Troubleshooting Errors

Fixing Broken Permalinks

Solution[1]

Edit the file /etc/apache2/apache2.conf and make sure of the following:

```
<Directory /var/www/>
        Options Indexes FollowSymLinks
        AllowOverride All
        Require all granted
</Directory>
```

Also in /etc/apache2/sites-available/your_site.conf:

```
<Directory /var/www/your_site_path/>
    AllowOverride All
</Directory>
```

Solution [2]

In /etc/apache2/apache2.conf

Make sure that AllowOverride is [all]

```
<Directory /var/www/>
        AllowOverride All
        Require all granted
</Directory>
```

Solution [3]

Remove and then re-add .htaccess file

Fixing Media and Photos Not Appearing In Media Library

Solution [1]

Add the following to wp-config.php before happy editing stuff

```
define( 'UPLOADS', 'wp-content/uploads' );
```

Solution [2]

Install the thumbnail regenerator plugin

```
https://wordpress.org/plugins/regenerate-thumbnails/
```

Deleting media library all at once

Solution [1]

Use the media cleaner plugin

```
https://wordpress.org/plugins/media-
cleaner/
```

Solution [2]

Login to my phpmyadmin and select the wordpress database. Execute the below commands in SQL editor

```
DELETE FROM `wp_posts` WHERE `post_type` =
"attachment";


DELETE FROM `wp_postmeta` WHERE `meta_key`
= "_wp_attached_file";


DELETE FROM `wp_postmeta` WHERE `meta_key`
= "_wp_attachment_metadata";
```

Disable wordpress automatic cropping of photos

```
https://wordpress.org/plugins/image-sizes/
```

Enabling plugin download without FTP

Add the following to wp-config.php before happy editing stuff

```
define('FS_METHOD','direct');
```

Changing Site-URL

Add the following to wp-config.php before happy editing stuff

```
define( 'WP_HOME', 'http://example.com' );
define( 'WP_SITEURL', 'http://example.com' );
```

Install SSL in Google Cloud

```
wget https://dl.eff.org/certbot-auto && chmod a+x certbot-auto

./certbot-auto certonly --webroot -w /var/www/html/ -d 1pagezen.com -d www.1pagezen.com
```

```
sudo nano /etc/apache2/sites-
available/default-ssl.conf>
```

Add this between Documentroot and ServerAdmin

```
  <Directory /var/www/html/>
Options Indexes FollowSymLinks MultiViews
AllowOverride All
Order allow,deny
allow from all
</Directory>
```

Then replace snakeoil certs with the following after editing your domain

```
SSLCertificateFile
"/etc/letsencrypt/live/1pagezen.com/cert.pem"
SSLCertificateKeyFile
"/etc/letsencrypt/live/1pagezen.com/privkey.pem"
SSLCertificateChainFile
"/etc/letsencrypt/live/1pagezen.com/chain.pem"
```

Then edit the following file
sudo nano /etc/apache2/sites-
available/wordpress.conf
Replace everything with:

```
<VirtualHost *:80>
ServerAdmin webmaster@localhost
DocumentRoot /var/www/html
ServerName www.1pagezen.com
ServerAlias 1pagezen.com
Redirect permanent /
https://www.1pagezen.com/
<Directory />
Options FollowSymLinks
AllowOverride None
</Directory>
<Directory /var/www/html/>
Options Indexes FollowSymLinks MultiViews
AllowOverride All
Order allow,deny
allow from all
</Directory>
ScriptAlias /cgi-bin/ /usr/lib/cgi-bin/
<Directory "/usr/lib/cgi-bin">
AllowOverride None
```

```
Options +ExecCGI -MultiViews
+SymLinksIfOwnerMatch
Order allow,deny
Allow from all
</Directory>
ErrorLog ${APACHE_LOG_DIR}/error.log
LogLevel warn
CustomLog ${APACHE_LOG_DIR}/access.log
combined
</VirtualHost>
```

Then

```
sudo a2ensite default-ssl
sudo a2enmod ssl
sudo service apache2 restart
```

Setup Autorenew

```
sudo mv certbot-auto /etc/letsencrypt/
sudo crontab -e
```

Add the following:

```
<45 2 * * 6 cd /etc/letsencrypt/ &&
./certbot-auto renew &&
```

```
/etc/init.d/apache2 restart>
```

Security

Disable Directory Browsing

Add the following to the end of .htaccess

```
Options All -Indexes
```

Cleaning a compromised wordpress website

Case 1 : Wordpress redirects to another website

#Solution [1]

Check your DNS settings and make sure that they point to the right IP and the right nameservers of your hosting.

#Solution [2]

If DNS records are clean, then the next probable culprit is either the main [index.php] file in the root of your wordpress installation or its either one of the plugins' files has been modified to include a malicious iframe.

Step [1]
Replace all core wordpress files with new ones

```
wp-admin
wp-includes
all php files in the main root directory
of you wordpress i.e; wp-login.php, wp-
settings.php..etc.
```

Step [2]
Delete the current theme and reupload it but with a fresh version from where you bought it.

```
cd /wp-content/themes
sudo rm -r [theme-name]
```

Step [3]
Disable all plugins

```
cd /wp-content/
sudo mv plugins pluginsx
```

Re-enable them back

```
sudo mv pluginsx plugins
```

And then start activating them one by one untill the problem reappears. Delete the infected plugins and reuplad it.

Restore the latest clean backup if all other above methods didn't work.

Case 2: Wordpress hacked and you can't login

Step [1]

Login to your hosting provider and naviage to [phpmyadmin]

step [2]

Find the table [wp-users]

step [3]

Find the strange user and delete it

Step [4]

Add a new admin user for you. From the SQL editor, execute the below

```
INSERT INTO `databasename`.`wp_users`
(`ID`, `user_login`, `user_pass`,
`user_nicename`, `user_email`, `user_url`,
`user_registered`, `user_activation_key`,
`user_status`, `display_name`) VALUES
```

```
('4', 'demo', MD5('demo'), 'Your Name',
'test@yourdomain.com',
'http://www.test.com/', '2011-06-07
00:00:00', '', '0', 'Your Name');

INSERT INTO `databasename`.`wp_usermeta`
(`umeta_id`, `user_id`, `meta_key`,
`meta_value`) VALUES (NULL, '4',
'wp_capabilities', 'a:1:
{s:13:"administrator";s:1:"1";}');

INSERT INTO `databasename`.`wp_usermeta`
(`umeta_id`, `user_id`, `meta_key`,
`meta_value`) VALUES (NULL, '4',
'wp_user_level', '10');
```

Hardening your website

Keep wordpress always up to date

Update themes and plugins regularly

Make sure the permissions are correctly set

Files should have [644] and directories should have [755] both should be owned by your local user not [www-data].

Example of hardening permissions

```
sudo find /var/www/html/mywebsite/ -type d
-exec chmod 755 {} +

sudo find /var/www/html/mywebsite/ -type f
-exec chmod 644 {} +

sudo find /var/www/html/mywebsite/ -type f
chown localuser:localuser {} +

sudo find /var/www/html/mywebsite/ -type d
chown localuser:localuser {} +
```

and finally make apache run as the current local user

```
sudo nano /etc/apache2/envvar
```

and insert your user here

```
export APACHE_RUN_USER=youruser
export APACHE_RUN_GROUP=youruser
```

restart apache2

```
sudo /etc/init.d/apache2 restart
```

Always keep php up to date

Steps to upgrade your php if your managing your server on your own.
Add the following repositories
[1]

```
root@Red-hat:~$:sudo apt -y install lsb-release apt-transport-https ca-certificates
```

[2]

```
root@Red-hat:~$:sudo wget -O /etc/apt/trusted.gpg.d/php.gpg https://packages.sury.org/php/apt.gpg
```

[3]

```
root@Red-hat:~$:sudo apt install software-properties-common
```

[4]

```
root@Red-hat:~$:sudo add-apt-repository
ppa:ondrej/php
```

or: replaces only the fourth command

```
root@Red-hat:~$:echo "deb
https://packages.sury.org/php/
$(lsb_release -sc) main" | sudo tee
/etc/apt/sources.list.d/php.list
```

[5]

```
sudo apt update
sudo apt -y install php7.[VERSION-NUMBER]
sudo apt-get install php7.[VERSION-NUMBER]
{bcmath,bz2,intl,gd,mbstring,mysql,zip}
apt install php7.4-fpm
```

Disable the old version and enable the new one

```
sudo a2dismod php7.0
sudo a2enmod php7.4
```

Restart apache

```
Sudo /etc/init.d/apache2 restart
```

Remove old versions

```
Sudo apt purge php7.0 php7.0-common
apt-get autoremove php7.0
```

Install PhpMyAdmin

```
sudo apt-get install phpMyAdmin php-
mbstring php-gettext

sudo ln -s /etc/phpmyadmin/apache.conf
/etc/apache2/conf-
available/phpmyadmin.conf

sudo a2enconf phpmyadmin.conf

sudo systemctl restart apache2
```

Installing Zlib Extension

```
apt-get update && apt-get install
libgcrypt11-dev zlib1g-dev
```

Then

```
nano /etc/php.ini
```

Make sure that

```
zlib.output_compression = On
zlib.output_compression_level = 6
```

Install wordfence security plugin

Tweaking Performance

Increase wordpress performance - wp-config.php

In wp-config.php, paste this before the 'happy editing'

```
@ini_set( 'upload_max_size' , '128M' );
@ini_set( 'post_max_size', '256M');
@ini_set( 'memory_limit', '512M' );
@ini_set( 'max_input_vars' , 7000 );
```

Increase wordpress performance - php.ini

```
max_input_vars=8000
max_execution_time=70000
memory_limit=256M
```

```
post_max_size=256M
upload_max_filesize=256M
max_input_time=80
```