# Documentation for FOC CA2

## Bash script to run all required tasks

#!/bin/bash  
### 20.04.1-Ubuntu  
### Follow all \*\*\*Instructions\*\*\* marked by 3 \*  
###  
  
### Variables  
### \*\*\*Change accordingly\*\*\*  
admNum=p1234567  
password=wordpress123  
ip=`ip -4 addr show ens33 | grep -oP '(?<=inet\s)\d+(\.\d+){3}'`  
  
### Update and Upgrade  
### \*\*\*Comment out if internet is weak\*\*\*  
apt-get update  
apt-get upgrade -y  
  
### Download required packages  
apt-get install apache2 -y  
apt-get install php libapache2-mod-php php-mysql -y  
apt-get install mysql-server -y  
apt-get install rsyslog -y  
apt-get install curl  
  
### Change hostname  
hostname $admNum  
  
### Add 2 groups and 3 users  
groupadd "Admin"  
groupadd "WPAdmin"  
  
usermod -aG Admin $USER  
usermod -aG WPAdmin www-data  
  
useradd -m -s /bin/bash -G Admin shawn  
echo "User shawn created. Please use 'passwd \*username\*' to change."  
  
useradd -m -s /bin/bash -G WPAdmin latisha  
echo "User latisha created. Please use 'passwd \*username\*' to change."  
  
useradd -m -s /bin/bash -G WPAdmin levon  
echo "User levon created. Please use 'passwd \*username\*' to change."  
  
# Give Admin sudo rights  
echo "%Admin ALL=(ALL:ALL) ALL" | EDITOR="tee -a" visudo  
  
### Replicates mysql\_secure\_installation   
mysql -e "DELETE FROM mysql.user WHERE User=''"  
mysql -e "DELETE FROM mysql.user WHERE User='root' AND Host NOT IN ('localhost', '127.0.0.1', '::1')"  
mysql -e "DROP DATABASE IF EXISTS test"  
mysql -e "DELETE FROM mysql.db WHERE Db='test' OR Db='test\\\_%'"  
mysql -e "FLUSH PRIVILEGES"  
  
### Create website directory and configure apache2 to point to that directory  
mkdir /var/www/html/$admNum  
sed -i -e "s\_<Directory /var/www/>\_<Directory /var/www/html/$admNum>\_" /etc/apache2/apache2.conf   
  
### Setup self-signed HTTPS  
### Create self-signed certificate  
sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/apache-selfsigned.key -out /etc/ssl/certs/apache-selfsigned.crt -subj "/C=SG/ST=Singapore/L=Singapore/O=We Sell Owls/OU=IT/CN=wesellowls.com"  
### Configure SSL settings  
cat << EOF > /etc/apache2/conf-available/ssl-params.conf  
SSLCipherSuite EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH  
SSLProtocol All -SSLv2 -SSLv3 -TLSv1 -TLSv1.1  
SSLHonorCipherOrder On  
Header always set X-Frame-Options DENY  
Header always set X-Content-Type-Options nosniff  
SSLCompression off  
SSLUseStapling on  
SSLStaplingCache "shmcb:logs/stapling-cache(150000)"  
SSLSessionTickets Off  
EOF  
  
### Set up ssl virtualhost  
sudo cp /etc/apache2/sites-available/default-ssl.conf /etc/apache2/sites-available/default-ssl.conf.bak  
cat << EOF > /etc/apache2/sites-available/default-ssl.conf  
<IfModule mod\_ssl.c>  
 <VirtualHost \_default\_:443>  
 ServerAdmin admin@wesellowls.com  
 ServerName $ip  
  
 DocumentRoot /var/www/html/$admNum  
  
 ErrorLog \${APACHE\_LOG\_DIR}/error.log  
 CustomLog \${APACHE\_LOG\_DIR}/access.log combined  
  
 SSLEngine on  
  
 SSLCertificateFile /etc/ssl/certs/apache-selfsigned.crt  
 SSLCertificateKeyFile /etc/ssl/private/apache-selfsigned.key  
  
 <FilesMatch "\.(cgi|shtml|phtml|php)\$">  
 SSLOptions +StdEnvVars  
 </FilesMatch>  
 <Directory /usr/lib/cgi-bin>  
 SSLOptions +StdEnvVars  
 </Directory>  
  
 </VirtualHost>  
</IfModule>  
EOF  
  
### redirect HTTP to HTTPS  
cat << EOF > /etc/apache2/sites-available/000-default.conf  
<VirtualHost \*:80>  
 ServerAdmin webmaster@localhost  
 DocumentRoot /var/www/html/$admNum  
 Redirect "/" "https://$ip"  
 ErrorLog \${APACHE\_LOG\_DIR}/error.log  
 CustomLog \${APACHE\_LOG\_DIR}/access.log combined  
</VirtualHost>  
EOF  
  
### Enable those stuff ^^^  
a2enmod ssl  
a2enmod headers  
a2ensite default-ssl  
a2enconf ssl-params  
systemctl reload apache2  
  
### Download wordpress and unpack it  
wget https://wordpress.org/latest.tar.gz -O /var/www/html/$admNum/wordpress.tar.gz  
tar --strip-components=1 -xvzf /var/www/html/$admNum/wordpress.tar.gz -C /var/www/html/$admNum  
rm /var/www/html/$admNum/wordpress.tar.gz  
cp /var/www/html/$admNum/wp-config-sample.php /var/www/html/$admNum/wp-config.php  
  
### Add www-data to WPAdmin group  
usermod -aG WPAdmin www-data  
chmod 775 -R /var/www/  
chown www-data:WPAdmin -R /var/www  
  
### Create wordpress database and wordpress user. Change mysql root password  
### \*\*\*ALTER USER is for (version 8) mysql\*\*\*  
mysql -e "CREATE USER 'wordpress-user-$admNum'@'localhost' IDENTIFIED BY '$password'"  
mysql -e "CREATE DATABASE \`wordpress-db-$admNum\`"  
mysql -e "GRANT ALL PRIVILEGES ON \`wordpress-db-$admNum\`.\* TO 'wordpress-user-$admNum'@'localhost'"  
mysql -e "FLUSH PRIVILEGES"  
mysql -e "ALTER USER 'root'@'localhost' IDENTIFIED WITH mysql\_native\_password BY '$password'"  
  
### Configure wordpress to use mysql   
sed -i -e "s/database\_name\_here/wordpress-db-$admNum/" /var/www/html/$admNum/wp-config.php  
sed -i -e "s/username\_here/wordpress-user-$admNum/" /var/www/html/$admNum/wp-config.php  
sed -i -e "s/password\_here/$password/" /var/www/html/$admNum/wp-config.php  
  
### Get security key  
SALT=$(curl -L https://api.wordpress.org/secret-key/1.1/salt/)  
STRING='put your unique phrase here'  
printf '%s\n' "g/$STRING/d" a "$SALT" . w | ed -s /var/www/html/$admNum/wp-config.php  
  
### Fix remote access  
echo "define('WP\_HOME','https://$ip');" >> /var/www/html/$admNum/wp-config.php  
echo "define('WP\_SITEURL','https://$ip');" >> /var/www/html/$admNum/wp-config.php  
  
### Increase file upload size  
sed -i -e "s/post\_max\_size\ =\ 8M/post\_max\_size\ =\ 10M/" /etc/php/\*/apache2/php.ini  
sed -i -e "s/upload\_max\_filesize\ =\ 2M/upload\_max\_filesize\ =\ 10M/" /etc/php/\*/apache2/php.ini  
  
### Location of logs  
tail -n 20 /var/log/apache2/access.log  
tail -n 20 /var/log/syslog  
tail -n 20 /var/log/mysql/error.log  
tail -n 20 /var/log/apache2/error.log

## Introduction

We will be installing stuff so use root (sudo su).

Why I am using 20.04 Ubuntu instead of the given ISO?

The ISO's kernel is exploitable to (Linux Kernel 4.10 < 5.1.17 - 'PTRACE\_TRACEME' pkexec Local Privilege Escalation)

That is why it is recommended to keep your servers up to date.

In terms of logging, it is also recommended to keep them somewhere else as a backup.

## Task 1

### Change hostname

hostname p0000000



\*Change /etc/hostname if your hostname is still the same.

## Task 2

### Install Apache web server, PHP and Mysql server

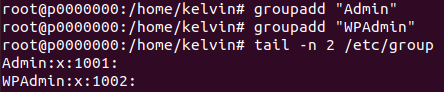
apt-get install apache2 -y  
apt-get install php libapache2-mod-php php-mysql -y  
apt-get install mysql-server -y

## Task 3

### Create Groups and Permissions

Create Groups

groupadd "Admin"  
groupadd "WPAdmin"



Create Users

-m (Create a user directory in /home)

-s (Configure user to use that shell)

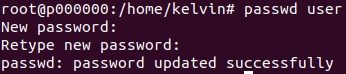
-G (Add user to group) \*OPTIONAL

useradd -m -s /bin/bash -G Admin user



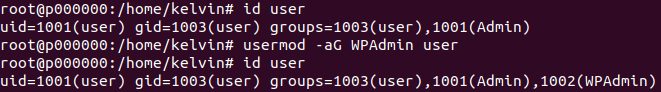
Change user password

passwd user



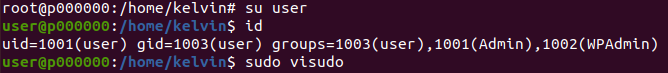
Add user to group

usermod -aG Admin user

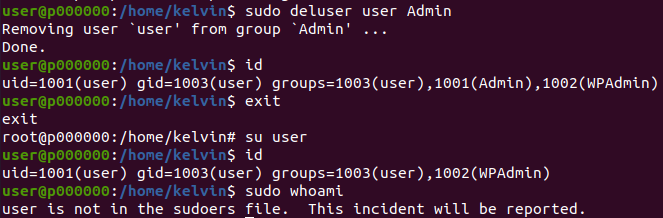


Give sudo rights to “Admin” group

echo "%Admin ALL=(ALL:ALL) ALL" | EDITOR="tee -a" visudo







## Task 4

### Install, Configure and Monitor Wordpress web site

#### Change apache2 directory

Make directory and point apache2 to that directory

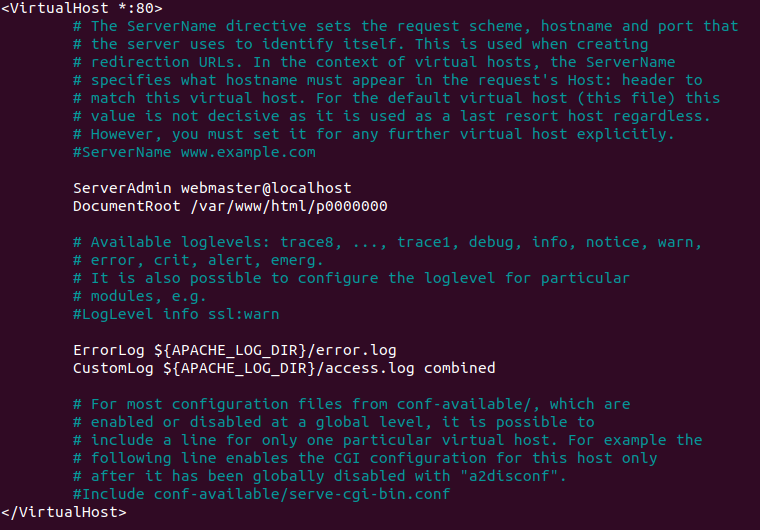
mkdir /var/www/html/p0000000  
sed -i -e "s\_<Directory /var/www/>\_<Directory /var/www/html/p0000000>\_" /etc/apache2/apache2.conf



#### HTTP

Change DocumentRoot to your new directory

cat << EOF > /etc/apache2/sites-available/000-default.conf  
<VirtualHost \*:80>  
 ServerAdmin webmaster@localhost  
 DocumentRoot /var/www/html/p0000000  
 ErrorLog \${APACHE\_LOG\_DIR}/error.log  
 CustomLog \${APACHE\_LOG\_DIR}/access.log combined  
</VirtualHost>  
EOF



#### HTTPS

Create self-signed certificate Remove everything after -subj if you want to go through the configurations or edit it

sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/apache-selfsigned.key -out /etc/ssl/certs/apache-selfsigned.crt -subj "/C=SG/ST=Singapore/L=Singapore/O=We Sell Owls/OU=IT/CN=wesellowls.com"

Set up SSL settings

cat << EOF > /etc/apache2/conf-available/ssl-params.conf  
SSLCipherSuite EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH  
SSLProtocol All -SSLv2 -SSLv3 -TLSv1 -TLSv1.1  
SSLHonorCipherOrder On  
Header always set X-Frame-Options DENY  
Header always set X-Content-Type-Options nosniff  
SSLCompression off  
SSLUseStapling on  
SSLStaplingCache "shmcb:logs/stapling-cache(150000)"  
SSLSessionTickets Off  
EOF

Set up ssl virtualhost

cat << EOF > /etc/apache2/sites-available/default-ssl.conf  
<IfModule mod\_ssl.c>  
 <VirtualHost \_default\_:443>  
 ServerAdmin admin@wesellowls.com  
 ServerName 10.10.10.10  
  
 DocumentRoot /var/www/html/p0000000   
  
 ErrorLog \${APACHE\_LOG\_DIR}/error.log  
 CustomLog \${APACHE\_LOG\_DIR}/access.log combined  
  
 SSLEngine on  
  
 SSLCertificateFile /etc/ssl/certs/apache-selfsigned.crt  
 SSLCertificateKeyFile /etc/ssl/private/apache-selfsigned.key  
  
 <FilesMatch "\.(cgi|shtml|phtml|php)\$">  
 SSLOptions +StdEnvVars  
 </FilesMatch>  
 <Directory /usr/lib/cgi-bin>  
 SSLOptions +StdEnvVars  
 </Directory>  
  
 </VirtualHost>  
</IfModule>  
EOF

Set up HTTP redirection to HTTPS

cat << EOF > /etc/apache2/sites-available/000-default.conf  
<VirtualHost \*:80>  
 ServerAdmin webmaster@localhost  
 DocumentRoot /var/www/html/p0000000   
 Redirect "/" "https://10.10.10.10"  
 ErrorLog \${APACHE\_LOG\_DIR}/error.log  
 CustomLog \${APACHE\_LOG\_DIR}/access.log combined  
</VirtualHost>  
EOF

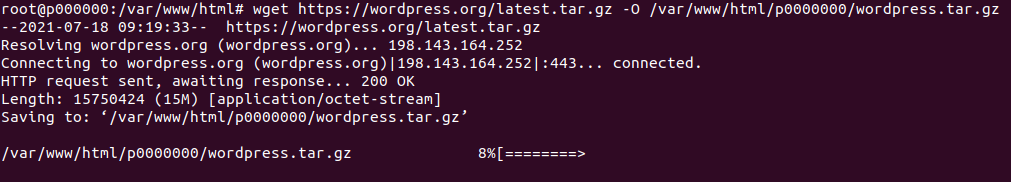
Run to enable previous configurations

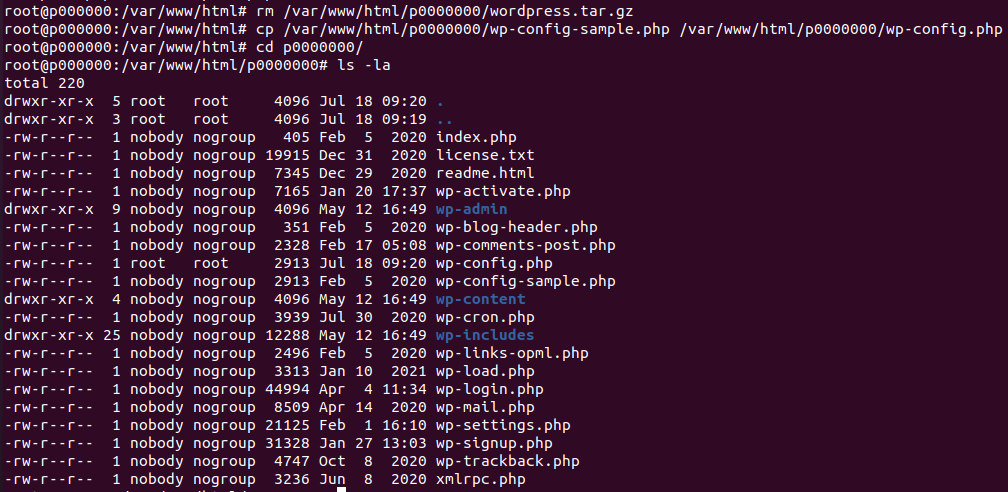
a2enmod ssl  
a2enmod headers  
a2ensite default-ssl  
a2enconf ssl-params  
systemctl reload apache2

#### Install wordpress

Download and untar wordpress to new directory Use wp-config-sample as base config file

wget https://wordpress.org/latest.tar.gz -O /var/www/html/p0000000/wordpress.tar.gz  
tar --strip-components=1 -xvzf /var/www/html/p0000000/wordpress.tar.gz -C /var/www/html/p0000000   
rm /var/www/html/p0000000/wordpress.tar.gz  
cp /var/www/html/p0000000/wp-config-sample.php /var/www/html/p0000000/wp-config.php

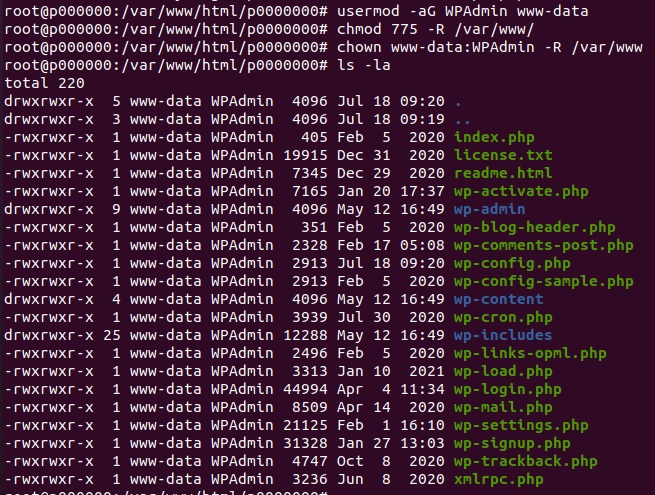




#### Add permissions

Give WPAdmin access to apache2 directory

usermod -aG WPAdmin www-data  
chmod 775 -R /var/www/  
chown www-data:WPAdmin -R /var/www



#### Replicate mysql\_secure\_installation

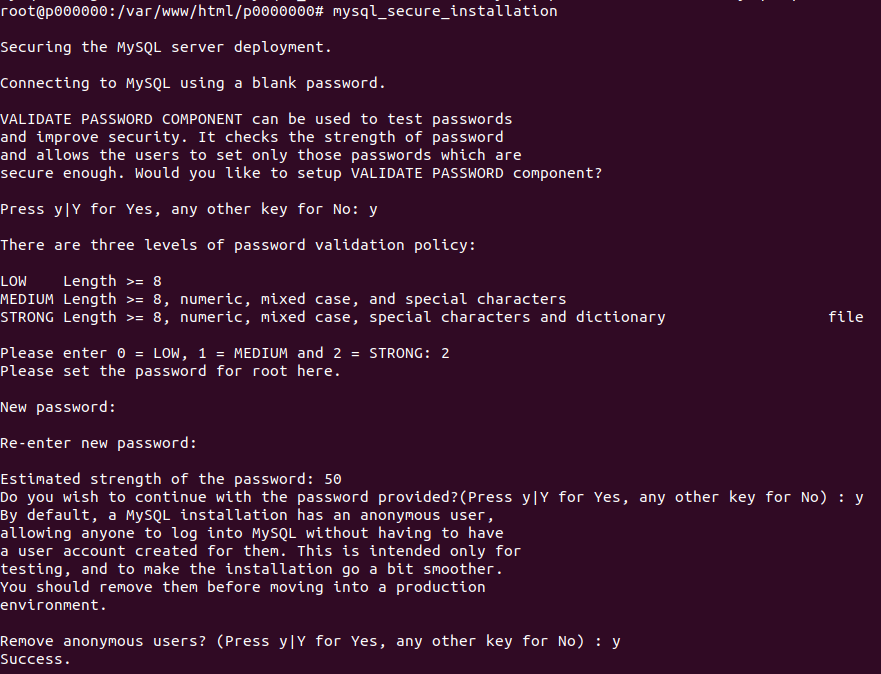
mysql -e "DELETE FROM mysql.user WHERE User=''"

mysql -e "DELETE FROM mysql.user WHERE User='root' AND Host NOT IN ('localhost', '127.0.0.1', '::1')"

mysql -e "DROP DATABASE IF EXISTS test"

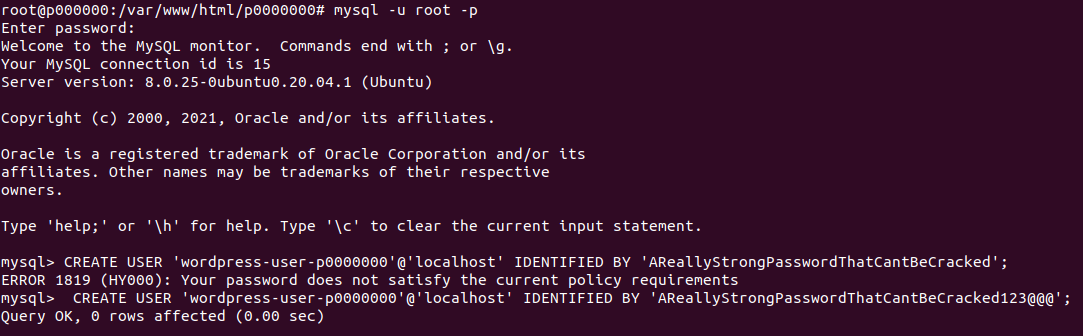
mysql -e "DELETE FROM mysql.db WHERE Db='test' OR Db='test\\\_%'"

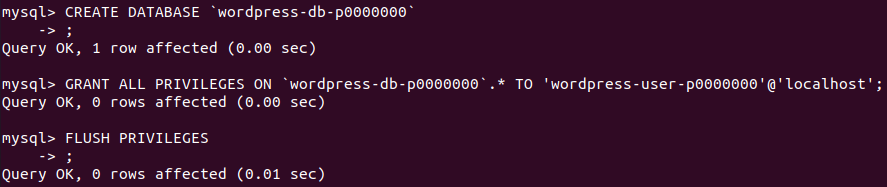
mysql -e "FLUSH PRIVILEGES"



#### Add database and user for wordpress

mysql -e "CREATE USER 'wordpress-user-p0000000'@'localhost' IDENTIFIED BY 'AReallyStrongPasswordThatCantBeCracked'"  
mysql -e "CREATE DATABASE \`wordpress-db-p0000000\`"  
mysql -e "GRANT ALL PRIVILEGES ON \`wordpress-db-p0000000\`.\* TO 'wordpress-user-p0000000'@'localhost'"  
mysql -e "FLUSH PRIVILEGES"





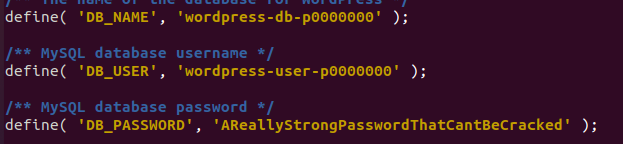
Finally change root password for MySQL

mysql -e "ALTER USER 'root'@'localhost' IDENTIFIED WITH mysql\_native\_password BY 'AReallyStrongPasswordThatCantBeCracked"

#### Configure Wordpress

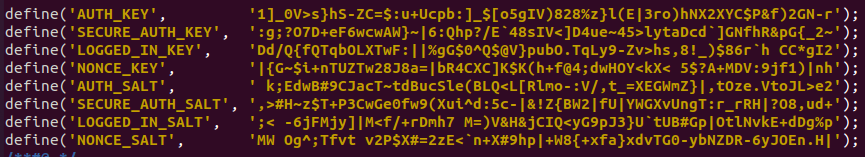
Configure wordpress to use MySQL database

sed -i -e "s/database\_name\_here/wordpress-db-p0000000/" /var/www/html/p0000000/wp-config.php  
sed -i -e "s/username\_here/wordpress-user-p0000000/" /var/www/html/p0000000/wp-config.php  
sed -i -e "s/password\_here/AReallyStrongPasswordThatCantBeCracked/" /var/www/html/p0000000/wp-config.php



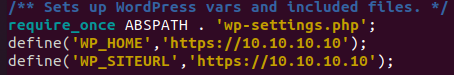
Set security key

SALT=$(curl -L https://api.wordpress.org/secret-key/1.1/salt/)  
STRING='put your unique phrase here'  
printf '%s\n' "g/$STRING/d" a "$SALT" . w | ed -s /var/www/html/p0000000/wp-config.php



Add this so that the website html point to the right IP

echo "define('WP\_HOME','https://10.10.10.10');" >> /var/www/html/p0000000/wp-config.php  
echo "define('WP\_SITEURL','https://10.10.10.10');" >> /var/www/html/p0000000/wp-config.php



Increase file upload size

sed -i -e "s/post\_max\_size\ =\ 8M/post\_max\_size\ =\ 10M/" /etc/php/\*/apache2/php.ini  
sed -i -e "s/upload\_max\_filesize\ =\ 2M/upload\_max\_filesize\ =\ 10M/" /etc/php/\*/apache2/php.ini



#### Getting the logs

tail -n 20 /var/log/apache2/access.log  
tail -n 20 /var/log/syslog  
tail -n 20 /var/log/mysql/error.log  
tail -n 20 /var/log/apache2/error.log

