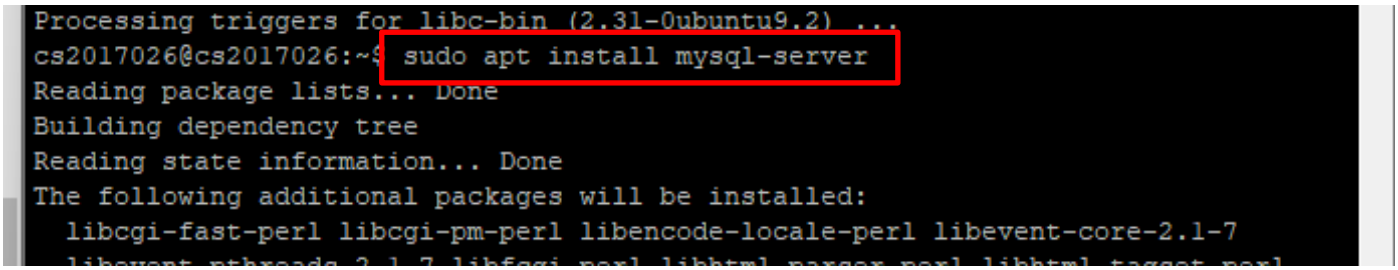
- In this command,

  sudo – Super user (root)

  apt - Advanced Package Tool

  So, we use this command to install the apache web server on ubuntu machine as super user.

- So, After the apache installation, we have to install the my sql server on the ubuntu server. MYSQL is a open-source database management system which needs to store, organize and manage the data on ubuntu server. I used following command to install the MYSQL database on ubuntu.



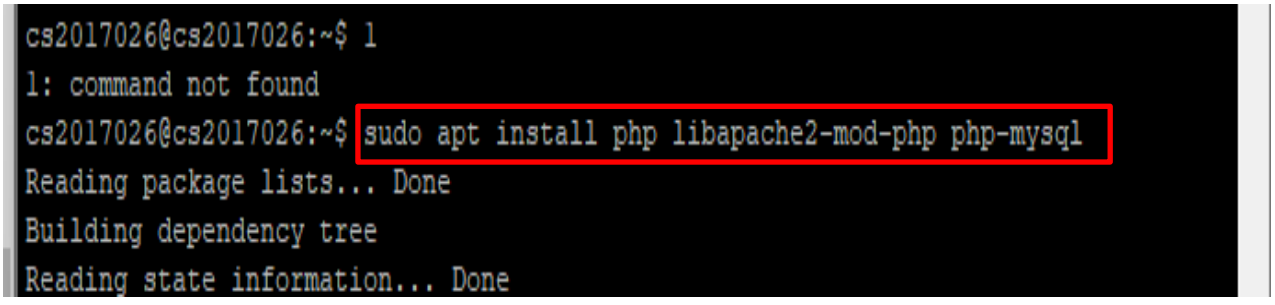
- In this command,

  sudo – Super user(root)

  apt - Advanced Package Tool

  This command is used to install the mysql database as a super user on the ubuntu machine.

- Then, we have to install the php installations. PHP is an open source scripting language which is mostly used to make dynamic websites. The following code is used to install the PHP on the ubuntu server.



- In this command,

  sudo – Super user(root)

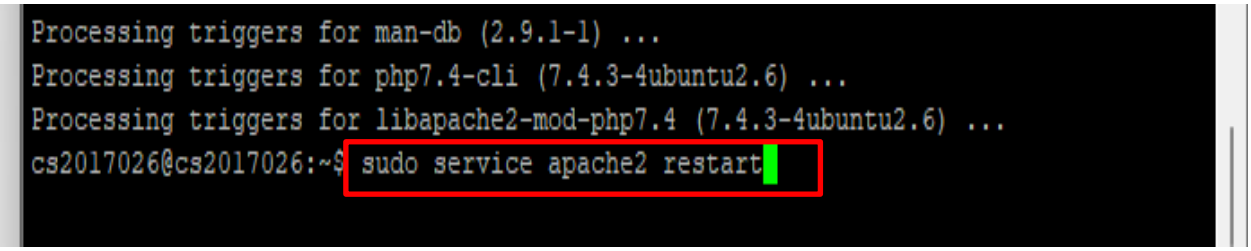
  apt – Advanced package tool

libapatch2-mod-php – This package provides the PHP for the Apache 2 webserver.

php-mysql –

This command is used to install php plugins in ubuntu server as a super user.

- ❖ After these installations, we should restart the apache web server to effect the changes that we did before. So, to do that, we should use the following command.



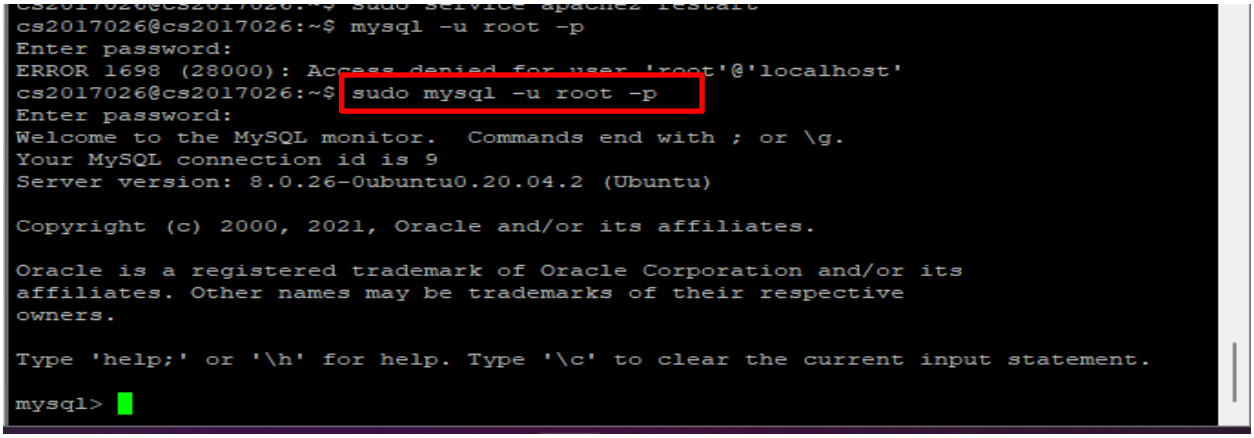
- ❖ In this command,

  sudo – Super user(root)

  we use this command to restart the apache services to make changes that we did before.

- ❖ After that, we have to do some LAMP configurations to install the WordPress.

- At first, we must set up a new MySQL database and user for WordPress.
  - ❖ Initially, we must log in to the MySQL database to fulfill this task. I used the following code to do this task.



- ❖ In this command,

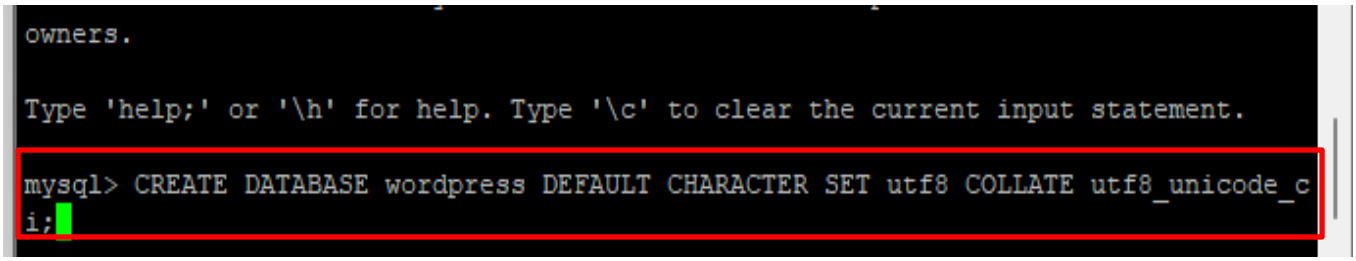
  sudo – Super user(root)

  -u – username

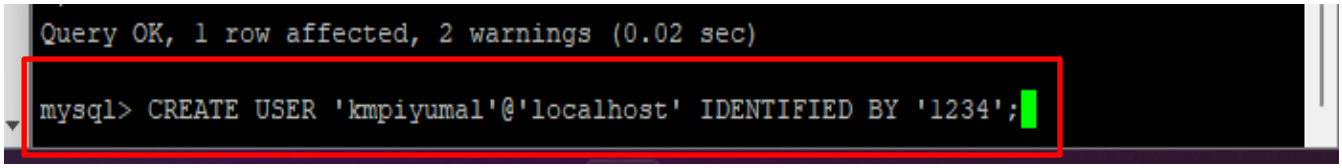
  -p – password

  So, we use this command to log into the MySQL database as a super user. After this command it asks about a password. As a super user we don't need to give password. Once hit on enter button, we can log into the MySQL database.

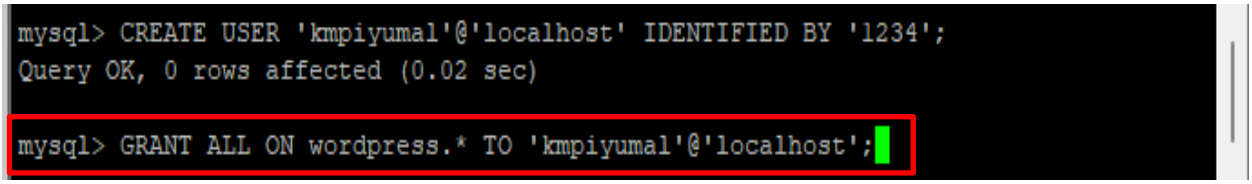
- Then we need to create a database to control the WordPress. You can use any name for this database name, but in this this case, I used it as ‘wordpress’. So, we must use the following code to create the database.



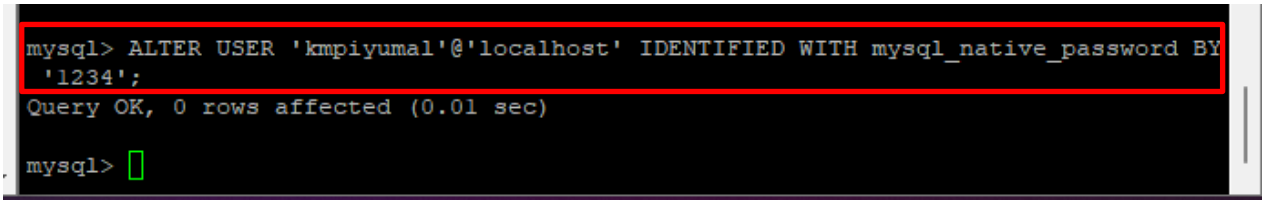
- In this command,
  utf8 – This is a variable with character encoding which is used for electronic communication and defined with Unicode standard.
  utf8_unicode_ci – This is a legacy collation which does not support contractions, expansions, or ignorable characters.
- After this one you will create a database which named as ‘wordpress’ and then we should create a user for this database.
- This following figure is shown this creating user step.



- In this command, I used ‘kmpiyumal’ as user name and took the password for the user as ‘1234’.
- Then, We must grant all privileges on the WordPress database to this user. To this, we must enter the following code.

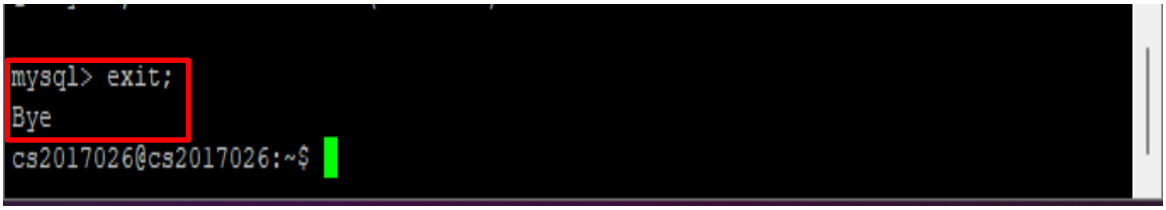


- So, once user granted the permissions then we must adjust login method to mysql_native_password. mysql_native_password is the traditional method to authentication process.
- The following figure shows this command.

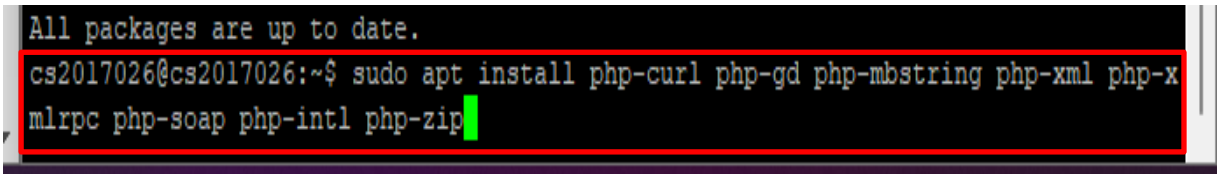


- Then the command 'FLUSH PRIVILAGES' is used to effect these changes very quickly. The following figure is shown this command.

- Then enter the exit command to exit in MySQL prompt. Now, we setting up the MySQL Database and User for WordPress successfully.



- Now, we must configure PHP to work with WordPress plugins. In this task, we must install some Php extensions first. The following command is shown this command.



- In this command.

  sudo – Super user(root)

  apt – Advances Package Tool

  php-curl – This is php library and most powerful extension of PHP

  php-gd – This is an open-source code library for the dynamic image crearions.

  php-mbstring – This is an extension of php which is used to manage the non-ASCII strings

  php-xml – php-xml is used to store, structure and transport data from one system to another system.

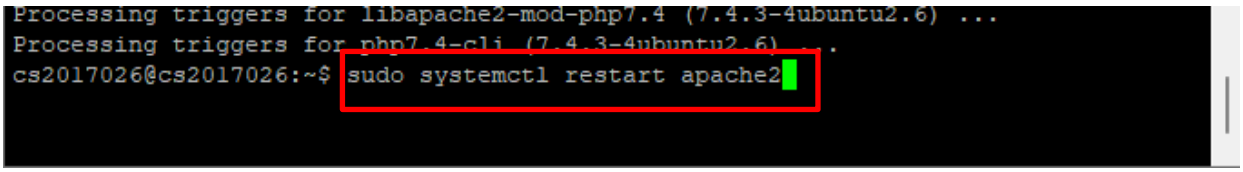
  php-xmlrpc – This is an extension of php used for server and client features in php.

  php-soap – This extension is used to provide and consume web services.

  php-intl – php-intl enables php programmers to to perform the USA-confoment collation and date/time/number/currency formatting in their scripts.

  php-zip – This one is an archive file format which supports lossless data pressure.

- Then restart the apache server to work these extensions. The following figure is shown this one.

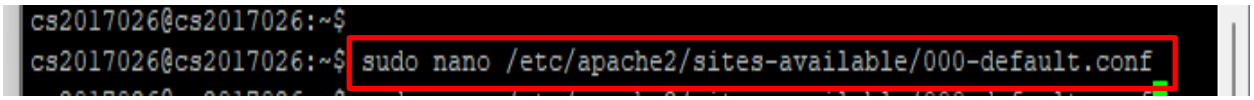


- In this command,

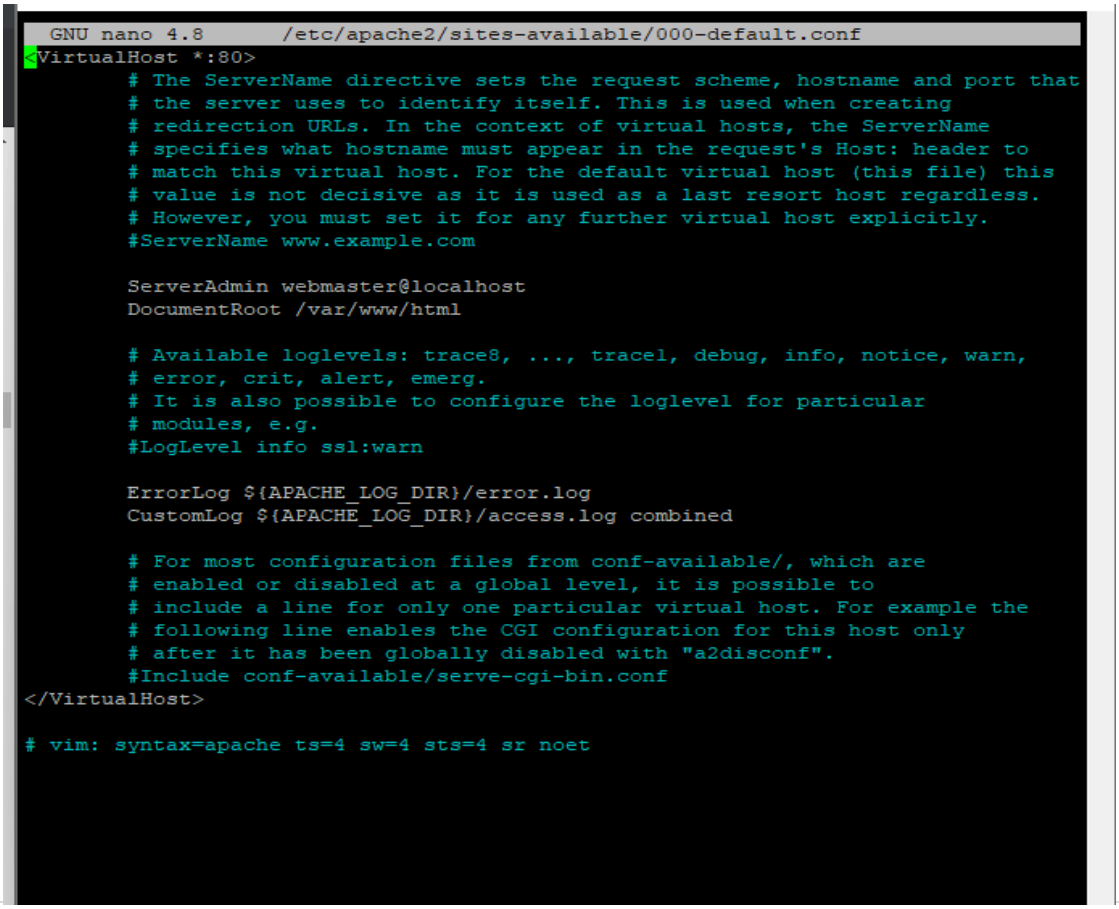
  sudo – Super user(root)

  systemctl – This is a utility that is responsible for examining and controlling the systemd system and service manager.

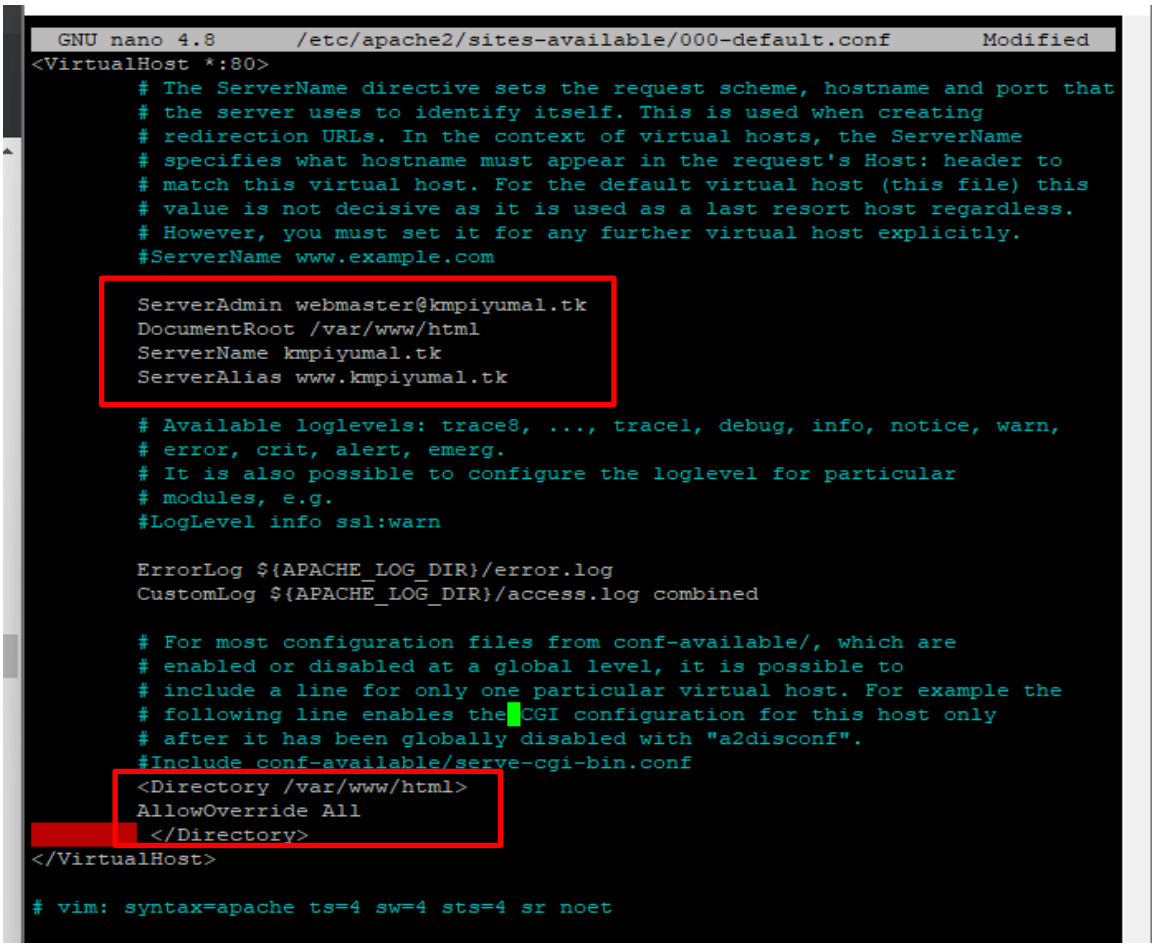
- Now the php configuring is over. So, we must consider about configuring the Apache's .htaccess to handle override and rewrite rules.
- .htaccess files are in root directory of a website. They contain rules which apache uses to direct requests in a manner. So, WordPress uses its .htaccess to manipulate how Apache serves files from its root directory and subsequent subdirectories. In this segment we use a virtual host to host our web site. The config files of this virtual hosts are stored in /etc/apache2/sites-available/ directory. The '000-default.conf' comes with the Apache's installation. This directory can only host one site. In default, the .htaccess directory override is disabled. For WordPress activities we must enable this directory overrides. We use virtual host files to do this. The following figure shows the command of this.



- In this command,
  sudo – Super user(root)
  nano – command line text editor
  After entering this path you may see below like figure.



- We must include following figure things to create virtual host.



- This must include the localhost as domain name of the website and server name and server alias and also AllowOverride directive is added within the directory block pointing to the webserver's document root. Include the directory block and update the document root.
- After including those things and give CTRL + O to save these things and CTRL + X to exit the editor.
- After that we think about enable the rewrite module. So, WordPress comes with a permalink feature that ensures great search engine optimized URLs. They depend on an Apache module called mod_rewrite. We can enable the rewrite module using the following command.

```
cs2017026@cs2017026:~$ sudo a2enmod rewrite
[sudo] password for cs2017026:
Enabling module rewrite.
To activate the new configuration, you need to run:
  systemctl restart apache2
cs2017026@cs2017026:~$
```

- In this command,
  - sudo – Super user (root)
  - a2enmod – This is a script which enables the specified module within the apache2 configuration.
- After entering this command, you can enable the rewrite module.
- Then, we need to test these changes work in properly. So, we need to enter the following command to check it.

```
cs2017026@cs2017026:~$ sudo apache2ctl configtest
AH00558: apache2: Could not reliably determine the server's fully qualified domain
 name, using 127.0.1.1. Set the 'ServerName' directive globally to suppress this m
essage
Syntax OK
cs2017026@cs2017026:~$
```

- In this command,
  - sudo – Super user(root)
  - apache2ctl – This is a front end to the Apache Hyper Text Transfer Protocol server which is designed to help to the administrator to control the functionality of the Apache httpd daemon.
  - configtest – This checks the configuration files.
- This command outputs the following figure.

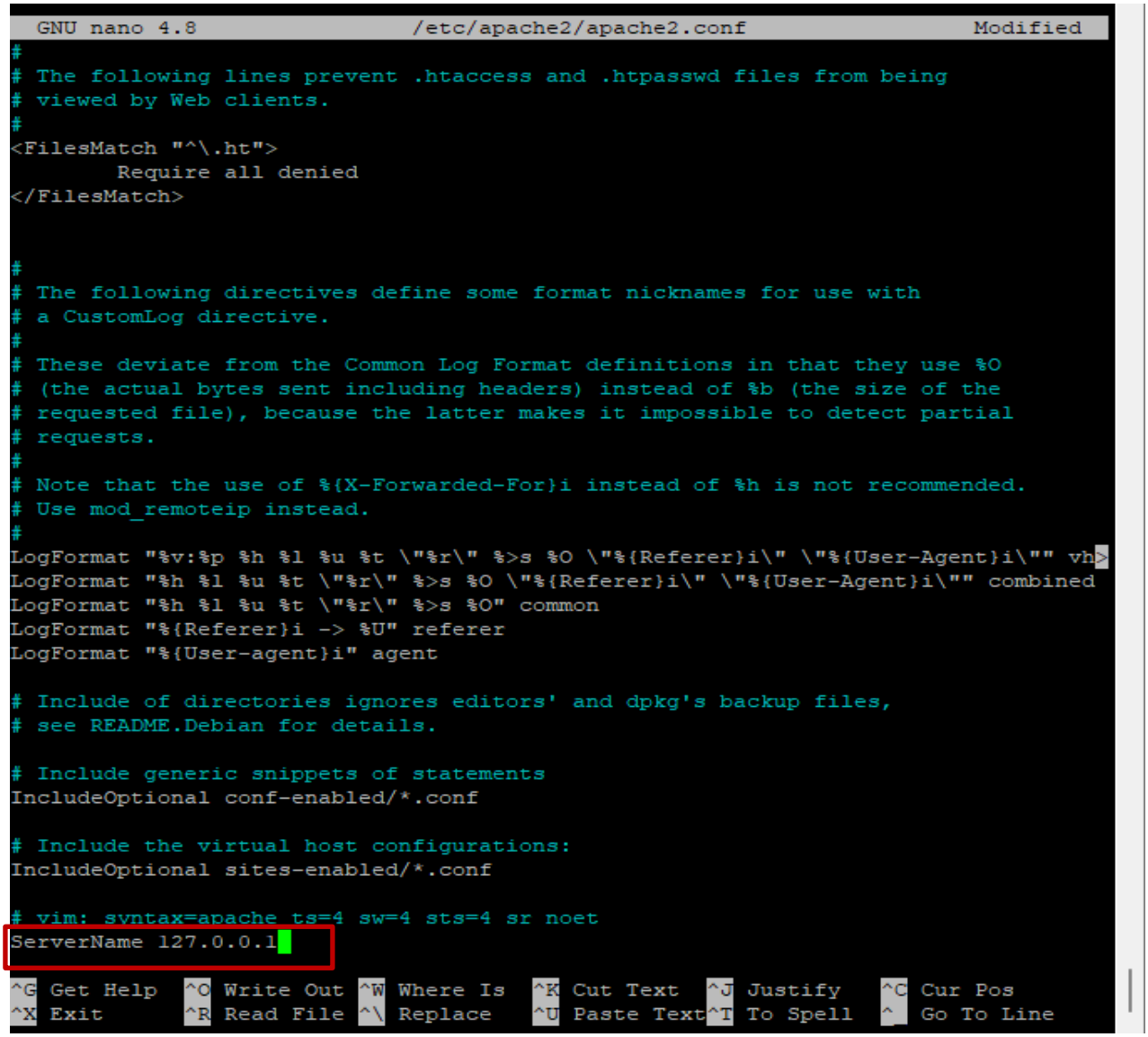
```
AH00558: apache2: Could not reliably determine the server's fully qualified domain
 name, using 127.0.1.1. Set the 'ServerName' directive globally to suppress this m
essage
Syntax OK
```

- This displays an error message. We can fix this error using following command.

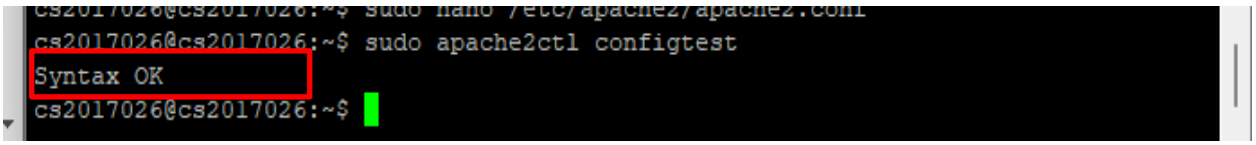
```
Syntax OK
cs2017026@cs2017026:~$ sudo nano /etc/apache2/apache2.conf
cs2017026@cs2017026:~$
```

- So, In this command,
  - sudo – Super user(root)
  - nano – command line text editor

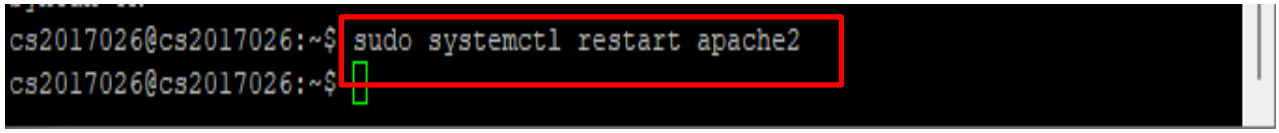
- To fix this issue, we must go to this path and add server name as following figure.



- Then the output be like the following figure.



- Then to enable new changes, enter the following command.

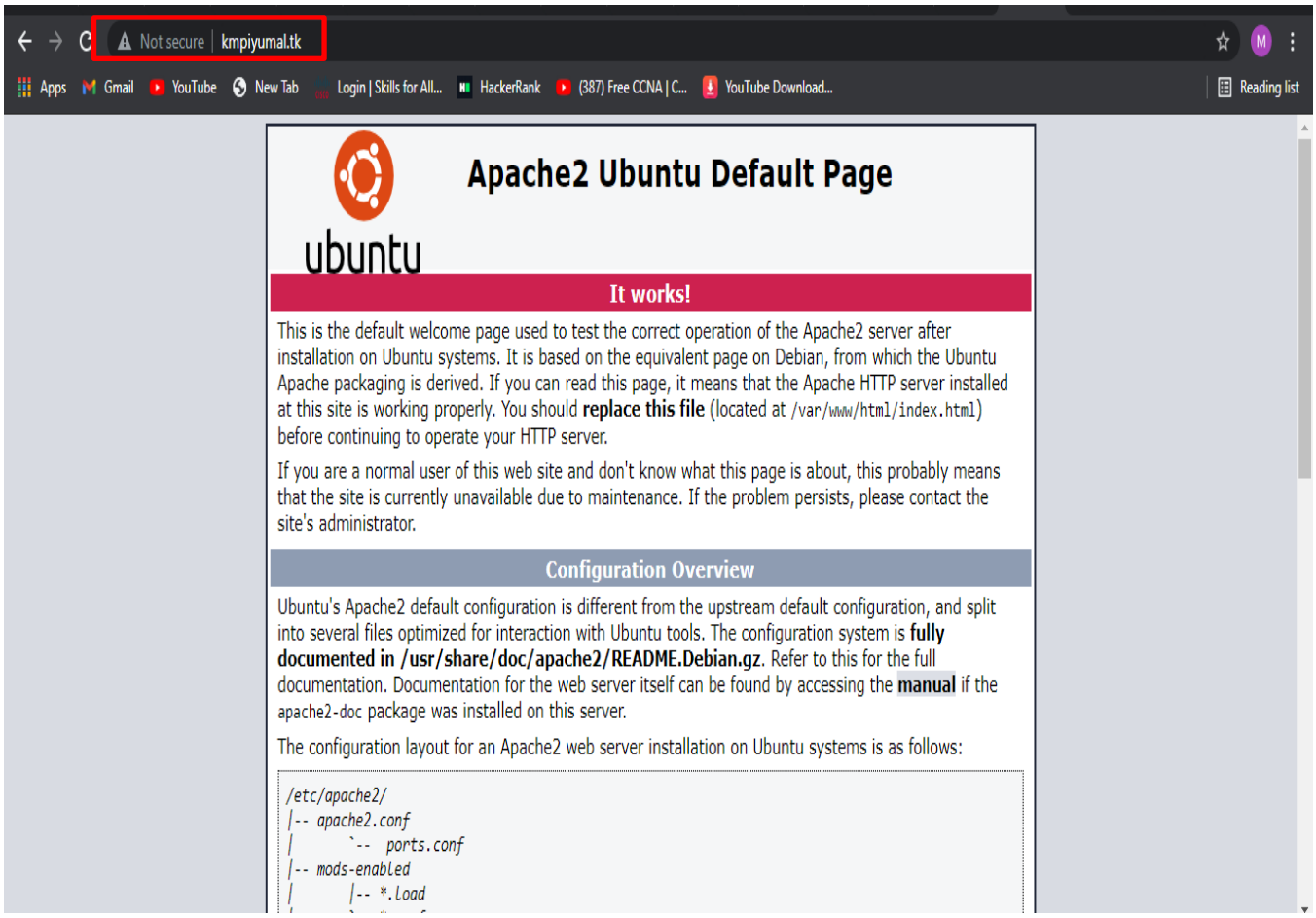


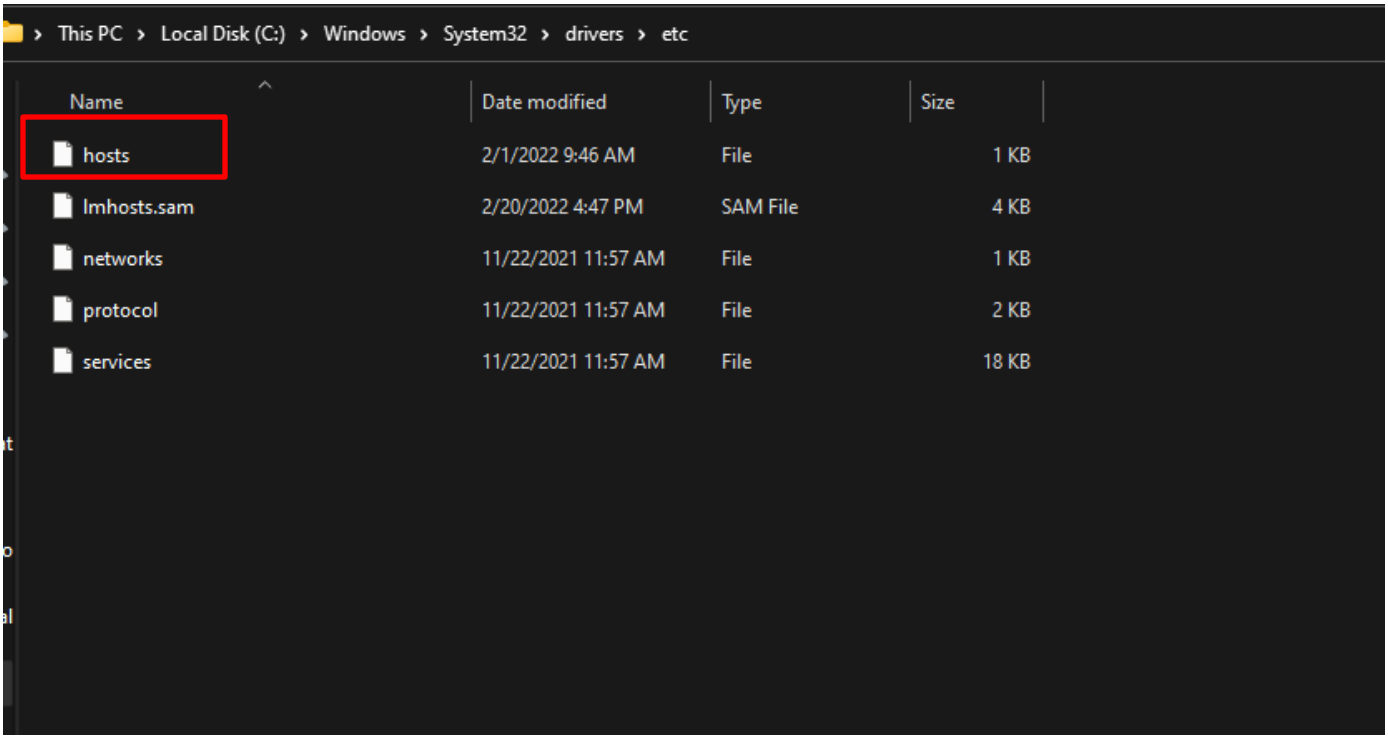
- In this command,

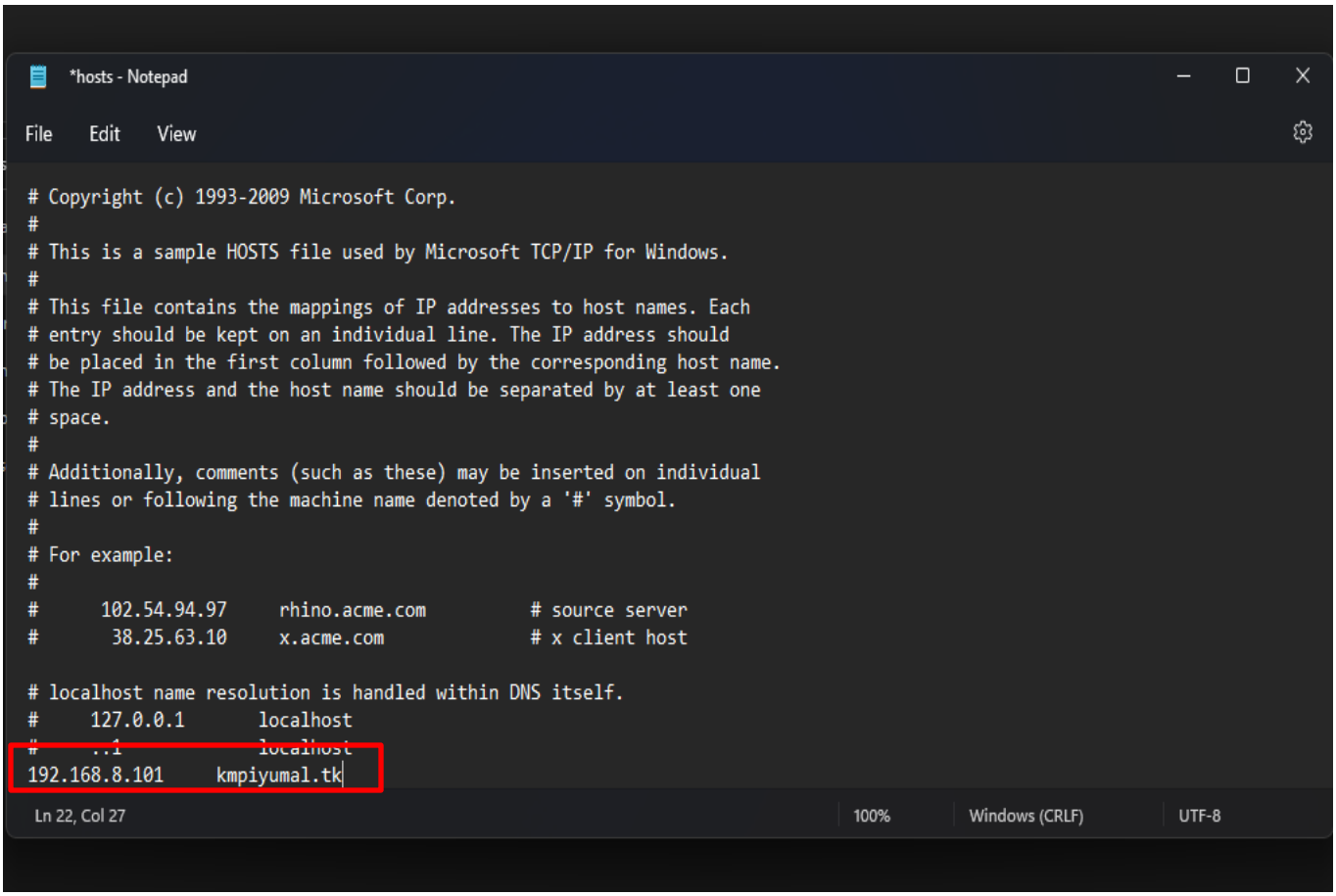
  sudo – Super user(root)

  systemctl – This is a utility that is responsible for examining and controlling the systemd system and service manager.

- After doing these things, you can check the server hosts your web server like following figure. To do this I entered my URL as ‘http://kmpiyumal.tk’



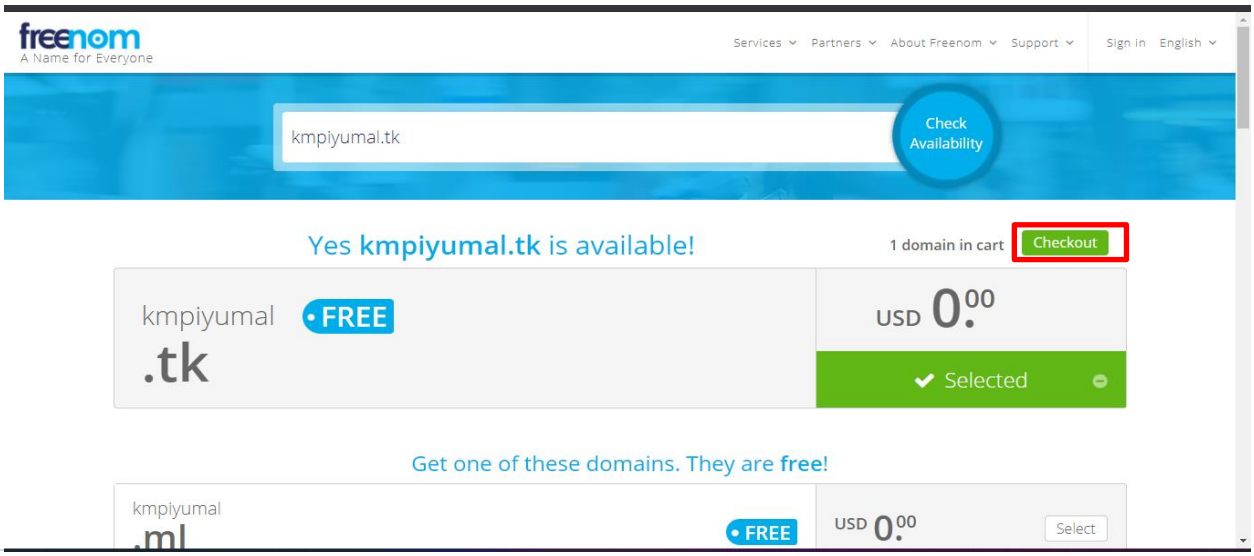

This PC › Local Disk (C:) › Windows › System32 › drivers › etc
Name
Date modified
Type
Size
hosts
2/1/2022 9:46 AM
File
1 KB
lmhosts.sam
2/20/2022 4:47 PM
SAM File
4 KB
networks
11/22/2021 11:57 AM
File
1 KB
protocol
11/22/2021 11:57 AM
File
2 KB
services
11/22/2021 11:57 AM
File
18 KB


*hosts - Notepad
File
Edit
View
Copyright (c) 1993-2009 Microsoft Corp.
#
This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
This file contains the mappings of IP addresses to host names. Each
entry should be kept on an individual line. The IP address should
be placed in the first column followed by the corresponding host name.
The IP address and the host name should be separated by at least one
space.
#
Additionally, comments (such as these) may be inserted on individual
lines or following the machine name denoted by a '#' symbol.
#
For example:
#
102.54.94.97   rhino.acme.com   # source server
38.25.63.10   x.acme.com   # x client host
localhost name resolution is handled within DNS itself.
127.0.0.1   localhost
::1   localhost
192.168.8.101   kmpiyumal.tk
Ln 22, Col 27
100%
Windows (CRLF)
UTF-8

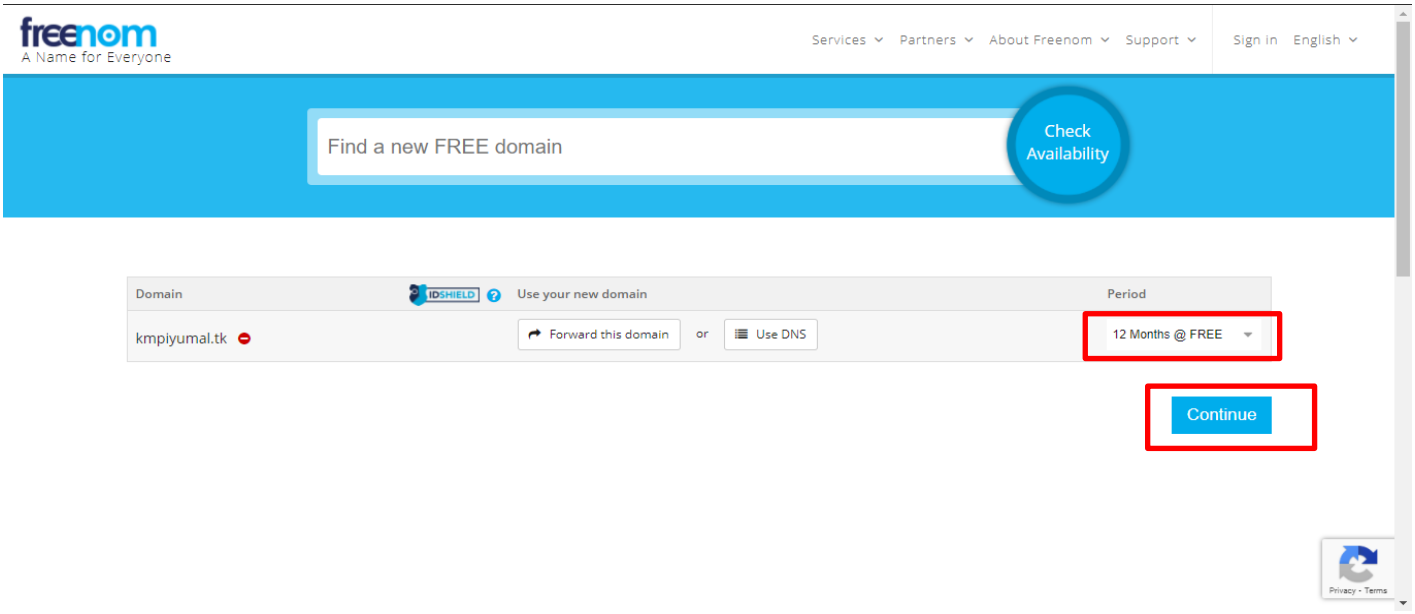
4. Getting a domain name

- In this section we are talking about getting the domain name. To get the domain name I used ‘freenom’ website. The process is showing the below.
- At first, we must visit to the ‘freenom’ web site using your favourite browser. Then you can see the below like figure.

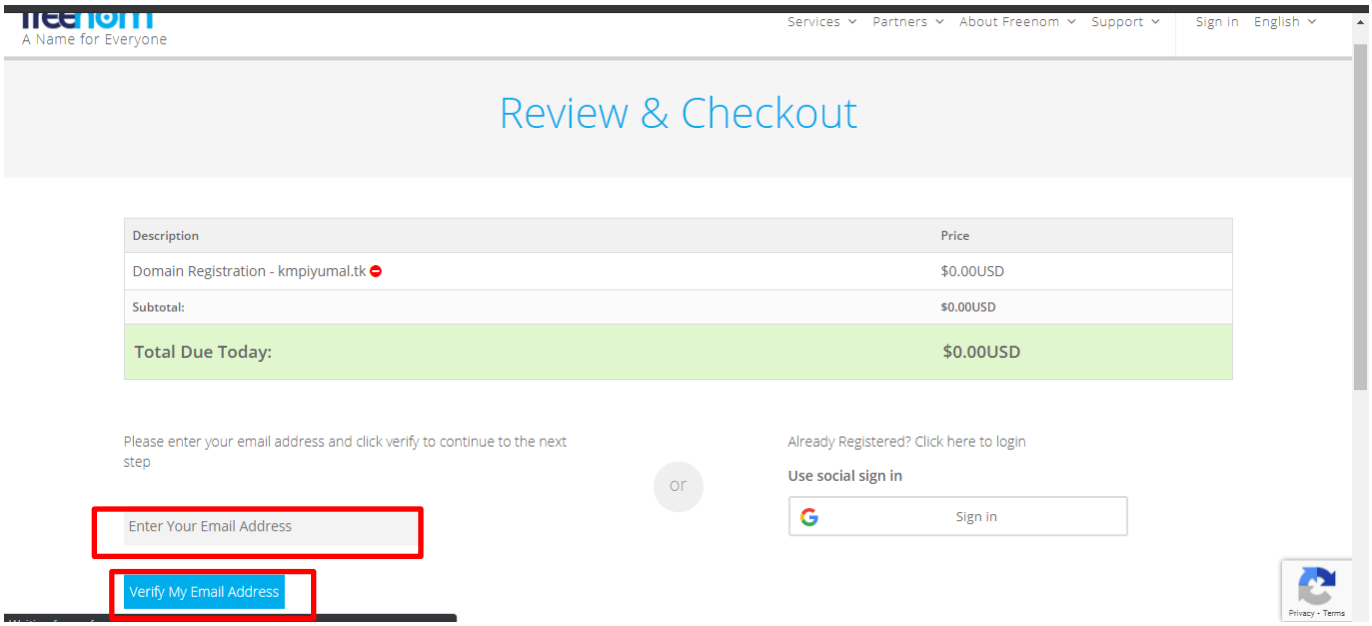
- After the visit you should enter the domain name as you like and then click on ‘Check Availability’. Then the following figure will display on your browser.



❖ Then click on checkout button in above figure and then you will display below like figure.



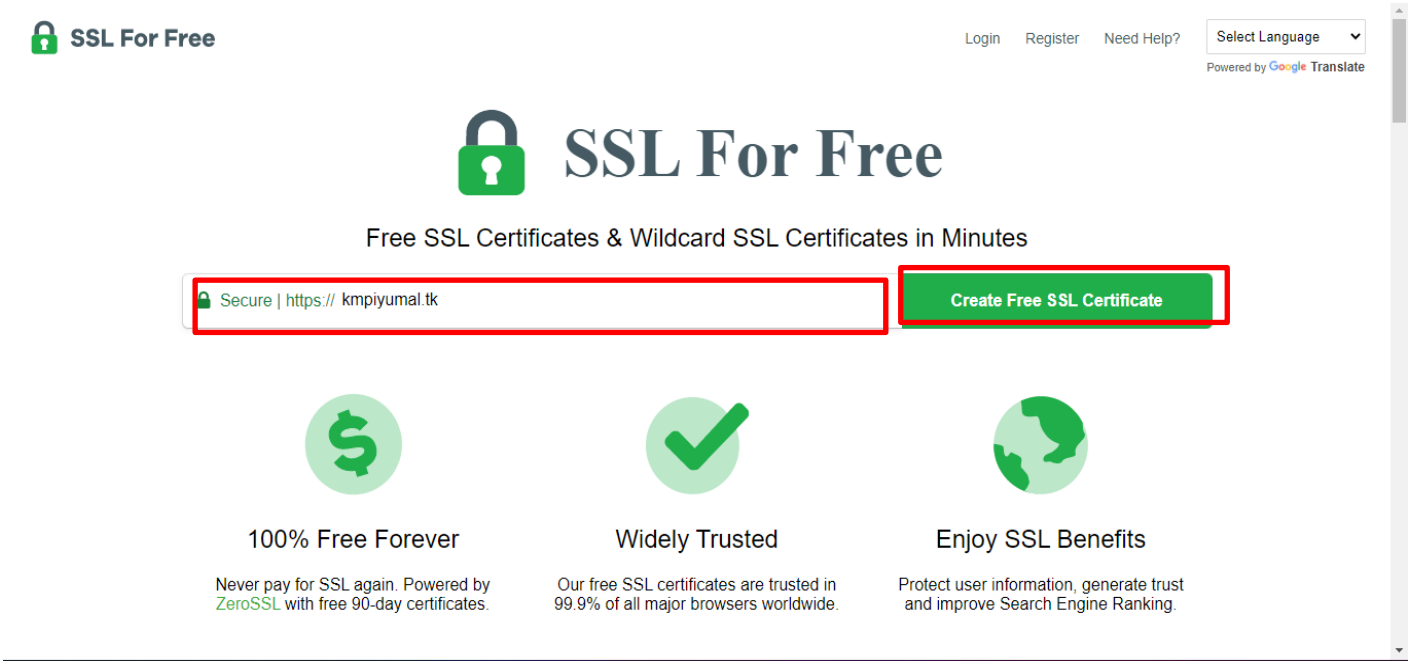
❖ Then select 12 months in above figure and click on continue. You will display below like figure.



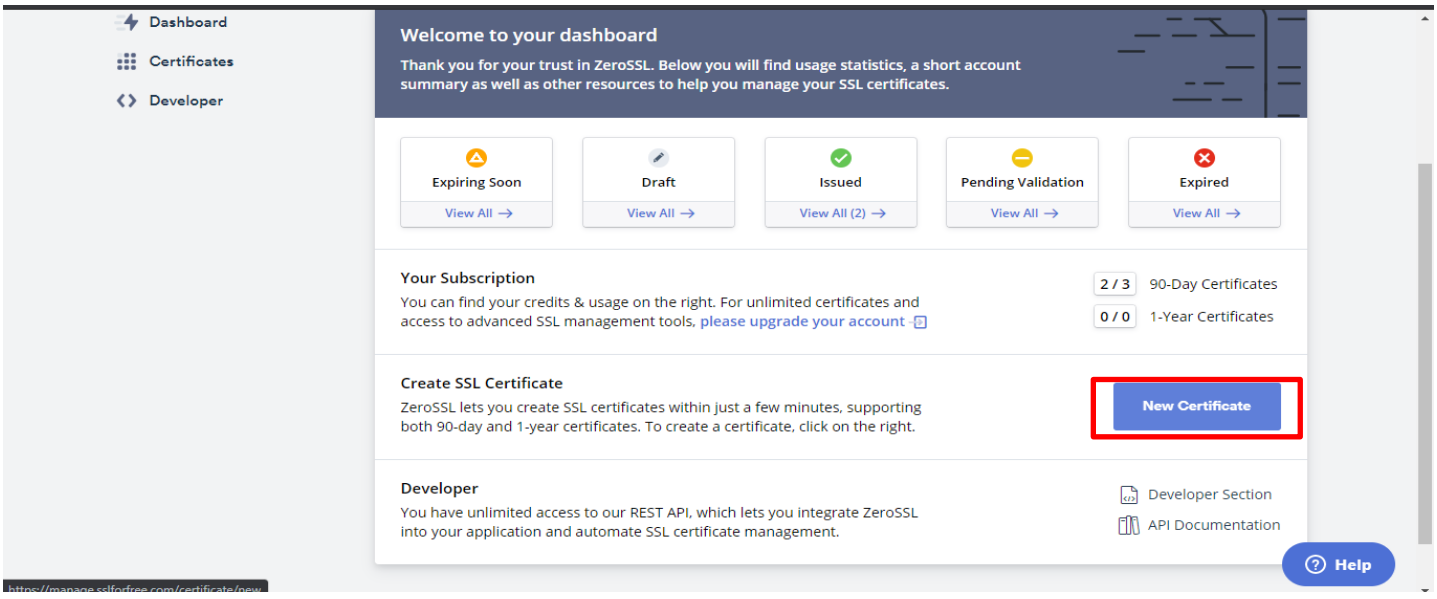
❖ Then enter your official e mail address and then click on ‘verify my email address’ in the above figure. Then verify the domain name using your e mail.

5.Getting a SSL certificate and configuration

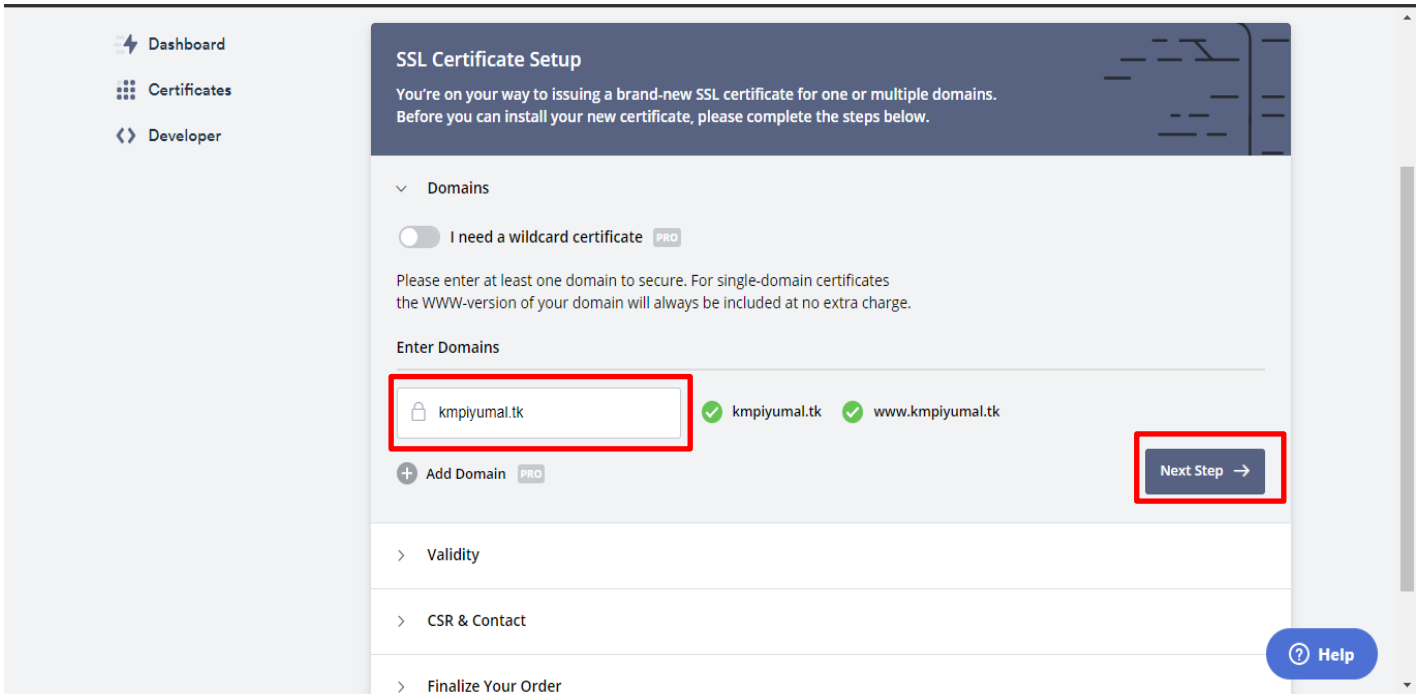
- In this section we are talking about how to verify and create a certificate to your domain name. To fulfill this, we use ‘SSL For Free’ web site. The ‘SSL For Free’ web site is in the below figure.



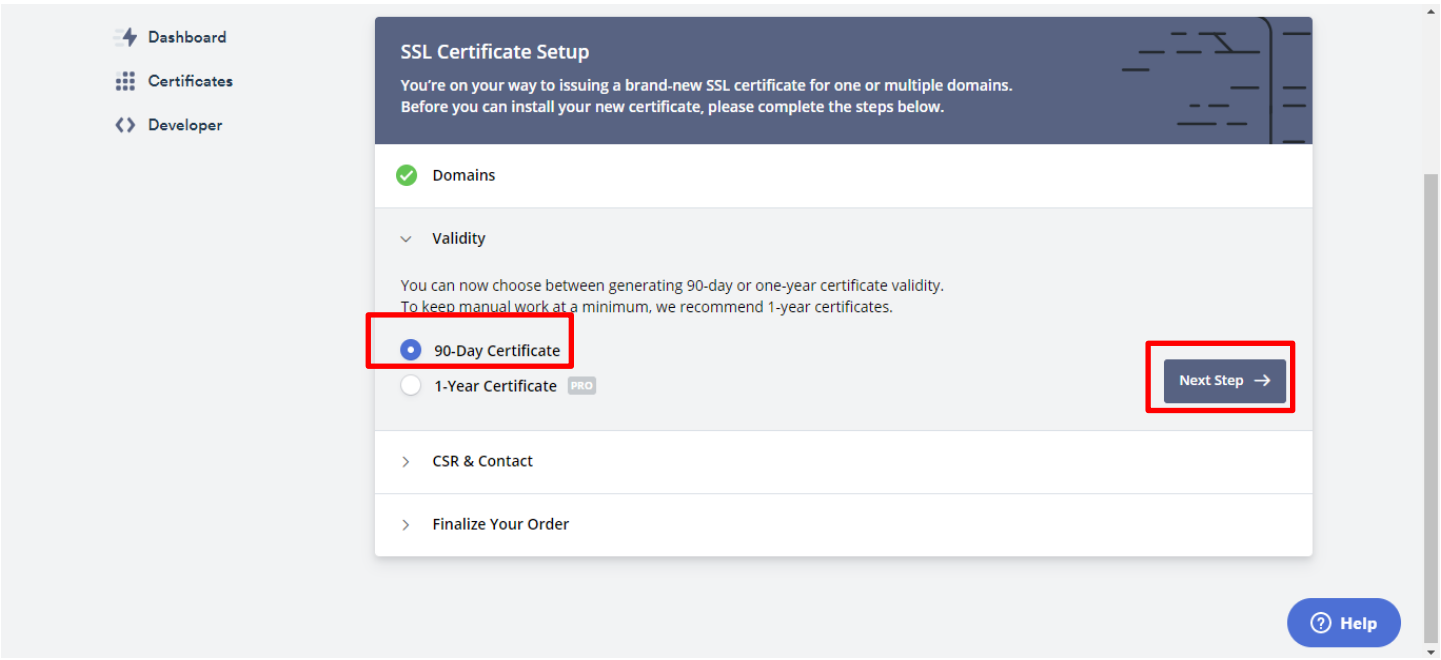
- After entering the website, you must include your domain name and then hit on ‘Create free SSL Certificate button. After that you will see below like figure.



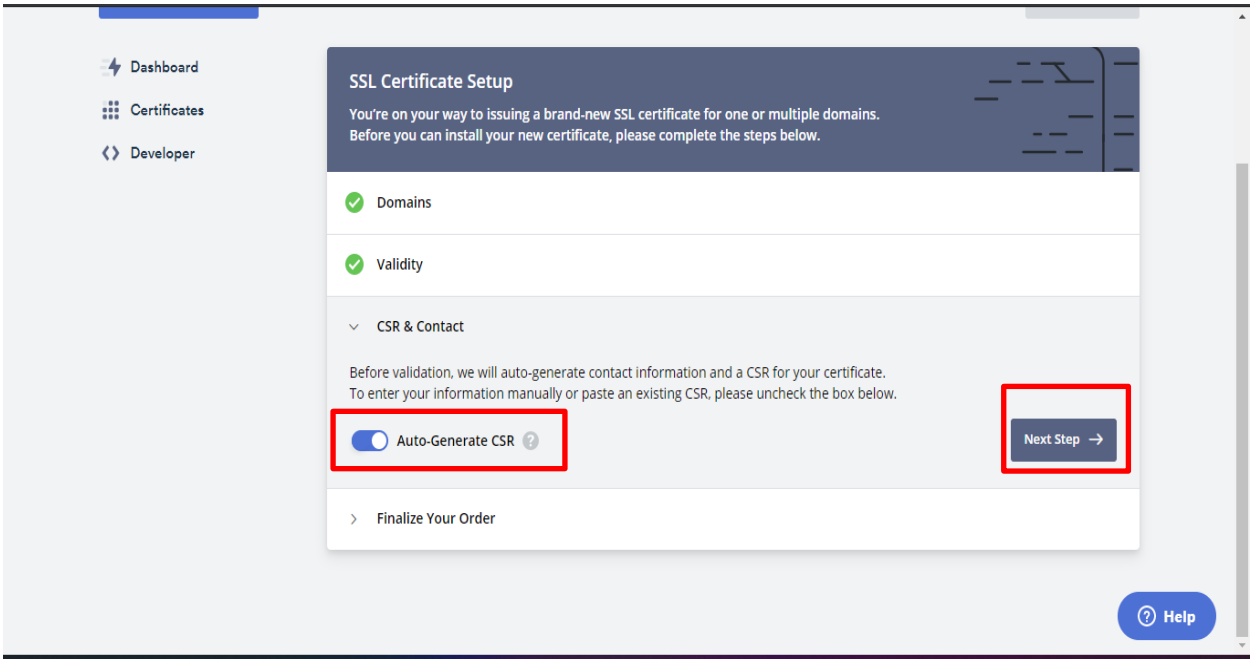
❖ Then click on ‘New Certificate’ Button. You can see below like figure.



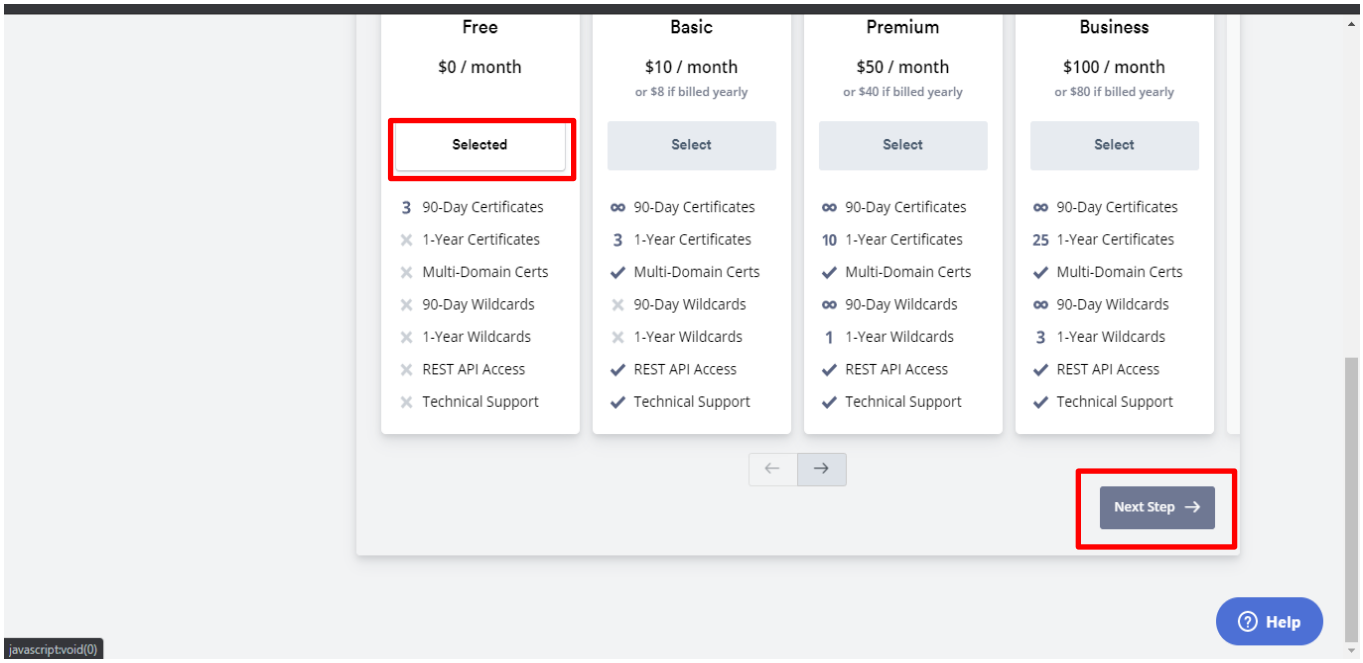
❖ Then enter your domain name in left side blank and then click on ‘Next Step’ button. After that you can see below like figure.



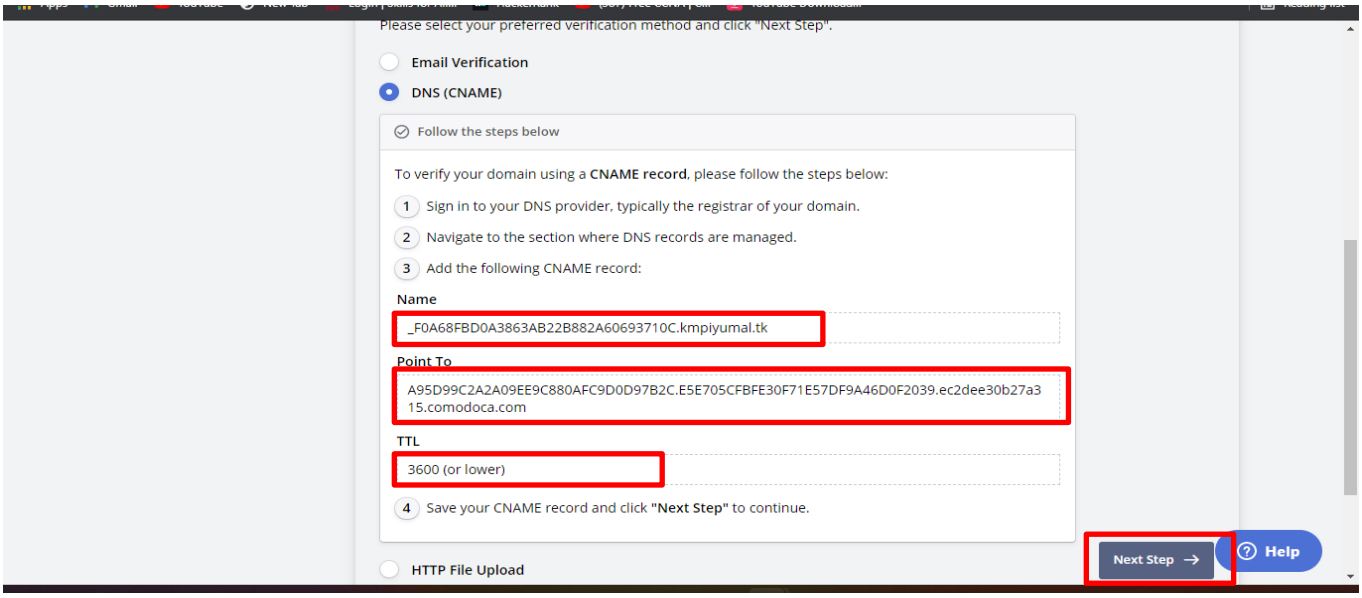
❖ As a normal user you can use 90-day certificate but if you are a pro user you can buy a 1-year certificate. After that click on ‘Next Step’. After that you will see below like figure.



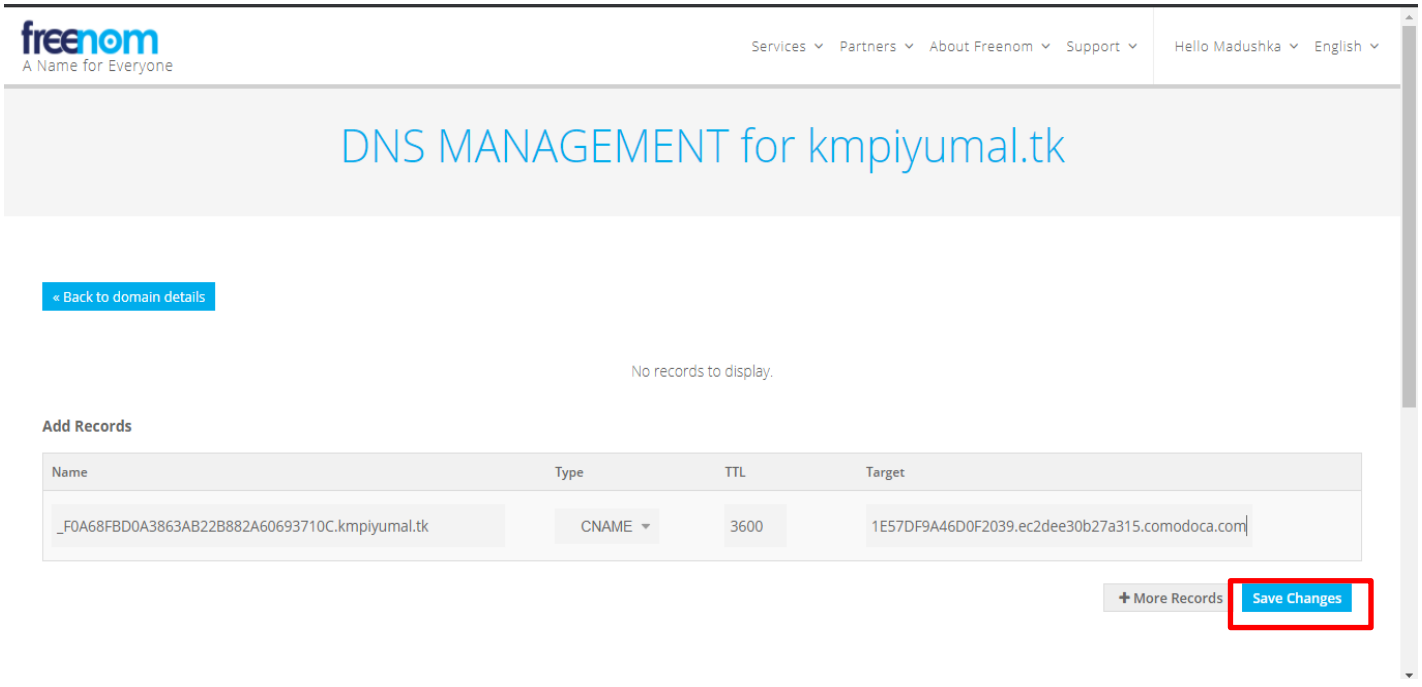
❖ Then activate the ‘Auto-Generate CSR’ and then click on ‘Next Step’. You can see below like figure.



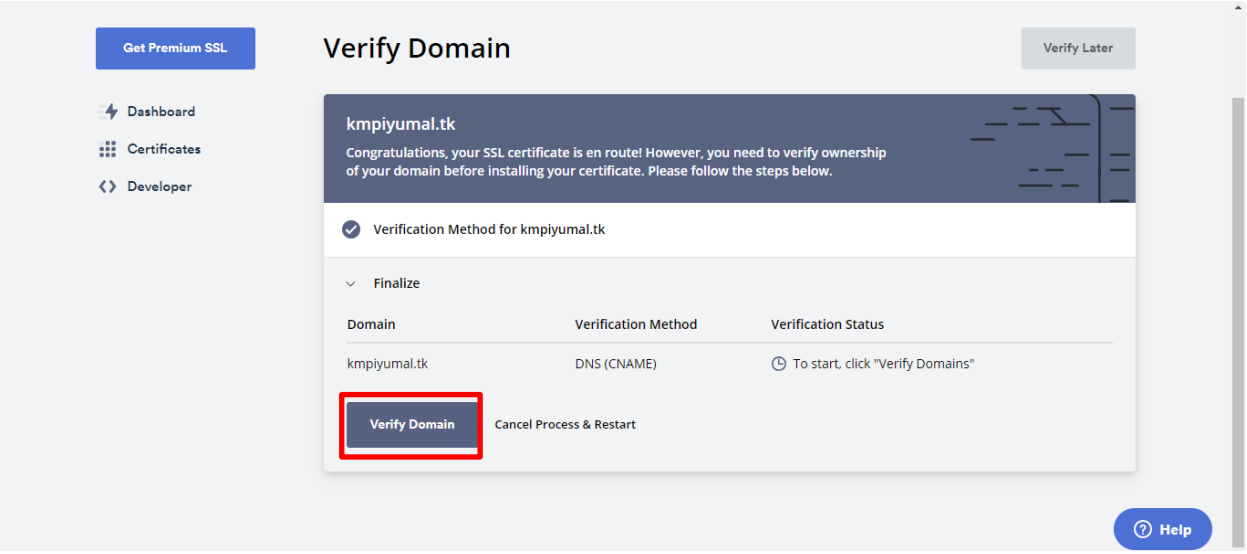
❖ In the above figure, you can select your certification plan and click on ‘Next Step’. After that you can see below like figure.



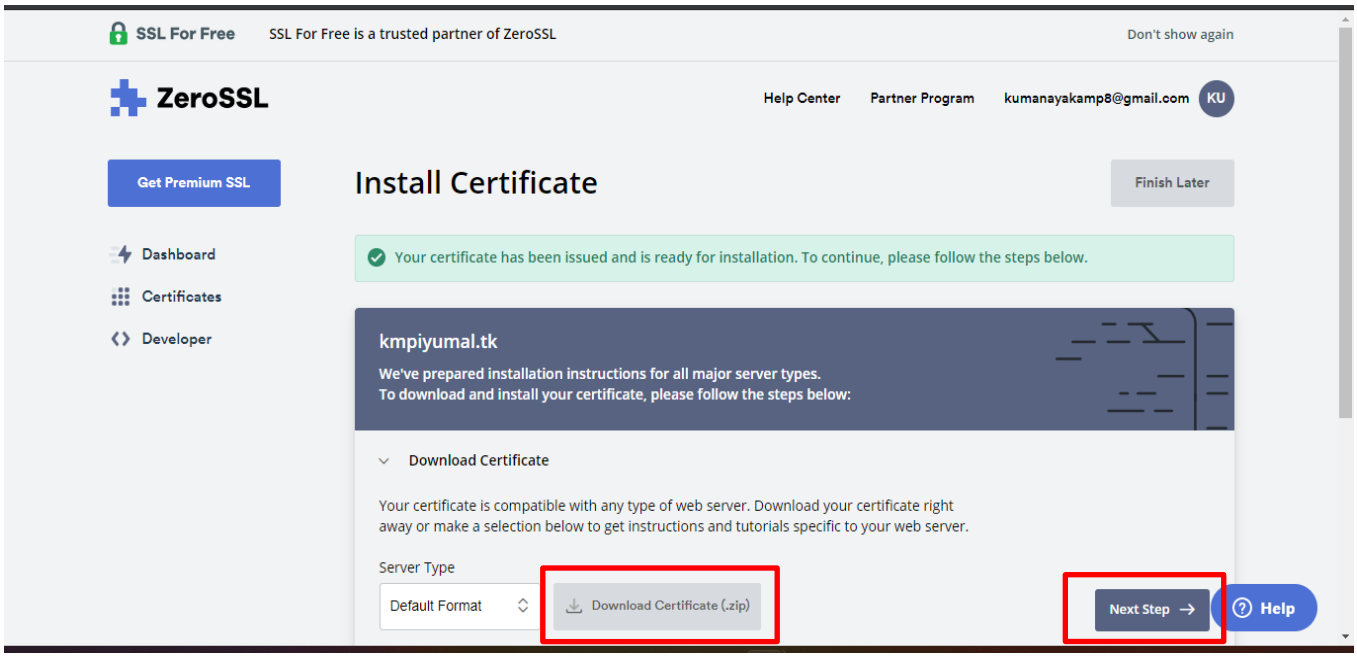
❖ In the above figure shows that verification method from your domain name server. In ‘freenom’ only provides DNS method. So, we must copy these fields and paste in ‘freenom’ account ‘DNS records’ section to verify your domain name and get the SSL certificate. The below figure is shown that.



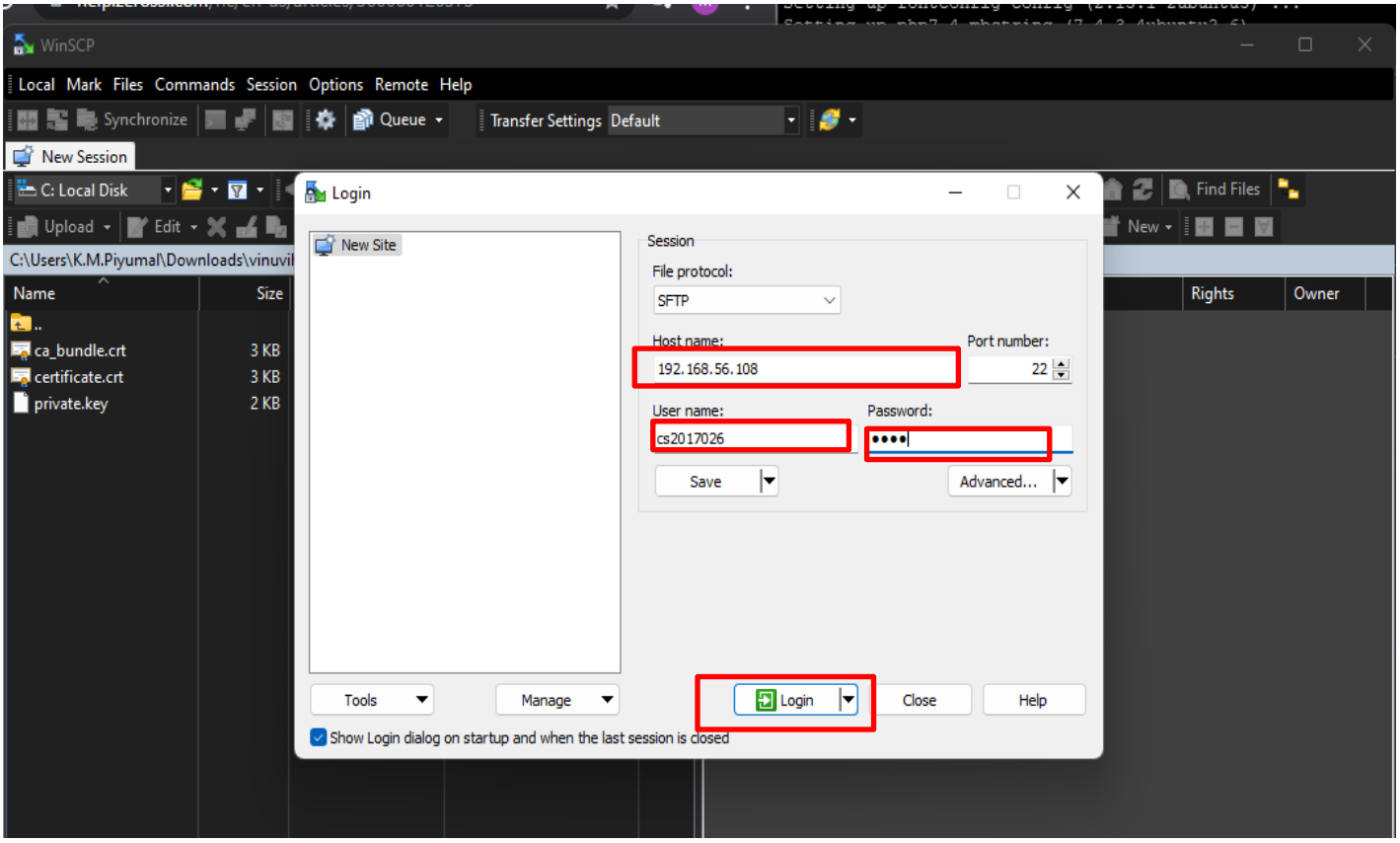
❖ After that click on save changes and then go to the ‘SSL For Free’ site to verify the domain.



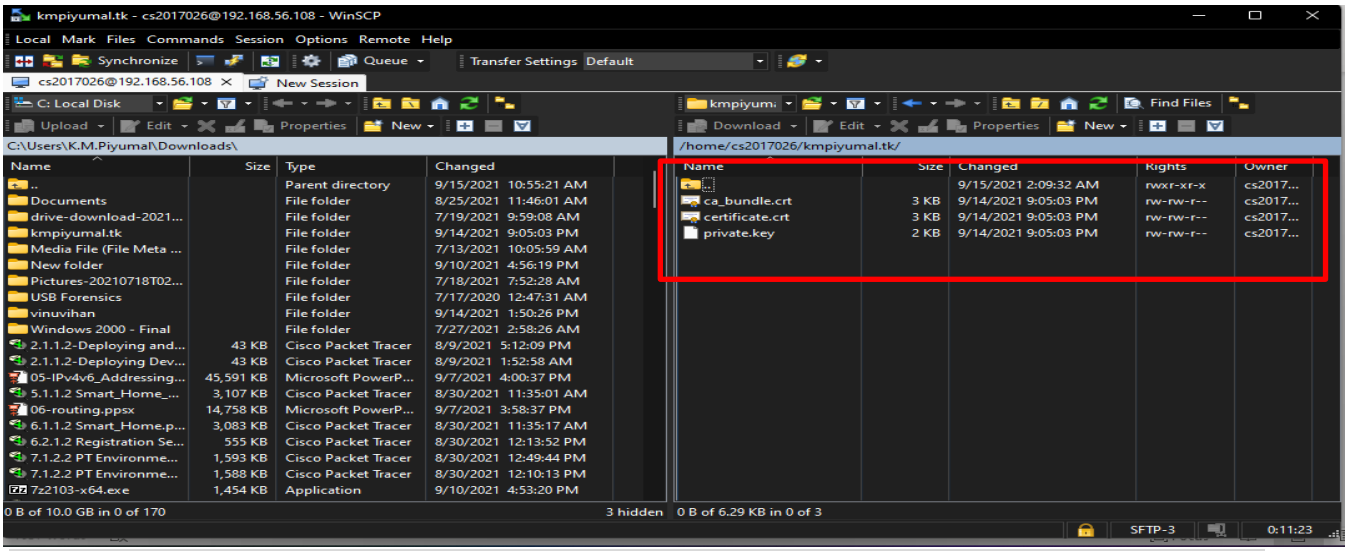
❖ Then click on ‘Verify Domain’ to verity the domain. So, it will take 5-10 minutes. After that you will see below like figure.



❖ Then click on ‘Download Certificate’ button to download your certificate. After that you should send this certificate to ubuntu server using ‘WinSCP’ application. Then belowfigure is shown that.



❖ Then enter your host’s ip address as host name and username and password of your host machine and after that click on the ‘Login’ button. After that you will see below like figure.



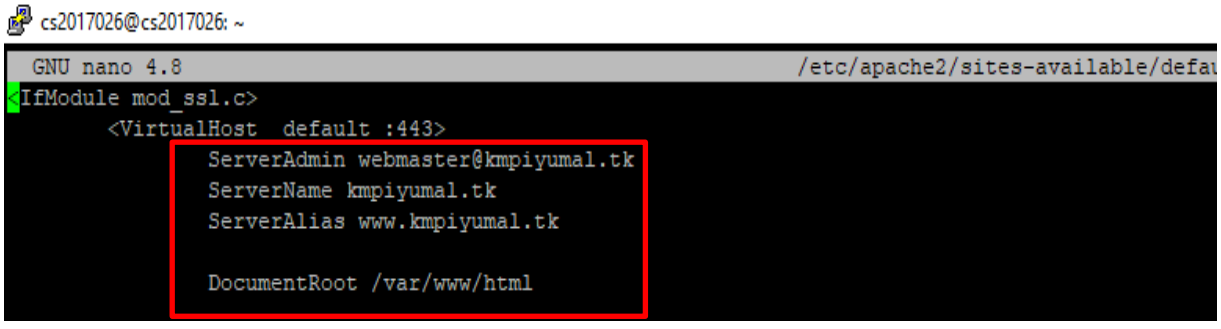
- So, you must drag and drop you certificate file like above to insert your certificate to your server. After that you should change the directory of these files to ubuntu certs and private key directories. Because these are the directories ubuntu server normally stores its certificates. The following figure is shown it.

```
cs2017026@cs2017026:~$ sudo cp /home/cs2017026/kmpiyumal.tk/certificate.crt /etc/s
sl/certs/cerficate.crt
cs2017026@cs2017026:~$ sudo cp /home/cs2017026/kmpiyumal.tk/ca_bundle.crt /etc/ssl
/certs/ca_bundle.crt
cs2017026@cs2017026:~$ sudo cp /home/cs2017026/kmpiyumal.tk/private.key /etc/ssl/p
rivate/private.key
```

- In these commands,
  - sudo – Super user(root)
  - cp – copy
- We copy these files using the command prompt because 'WinSCP' cannot have permission to copy these files in these directories.
- Then we need some changes in 'default-ssl.conf' file. We should enter the following command to go to the 'default-ssl.conf' file.

```
cs2017026@cs2017026:~$ sudo nano /etc/apache2/sites-available/default-ssl.conf
```

- Then we must do the following changes in this file. The following figure is shown those changes.



```
#   SSLCertificateFile directive is needed.
SSLCertificateFile      /etc/ssl/certs/certificate.crt
SSLCertificateKeyFile /etc/ssl/private/private.key

#   Server Certificate Chain:
#   Point SSLCertificateChainFile at a file containing the
#   concatenation of PEM encoded CA certificates which form the
#   certificate chain for the server certificate. Alternatively
#   the referenced file can be the same as SSLCertificateFile
#   when the CA certificates are directly appended to the server
#   certificate for convinience.
SSLCertificateChainFile /etc/ssl/certs/ca_bundle.crt

#   Certificate Authority (CA):
```

```
        <Directory /var/www/html>
        AllowOverride All
        </Directory>
    </VirtualHost>
</IfModule>
```

- Then, we should restart the apache server to make these changes. Then we should enable the 'default-ssl.conf' site using the following command.

```
cs2017026@cs2017026:~$ sudo a2ensite default-ssl.conf
Enabling site default-ssl.
To activate the new configuration, you need to run:
  systemctl reload apache2
```

- In this command,
  - sudo – Super user(root)
  - a2ensite – This is a script which enables the specified site.
- Then again you should restart the apache server to make these changes. After that you should make to redirect http to https. To full fill this task you should add commands to 'apache2.conf' file. To visit this directory, you may use the following command.

```
cs2017026@cs2017026:~$ sudo nano /etc/apache2/apache2.conf
```

- Then you should add the following command lines to this file and save and exit using CTRL + O and CTRL + X respectively.

```
#HTTP to HTTPS redirect
RewriteEngine On
RewriteCond %{HTTPS} !=on
RewriteRule ^/?(.*) https://%{SERVER_NAME}/$1 [R,L]

^G Get Help     ^O Write Out    ^W Where Is     ^K Cut Text
^X Exit         ^R Read File    ^\ Replace      ^U Paste Text
```

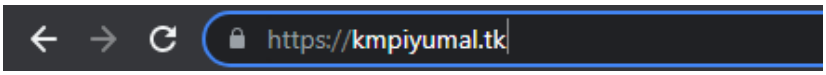
- Then again you should restart the apache server to make these changes and then enable the the ssl certificate using the below command.

```
cs2017026@cs2017026:~$ sudo a2enmod ssl
```

- In this command,
  - sudo – Super user(root)
  - a2enmod – This is a script which enables the specified module within the apache2 configuration.
- Then you will see below like output.

```
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create sel
f-signed certificates.
To activate the new configuration, you need to run:
  systemctl restart apache2
```

- Then again you should restart the apache server to apply these changes in web server. After that go to your browser and give the domain with 'https'. In my case, I gave that as 'https://kmpiyumal.tk'. Then you will see the verified domain as below like figure.



- So, now we have successfully configured the SSL certificate to the ubuntu server. So, our next task is to installation of WordPress in our web server.

6. WordPress installation

- Now we have to install the word press to open in our web server. Our site document root is in /var/www/html directory. We should replace the apache welcome page. At first, we should download the WordPress to our server.
- First, we need to change the directory of our server to tmp using 'cd /tmp' command and you will see below like output.

```
cs2017026@cs2017026:~$ cd /tmp
cs2017026@cs2017026:/tmp$
```

- In this command,

  cd – Change directory.

- After changing the directory, download the WordPress compressed file using below command.

```
cs2017026@cs2017026:/tmp$ curl -O https://wordpress.org/latest.tar.gz
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  7 14.3M    7 1039k    0     0   373k      0  0:00:39  0:00:02  0:00:37  373k
```

- In this command,

  curl – This is a command line tool to transfer data to or from server.

  -O – Output

- Then, enter the following command to extract the compressed file.

```
cs2017026@cs2017026:/tmp$ tar xzvf latest.tar.gz
```

- In this command,

  tar – Used to extract the file.

- These files will go to the /tmp/wordpress directory. Now, create a .htaccess file which is used by WordPress. The following figure is shown this command.

```
cs2017026@cs2017026:/tmp$ touch /tmp/wordpress/.htaccess
```

- In this command,

  touch – This command creates empty files or change files timestamps.
- Our WordPress configurations are saved in the wp-config.php file. Then, a new WordPress installation comes with a sample config file which can copy to the wp-config.php file. We do this copy using the following command.

```
cs2017026@cs2017026:/tmp$ cp /tmp/wordpress/wp-config-sample.php /tmp/wordpress/wp
-config.php
cs2017026@cs2017026:/tmp$
```

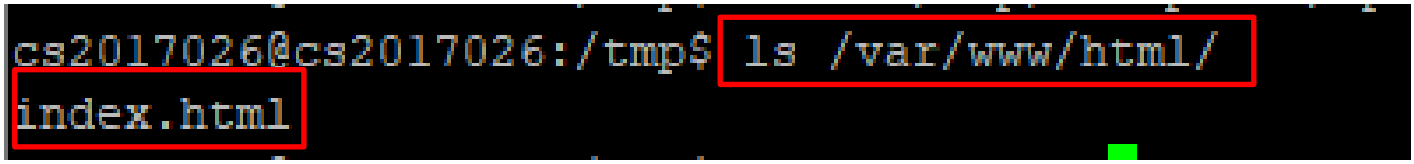
- In this command,

  cp – copy
- Basically, WordPress sends upgrades or security patches after they discovered a vulnerability. They are handled initially by upgrades directory. So, you should create a directory to prevent WordPress from running into the permission issues. The following figure shows this creating of this directory.

```
cs2017026@cs2017026:/tmp$ mkdir /tmp/wordpress/wp-content/upgrade
```

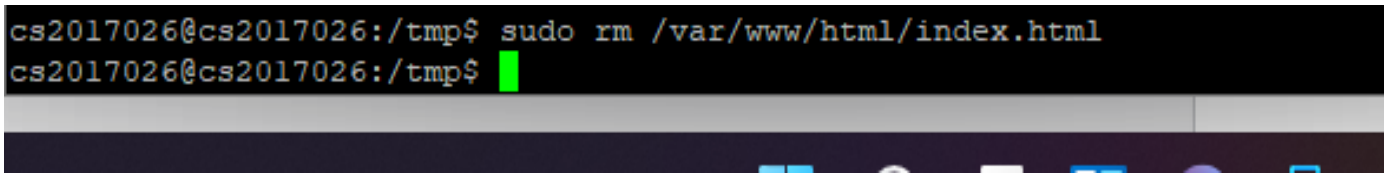
- In this command,

  mkdir – make directory
- After that the contents of /tmp/wordpress directory need to be moved into the /var/www/html directory. At first, we must identify files in that directory using following command.



- In this previous command,
  ls – list

- There is a file called 'index.html' there. So, we should remove this file in this directory because server can host only one page at a time. To remove, you can use the following command.



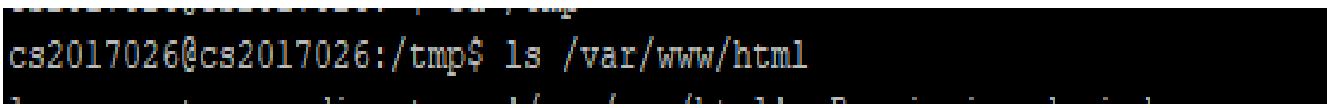
- In this command,
  sudo – Super user(root)
  rm – remove files

- Then, we should copy the extracted WordPress files from the /tmp directory. We can do this one using the following command.

- In this command,

  sudo – Super user(root)
  cp – copy files
  '.' – Ensures every content of the directory is copied.
  /tmp/wordpress/ - Source directory
  /var/www/html/ - destination directory

- If you change the directory into /var/www/html directory and list of contents, then you can see the WordPress files like below figure.



```
index.php          wp-blog-header.php    wp-cron.php          wp-mail.php
license.txt        wp-comments-post.php  wp-includes          wp-settings.php
readme.html        wp-config.php         wp-links-opml.php    wp-signup.php
wp-activate.php    wp-config-sample.php  wp-load.php          wp-trackback.php
wp-admin           wp-content            wp-login.php         xmlrpc.php
```

- After do that one, we should set up user permissions and database credentials in the WordPress directory. The ownership of the WordPress directory currently available for sudo user. So, we should change the ownership to the www-data user and group. That uses the apache web server. This ownership change allows WordPress to read and write files. So, we can do this task using the following command.

```
cs2017026@cs2017026:/tmp$ sudo chown -R www-data:www-data /var/www/html
cs2017026@cs2017026:/tmp$
```

- In this command,
  - sudo – Super user(root)
  - chown – This allows to change the user and group ownership of a given directory or file.
- All of subdirectories of WordPress installation need the right permissions. Thus, we can change their permissions using the following commands.

```
cs2017026@cs2017026:/tmp$ sudo find /var/www/html/ -type d -exec chmod 750 {} \;
cs2017026@cs2017026:/tmp$ sudo find /var/www/html/ -type f -exec chmod 640 {} \;
```

- In these commands,

  sudo – Super user(root)
  find – Search for files in a directory hierarchy in a database or not.
  chmod – This allows to change the permissions on a file using a symbolic or numeric mode or a reference file.

- Then we need to update the WordPress configuration file. At first, we need to change the secret keys to improve the security of the installation. So, the WordPress offers a secret key generator utility, we can use this to get some very high secure keys. The following command illustrates this one.

```
cs2017026@cs2017026:/tmp$ curl -s https://api.wordpress.org/secret-key/1.1/salt/
```

- In this code,

  curl – This is a command line tool to transfer data to or from a server.

- After entering this command, you will see below like figure.

```
define('AUTH_KEY',         'a}$HO$tHesJJ{,@eRq` R|h6w+#)Me|c,F8:V|Et7E@aiX(tAsloqe
-BAj| s7:e');
define('SECURE_AUTH_KEY',  'xDP=7$n?XUeAE@Atdx+w[0!2F-G^P._T5iR@.~oLtJVb`3!-flXQtY
^N7v%,/[`>');
define('LOGGED_IN_KEY',    'LihLdRN~eCN=o{Z)w6goVL-sA{LPQbB3Cn6_*%w VkC*#0q6#Bq-(l
$lixnEL^k(');
define('NONCE_KEY',        'JG|cFlUPTAI,gi%^Kj4-qmocW<7w;fCFF:o%cAb?[++yTT9J[&T_ay
yb!i?;Ls46');
define('AUTH_SALT',        '#`B#XoSd)3,d<|b`xE,qB8]&PCmYTrV&TcCB<Bm?ZhLnkUbMbIJ.X
lS%ZjJ;}7w');
define('SECURE_AUTH_SALT', 'yS4gkR60p>+c6RU ;6{`^u-ssgG+FWLIYv^RaeMs!Ln?<|=S3cuBgl
/ve*lKZ2}-');
define('LOGGED_IN_SALT',   '|-V@GD*N$@-N)sN8+L>N7~PlxY.!mGH9ZU|)z+;0ed4/JC|+b(z,bj
Z-]E7h!v|y');
define('NONCE_SALT',       'H>n+svMv*F+X5^dWkf]Wx}V{f_7|QCR|}]mw7]=b=hg8{`decmx]yg
nJp7>lG}Ge');
cs2017026@cs2017026:/tmp$
```

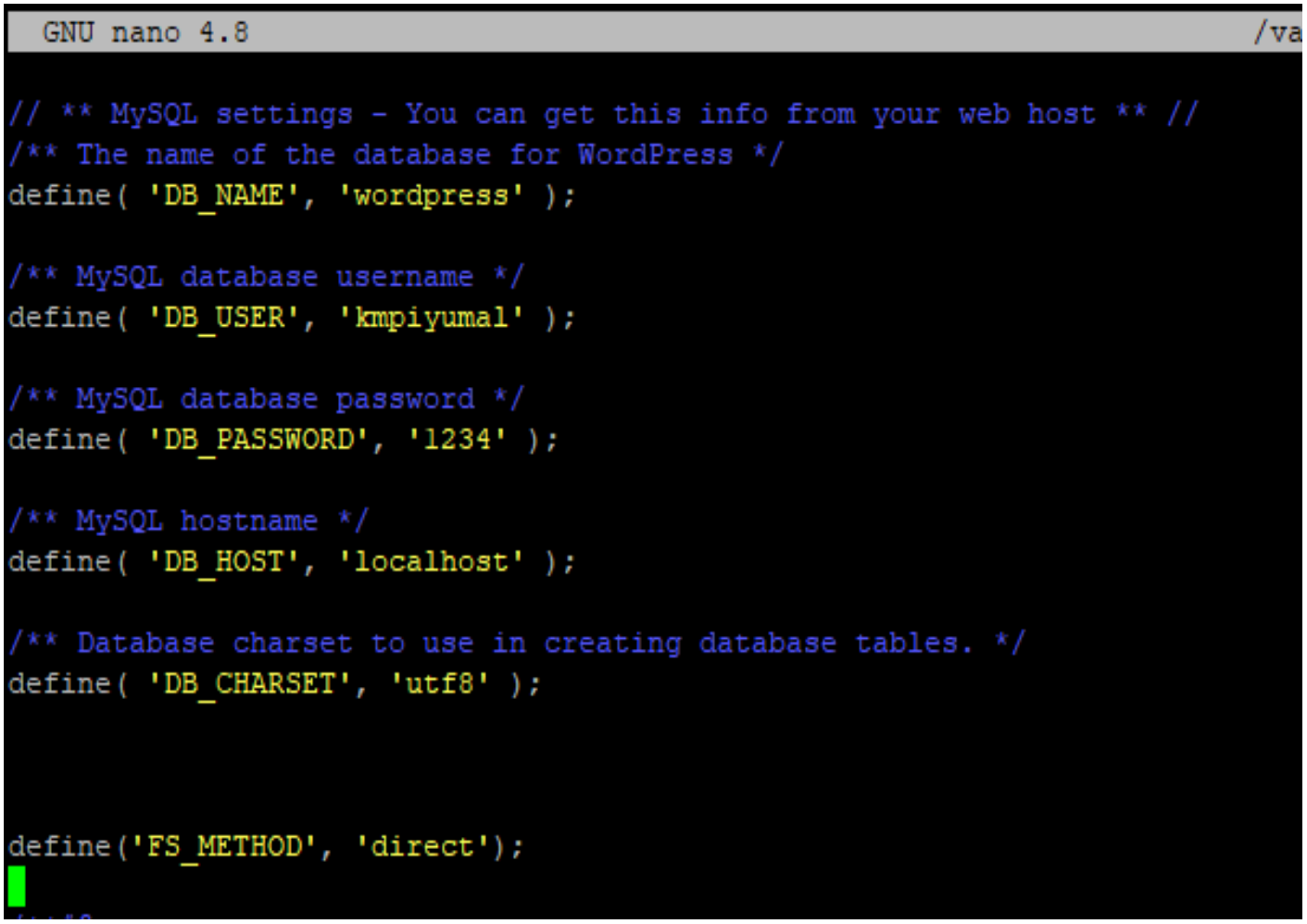
- So, now we should copy these keys and paste in the wp-config.php file. So, you can open the wp-config.php file using the following command.

```
cs2017026@cs2017026:/tmp$ sudo nano /var/www/html/wp-config.php
```

- You can paste the sections like in below figure.

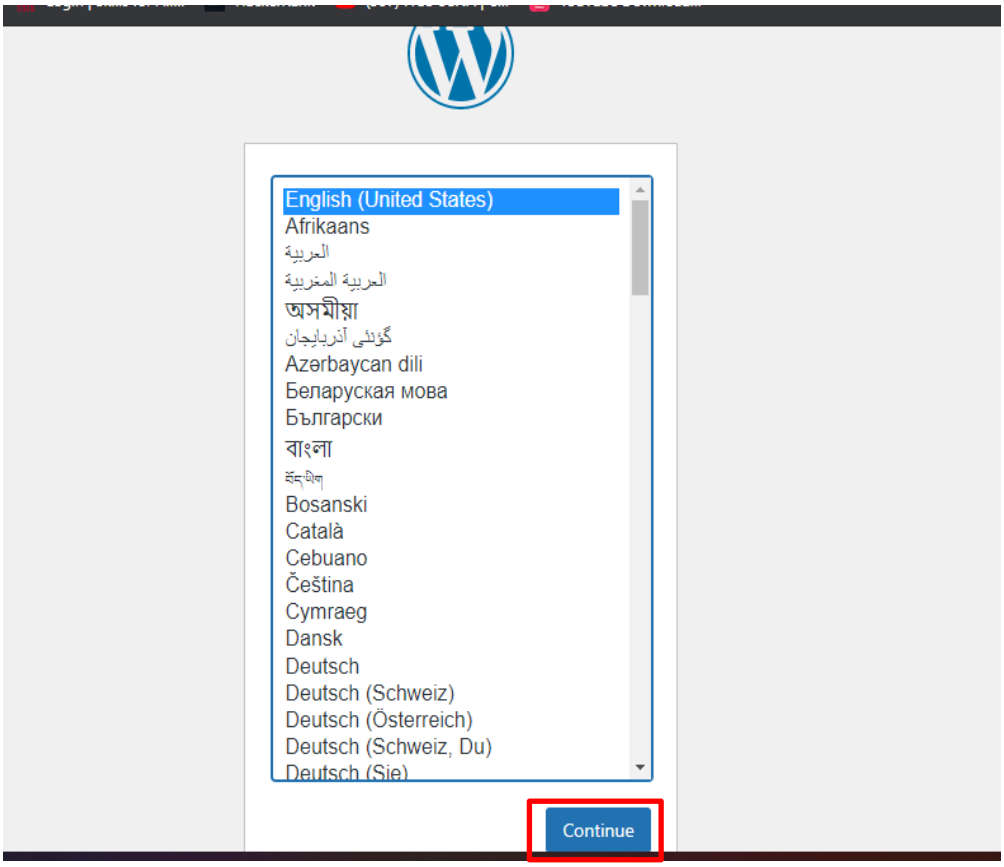
```
 * @since 2.6.0
 */
define( 'AUTH_KEY',         'a}$HO$tHesJJ{,@eRq` R|h6w+#)Me|c,F8:V|Et7E@aiX(tAsloqe-BAj| s7:e' );
define( 'SECURE_AUTH_KEY',  'xDP=7$n?XUeAE@Atdx+w[0!2F-G^P._T5iR@.~oLtJVb`3!-flXQtY^N7v%,/[`>' );
define( 'LOGGED_IN_KEY',    'LihLdRN~eCN=o{Z)w6goVL-sA{LPQbB3Cn6_*%w VkC*#0q6#Bq-(l$lixnEL^k(' );
define( 'NONCE_KEY',        'JG|cFlUPTAI,gi%^Kj4-qmocW<7w;fCFF:o%cAb?[++yTT9J[&T_ayyb!i?;Ls46' );
define( 'AUTH_SALT',        '#`B#XoSd)3,d<|b`xE,qB8]&PCmYTrV&TcCB<Bm?ZhLnkUbMbIJ.X lS%ZjJ;}7w' );
define( 'SECURE_AUTH_SALT', 'yS4gkR60p>+c6RU ;6{`^u-ssgG+FWLIYv^RaeMs!Ln?<|=S3cuBgl/ve*lKZ2}-' );
define( 'LOGGED_IN_SALT',   '|-V@GD*N$@-N)sN8+L>N7~PlxY.!mGH9ZU|)z+;0ed4/JC|+b(z,bjZ-]E7h!v|y' );
define( 'NONCE_SALT',       'H>n+svMv*F+X5^dWkf]Wx}V{f_7|QCR|}]mw7]=b=hg8{`decmx]ygnJp7>lG}Ge' );

/**#@-*/

/**
```

- After that you should think about the communication between WordPress and MySQL database, at the beginning of this config file MySQL settings section. It should fill using your previously given information about the MySQL database. The following figure is shown the filled data set.

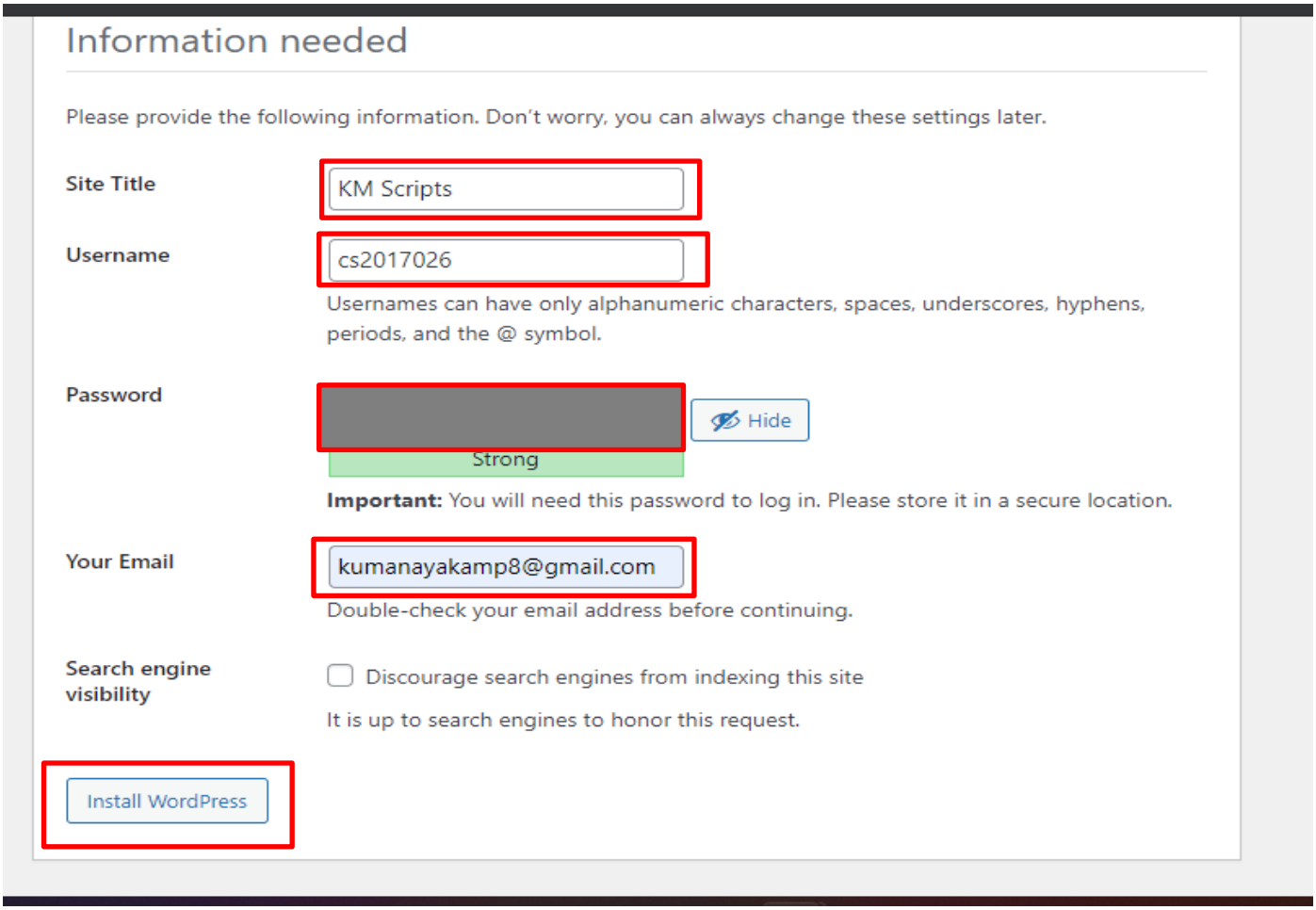


- So, you have to change DB_NAME, DB_USER and password as your credentials. Then you need to define a method that WordPress use to write on the file system. The Apache server has the right permissions to access all of directories in the WordPress installation directory, you can set the file system access method to direct. 'define('FS_METHOD', 'direct')' is the that method. After the changes you can close this file using CTRL + O to save and then CTRL + X to exit in the wp-config file.

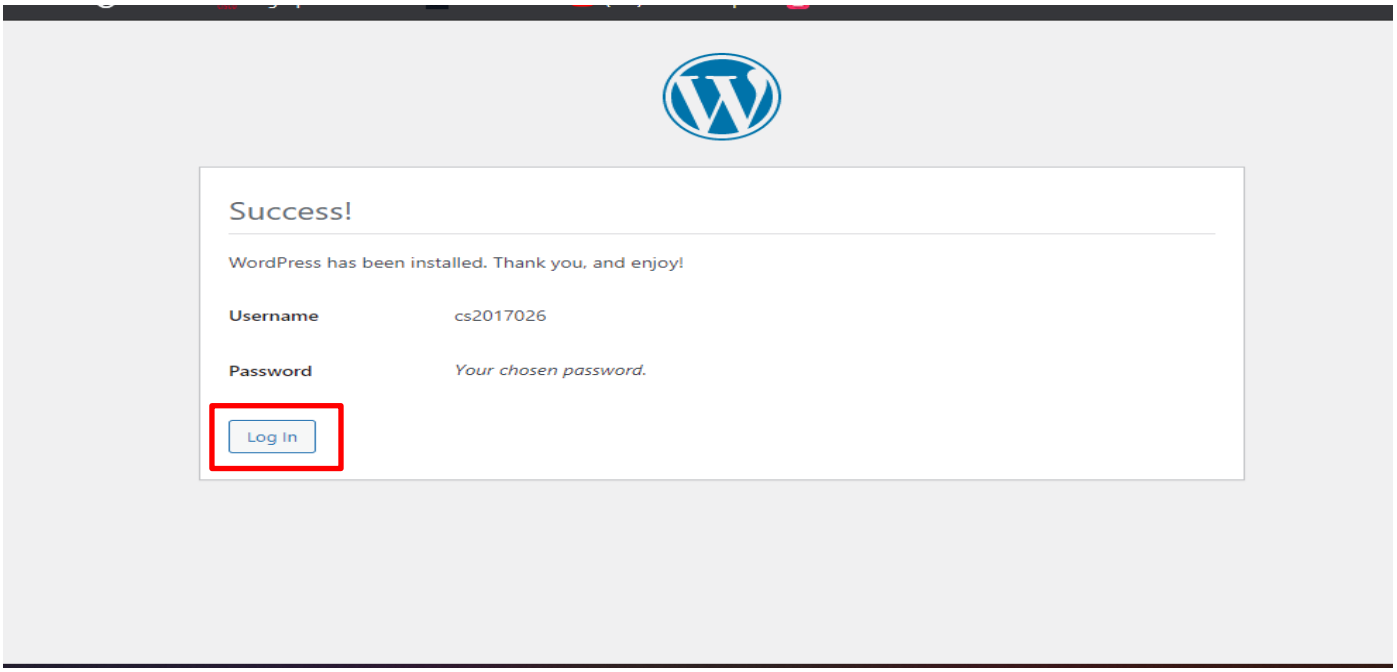
- After that you can finalize your installation through your website. At the beginning you can see below like figure in your website.



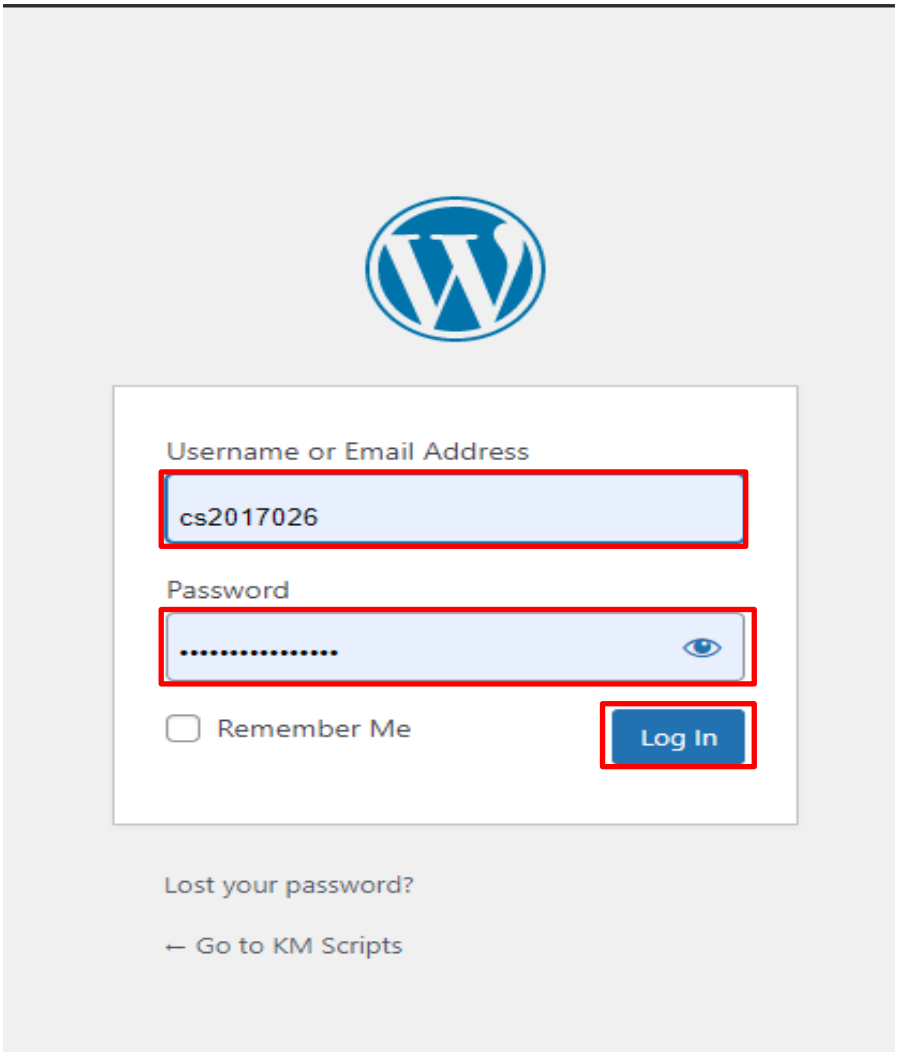
- At first you should select your language from the above list and then click on continue button. After that you will see a below like figure.



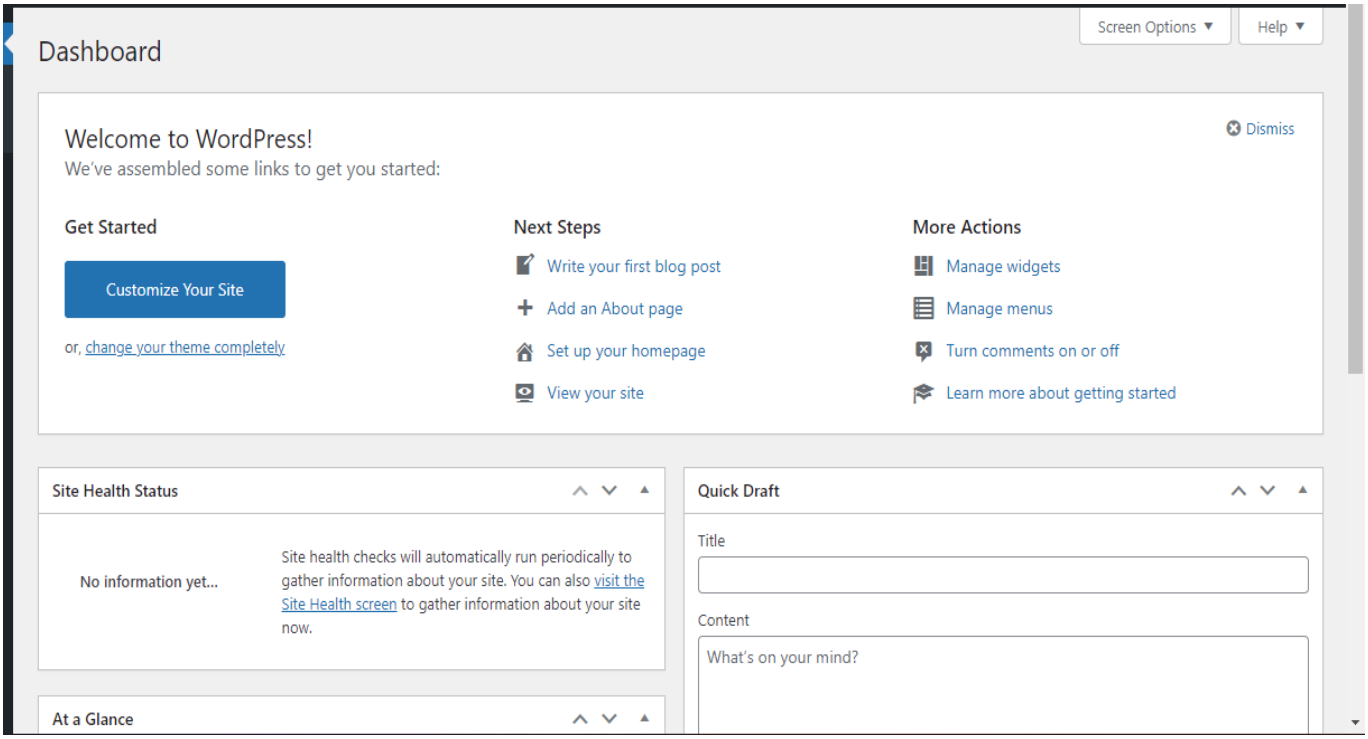
❖ After that you should fill those fields as you like in above figure. Then click on install WordPress'. After, you will see a below like figure.



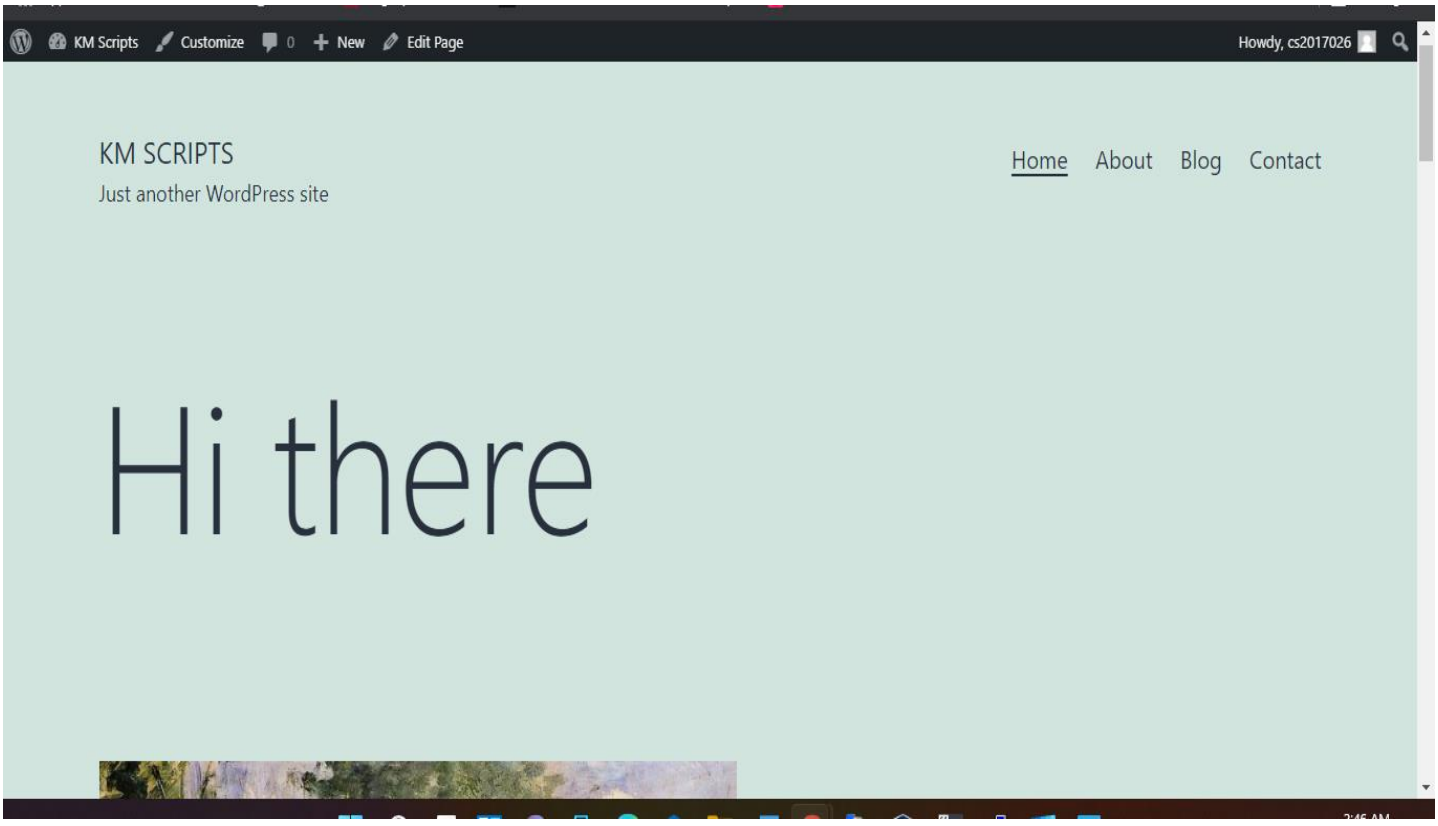
- In the above figure you have to click on Log in button. After that you can see the below figure.



- Then you have to give your username and password. After that click on Log in button to log into the WordPress. Then you will see a below like figure.



- After that you can create your own web site as you like.



7. Summery

In this whole document is mainly delivering about creating a own web server for a company. So, when building this web server, I used LAMP(Linux, Apache, MySQL, Php) method to create this web server. I started with some basic configurations such as ubuntu installation, putty configuration and setting up the time zones. Then I made the LAMP configuration. In LAMP configuration is started with updating and installing the Linux environment, Apache server, MySQL database and Php. Then doing such things in these environments and get a non-secured server with 'http' connection. To fulfill this task, in the above steps I used 'freenom' website to get a valid domain name and I used 'SSL For Free' web site to get a SSL certificate. After that, I installed the WordPress' in our web server. Finally, I configured the WordPress in our web server and create a small frond side web site. Also, to fulfill this task, I used 'putty', 'WinSCP' applications.

8. References

CloudSigma. 2021. *How to Install WordPress with LAMP on Ubuntu 20.04*. [online] Available at: <https://www.cloudsigma.com/how-to-install-wordpress-with-lamp-on-ubuntu-20-04/> [Accessed 16 September 2021].

CloudSigma. 2021. *LAMP Stack setup - Linux Apache MySQL PHP*. [online] Available at: <https://www.cloudsigma.com/lamp-stack-setup-linux-apache-mysql-php/> [Accessed 16 September 2021].

CloudSigma. 2021. *Setting Up Apache Virtual Hosts on Ubuntu 20.04*. [online] Available at: <https://www.cloudsigma.com/setting-up-apache-virtual-hosts-on-ubuntu-20-04/> [Accessed 16 September 2021].

DigitalOcean. 2021. *Apache Configuration Error AH00558: Could not reliably determine the server's fully qualified domain name | DigitalOcean*. [online] Available at: <https://www.digitalocean.com/community/tutorials/apache-configuration-error-ah00558-could-not-reliably-determine-the-server-s-fully-qualified-domain-name> [Accessed 16 September 2021].

Manage.sslforfree.com. 2021. *SSL For Free Login*. [online] Available at: <https://manage.sslforfree.com/certificate/install/ad1fa44a8f1280aa272d8a95e3398954> [Accessed 15 September 2021].

My.freenom.com. 2021. *Client Area - Freenom*. [online] Available at: <https://my.freenom.com/clientarea.php?managedns=kmpiyumal.tk&domainid=1120668432> [Accessed 15 September 2021].

Savvy Security. 2021. *How to Install SSL Certificate on Ubuntu using Apache*. [online] Available at: <https://cheapsslsecurity.com/blog/install-ssl-certificate-ubuntu-server-using-apache/> [Accessed 16 September 2021].

Wilson, J., 2021. *How to Install WordPress with LEMP on Ubuntu 20.04*. [online] RoseHosting. Available at: <https://www.rosehosting.com/blog/how-to-install-wordpress-with-lemp-on-ubuntu-20-04/> [Accessed 15 September 2021].

Youtube.com. 2021. [online] Available at: <https://www.youtube.com/watch?v=HxyKP4oesY0> [Accessed 15 September 2021].