Wordpress Security

1. Disable custom HTML when possible

Added this code in **wp-config.php** File

```
define( 'DISALLOW_UNFILTERED_HTML', true );
```

2. Remove all Default posts and Comments

Remove all default posts and comments. If malicious hackers find those on your site, it may indicate to them you have a new Wordpress site, and brand new sites are often easier to crack into.

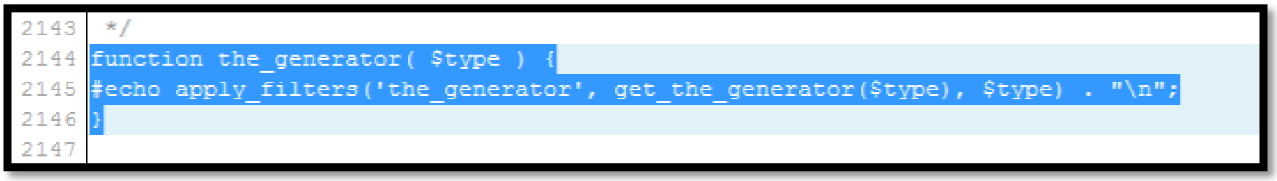
Just to this file **“wp-includes/general-template.php”**

```
function the_generator( $type ) {
echo apply_filters('the_generator', get_the_generator($type), $type) . "\n";
}

After Security

function the_generator( $type ) {
#echo apply_filters('the_generator', get_the_generator($type), $type) . "\n";
}
```

Make sure a hash is applied next to the “echo” command so that it looks like this:



```
 */
function the_generator( $type ) {
#echo apply_filters('the_generator', get_the_generator($type), $type) . "\n";
}
```

3. Delete wp-admin/install.php and wp-admin/upgrade.php

Be sure to delete **/wp-admin/install.php** and **/wp-admin/upgrade.php** after every Wordpress installation or upgrade.

4. Hide indexes

Just open **.htaccess** file and type this code

```
Options –indexes
```

5. Block Some Crucial directories

Your site's **wp-includes/** directory is the most important one to block.

Find the **.htaccess** file there and insert

```
RewriteRule ^(wp-includes)\/.*$ ./ [NC,R=301,L]
```

If there are subdirectories, then use this code

```
RewriteRule ^(wp-includes|subdirectory-name-here)\/.*$ ./ [NC,R=301,L]
```

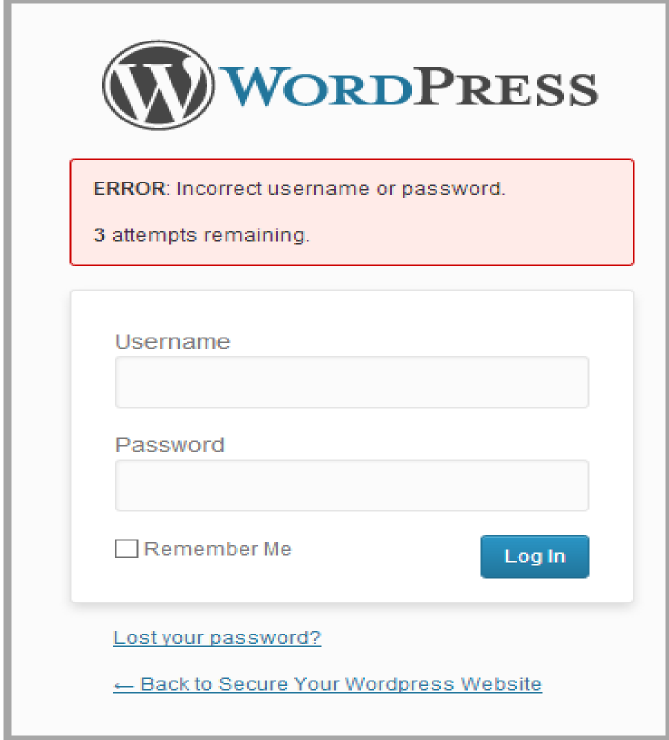
6. **Secure your Admin page with YUBICO**

http://www.yubico.com/ = PAID Plugin

7. **Limit Login Attempts**

Limit the number of login attempts possible both through normal login as well as using auth cookies.

http://wordpress.org/extend/plugins/limit-login-attempts/



ERROR: Incorrect username or password.

3 attempts remaining.

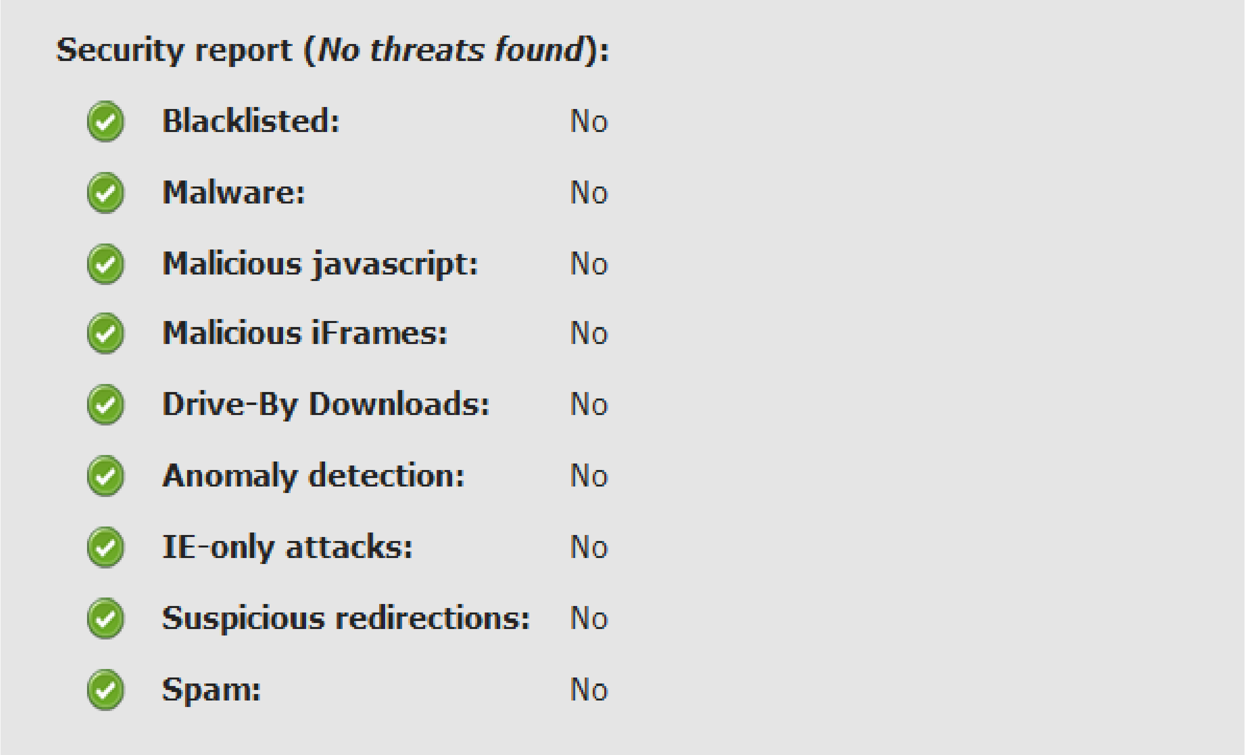
OR

http://wordpress.org/extend/plugins/login-lockdown/

8. Server Side Scanning Online FREE

Web-malware continues to evolve making it challenging to detect using only HTTP fingerprinting techniques, such as the ones Site Check is restricted to.

http://sitecheck.sucuri.net/scanner/



Security report (*No threats found*):

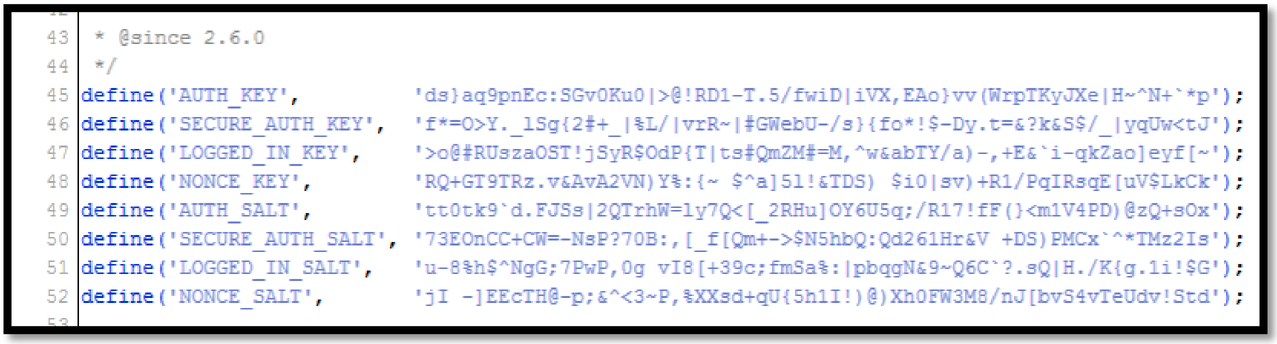
✓	Blacklisted:	No
✓	Malware:	No
✓	Malicious javascript:	No
✓	Malicious iFrames:	No
✓	Drive-By Downloads:	No
✓	Anomaly detection:	No
✓	IE-only attacks:	No
✓	Suspicious redirections:	No
✓	Spam:	No

http://wordpress.org/extend/plugins/better-wp-security/

9. Create Custom Secret Keys

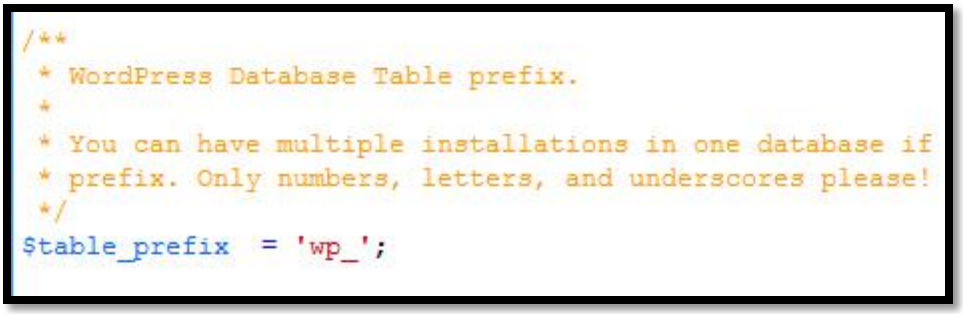
All of the confidential details for your Wordpress site are stored in the **wp-config.php** in your Wordpress root directory. Change these codes as according you like.

For Random Secret Keys, https://api.wordpress.org/secret-key/1.1/salt/



```
 * @since 2.6.0
 */
define('AUTH_KEY',         'ds}aq9pnEc:SGv0Ku0|>@!RD1-T.5/fwiD|iVX,EAo}vv(WrpTKyJXe|H~^N+`*p');
define('SECURE_AUTH_KEY',  'f*=O>Y._lSg{2#+_|%L/|vrR~|#GWebU-/s}{fo*!$-Dy.t=&?k&S$/_|yqUw<tJ');
define('LOGGED_IN_KEY',    '>o@#RUszaOST!jSyR$OdP{T|ts#QmZM#=M,^w&abTY/a)-,+E&`i-qkZao]eyf[~');
define('NONCE_KEY',        'RQ+GT9TRz.v&AvA2VN)Y%:{~ $^a]51!&TDS) $i0|sv)+R1/PqIRsqE[uV$LkCk');
define('AUTH_SALT',        'tt0tk9`d.FJSs|2QTrhW=ly7Q<[_2RHu]OY6U5q;/R17!fF()<m1V4PD)@zQ+sOx');
define('SECURE_AUTH_SALT', '73EOnCC+CW=-NsP?70B:,[_f[Qm+->$N5hbQ:Qd261Hr&V +DS)PMCx`^*TMz2Is');
define('LOGGED_IN_SALT',   'u-8%h$^NgG;7PwP,0g vI8[+39c;fmSa%:|pbqgN&9~Q6C`?.sQ|H./K{g.1i!$G');
define('NONCE_SALT',       'jI -]EEcTH@-p;&^<3~P,%XXsd+qU{5h1I!)@)Xh0FW3M8/nJ[bvS4vTeUdv!Std');
```

10. Change the default database Prefix.



```
/**
 * WordPress Database Table prefix.
 *
 * You can have multiple installations in one database if
 * prefix. Only numbers, letters, and underscores please!
 */
$table_prefix  = 'wp_';
```

11. Protect your wp-config file

As **wp-config.php** file contains all the confidential details of your site. So it's pretty important that you protect it at all costs. An easy way to protect this file is to simply place the following code in your **.htaccess** file on your server.

```
<Files wp-config.php>
order allow,deny
deny from all
</Files>
```

12. Protect your .htaccess file

You just need to place below code in your **.htaccess** file.

```
<Files .htaccess>
order allow,deny
deny from all
</Files>
```

13. Hide your Wordpress Version

To do this you need to place below code in **function.php** of your active theme.

```
remove_action('wp_head', 'wp_generator');
```

You can go one step further and additionally remove it from RSS feeds using this:

```
function wpt_remove_version() {
return '';
}
add_filter('the_generator', 'wpt_remove_version');
```

14. Install Wordpress Security Scan Plugin

This is a good plugin which scans your Wordpress installation and give the suggestion accordingly. This plugin will check for below things:

- Passwords
- File Permissions
- Database Security
- Wordpress Admin protection

http://wordpress.org/extend/plugins/wp-security-scan/

15. Ask Apache Password Protect

You can protect your site with 401 authorization in easy steps.

http://wordpress.org/extend/plugins/askapache-password-protect/

16. Automatically Backup your site

http://wordpress.org/extend/plugins/backwpup/

17. Two Factor Authenticator

The Google Authenticator plugin for Wordpress gives you two-factor authentication using the Google Authenticator app for Android/iPhone/Blackberry.

http://wordpress.org/extend/plugins/google-authenticator/

18. Using .htaccess file as a FIREWALL

```
RedirectMatch 403 \[
```

19. 5G Firewall Beta

http://perishablepress.com/5g-firewall-beta/

20. Allow some IPs

Dashboard from your home or office, this method will help a lot.

```
AuthType Basic
order deny,allow
deny from all
# your home IP address
allow from xxx.xxx.xxx.xxx
# your office IP address
allow from yy.yyy.yyy.yyy
```

21. Protect wp-includes Directory

If you go to http://www.your-site.com/wp-includes, you will see an open folder and this is definitely not safe. You need to create a redirect file in order to forward visitors who access that URL to your main home page.

If you ask yourself, who in the world would access that URL? Well, hackers would? To redirect visitors away from that URL, simply create a new file named **index.html** and put this code in it:

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<html>
<head>
<meta http-equiv="REFRESH" content="0;url=http://www.your-site.com/"></HEAD>
<BODY></BODY>
</HTML>
```

22. Change your permissions

Make sure you change your files permissions to **0744** which means they are read-only to everyone except you. This makes sure that other people are not able to change any of the files on your server.

Set file permissions at **644** and **755** for folders.

23. Install Antivirus for Wordpress

Use this antivirus http://wpantivirus.com/

24. Block Access to wp-content Folder

To block access to your wp-content folder create a new htaccess file and save this at the root level of your wp-content folder.

```
Order deny,allow
Deny from all
<Files ~ ".(xml|css|jpe?g|png|gif|js)$">
Allow from all
</Files>
```

25. Hide Login Error Messages

There is a login page hook to access to remove any error message from the login page.

Copy the following in your **functions.php** file.

```
add_filter('login_errors',create_function('$a', "return null;"));
```

26. Disable Theme and plugin Editor

If you want to stop the editor links from appearing in the admin area you can add the following to your **wp-config.php** file so people cannot edit the theme directly in the admin area.

```
define( 'DISALLOW_FILE_EDIT', true);
```

27. Security from SQL Injection

To avoid that, you can try to secure your files using Apache with a code like this in your **.htaccess file**:

```
<IfModule mod_rewrite.c>
RewriteEngine On
RewriteBase /
RewriteCond %{REQUEST_METHOD} ^(HEAD|TRACE|DELETE|TRACK) [NC]
RewriteRule ^(.*)$ - [F,L]
RewriteCond %{QUERY_STRING} ../ [NC,OR]
RewriteCond %{QUERY_STRING} boot.ini [NC,OR]
RewriteCond %{QUERY_STRING} tag= [NC,OR]
RewriteCond %{QUERY_STRING} ftp:  [NC,OR]
RewriteCond %{QUERY_STRING} http:  [NC,OR]
RewriteCond %{QUERY_STRING} https:  [NC,OR]
RewriteCond %{QUERY_STRING} (<|%3C).*script.*(>|%3E) [NC,OR]
RewriteCond %{QUERY_STRING} mosConfig_[a-zA-Z_]{1,21}(=|%3D) [NC,OR]
RewriteCond %{QUERY_STRING} base64_encode.*(.*) [NC,OR]
RewriteCond %{QUERY_STRING} ^.*([|]|(|)|<|>|ê|"|;|?|*|=$).* [NC,OR]
RewriteCond %{QUERY_STRING} ^.*("|'|<|>||{||).* [NC,OR]
RewriteCond %{QUERY_STRING} ^.*(%24&x).* [NC,OR]
RewriteCond %{QUERY_STRING} ^.*(%0|%A|%B|%C|%D|%E|%F|127.0).* [NC,OR]
RewriteCond %{QUERY_STRING} ^.*(globals|encode|localhost|loopback).* [NC,OR]
RewriteCond %{QUERY_STRING} ^.*(request|select|insert|union|declare).* [NC]
RewriteCond %{HTTP_COOKIE} !^.*wordpress_logged_in_.*$
RewriteRule ^(.*)$ - [F,L]
</IfModule>
```

28. Clean out Old Unneeded Core Files

Clean out old unneeded core files with help from this free Wordpress plugin:

http://wordpress.org/extend/plugins/old-core-files/

29. Activate Akismet Plugin

To block the comment spam automatically using Akismet Which a Wordpress plugin.

30. **Monitoring Your Wordpress**

http://wordpress.org/extend/plugins/wordpress-file-monitor-plus/

31. **Hide Your Login Page**

http://wordpress.org/extend/plugins/hide-login/

32. **Content Security**

Try checking http://copyscape.com/

33. **Check for Exploits**

http://wordpress.org/extend/plugins/exploit-scanner/

34. **Select Email Address as Your Login Key**

http://wordpress.org/extend/plugins/wp-email-login/

35. **Change Database Prefix Plugin**

http://wordpress.org/extend/plugins/db-prefix-change/

36. **Keep a log of Wordpress PHP and Database Errors**

http://wordpress.org/extend/plugins/error-log-monitor/

37. **Outstanding Security Plugin**

http://wordpress.org/extend/plugins/login-dongle/

http://wordpress.org/extend/plugins/better-wp-security/

http://wordpress.org/extend/plugins/wordfence/

38. **Website Defender Plugin**

http://wordpress.org/extend/plugins/websitedefender-wordpress-security/

39. **Maintenance Mode Plugin**

http://wordpress.org/extend/plugins/maintenance-mode/

40. **Admin Access from your IP Only**

You can limit who can access your admin folder by IP address, to do this you would need to create a new **.htaccess** file in your text editor and upload to your wp-admin folder.

```
order deny,allow
allow from 202.090.21.1 (replace with your IP address)
deny from all
```

41. Banning Bad Users

You can ban this person using .htaccess with this simple snippet:

```
<Limit GET POST>
order allow,deny
deny from 202.090.21.1
allow from all
</Limit>
```

42. Prevent Access to Wp-content

Create a custom **.htaccess** file in wp-content directory

```
Order deny,allow
Deny from all
<Files ~ ".(xml|css|jpe?g|png|gif|js)$">
Allow from all
</Files>
```

43. Individual File Protection

There are certain files you might want to protect individually rather than blocking a whole folder or selection. The example snippet shows how you would prevent access to the **.htaccess file** and will throw a 403 if accessed by anyone. The file name can be changed to whatever file you wish to protect:

```
# Protect the .htaccess
<files .htaccess="">
order allow,deny
deny from all
</files>
```

44. Disable Hotlinking

Sometimes another site may directly link images from your site. It saves hard disk space by not having to store the images. But your site ends up serving the requests for them, thus using up your precious bandwidth. This is known as **'hotlinking'**. To disable this you can add these lines to the .htaccess

```
#disable hotlinking of images with forbidden or custom image option
RewriteEngine on
RewriteCond %{HTTP_REFERER} !^$
RewriteCond %{HTTP_REFERER} !^http://(www\.)?yourdomain.com/.*$ [NC]
```

```
#RewriteRule \.(gif|jpg)$ – [F]
RewriteRule \.(gif|jpg)$ http://www.yourdomain.com/stealingisbad.gif [R,L]
```

45. Stop Spammers

Like hotlinking, spammers are notorious to use up your site's resources. There are a number of ways to identify a potential spammer. One of them is to detect requests with 'no referrer'. Spammers use bots to post comments on blogs and they come from 'nowhere'. Add these lines to stop the spammers

```
RewriteEngine On
RewriteCond %{REQUEST_METHOD} POST
RewriteCond %{REQUEST_URI} .wp-comments-post\.php*
RewriteCond %{HTTP_REFERER} !.*yourblog.com.* [OR]
RewriteCond %{HTTP_USER_AGENT} ^$
RewriteRule (.*) ^http://%{REMOTE_ADDR}/$ [R=301,L]
```

46. Database Optimization

http://wordpress.org/extend/plugins/wp-optimize/

FOR MORE INFO - >

http://www.hongkiat.com/blog/hardening-wordpress-security/

Wordpress Security Basics Checklist

1. Rename user Admin to something else.
2. Change the ID field on the first user from 1 to something else.
3. Enforce strong password requirements for all system users
4. Don't let anybody but admins see available WP updates.
5. Remove the ability for non-admins to modify theme files.
6. Tweak the database so tables aren't prefixed with wp_.
7. Don't use the MySQL root user to access the database.
8. Limit the MySQL account used to the site database only.
9. Restrict the MySQL account so it can't perform destructive actions (i.e. DROP, etc.)
10. Give the MySQL account a very long, randomised password.
11. Don't allow the server's root user access via SSH. Use an account with SUDO privileges instead.
12. Ensure all the secret key fields in wp-config.php are completed with 16-bit SHA keys.
13. Disallow indexes on all site folders.
14. Hide the admin area.
15. Rename the wp-content directory to something else.
16. Block bad hosts and agents with blacklists.
17. Make any .htaccess files and wp-config.php non-writeable.
18. Make the admin area inaccessible outside of work hours (handle this one with care)
19. Schedule regular database backups.
20. Restrict the length of allowed URLs to 255 characters or less.
21. Require SSL connections on the admin area (if possible; this one has an on-cost attached)
22. If possible, install and run server-side antivirus software such as ClamAV.
23. Consider restricting the server's FTP service to only accept connections from certain, whitelisted IP addresses (only applicable if you have at least one static IP).
24. When deploy complete, consider stopping the server's FTP service completely. You can always temporarily switch it on again if required.
25. If your web server is allowing proxying (for example, if you're load-balancing), ensure it's not configured as an open HTTP proxy.
26. Remove any open SMTP proxies on your server.