WordPress: Developing Secure Sites:

Back up Your site:

Keeping Backups of your site is most important thing. It's like life insurance of your site. There are many plugins to keep backups but most popular is **UpdraftPlus.** After installation and activation, configure it. go to settings and chose settings according to your requirement.

Restore Your Site:

1) Get the most current version of your backup files and database.

2) Set up a temporary maintenance page.

3) Upload new files.

4) Restore database.

5) Test thoroughly.

6) Remove the temporary maintenance page.

Open the web server php my admin. Keep your ftp client ready. Set up the maintenance page so that restoration is done without any interruption. To set it up, copy this code:

TEMP MAINTENANCE PAGE

<IfModule mod_rewrite.c>

RewriteEngine On

RewriteCond %{REMOTE_ADDR} !^000.000.000.000$ //here put your own //Ip. You can searvh on google about your Ip.

RewriteRule .* - [R=503,L]

</IfModule>

ErrorDocument 503 "<h1>The site is getting an update</h1> Back in 30 minutes!

<IfModule mod_headers.c>

3600 = 60 minutes

86400 = 1 day

Header always set Retry-After "86400"

</IfModule>

And put it in your site .htaccess file.

Upload this file and we are ready to go.

Now visitors will get “We will be back message”.

Now in the web server, you will see only cgi-bin folder and .htaccess file. Its like a clean slate and you are ready to update it with backup. Select all files in web server, right click and choose upload. Files will be uploaded from your backup through ftp client.

Now **update the database** in php my admin. Ist step is check all files and drop them.

Now click on import tab and locate your database and upload it.

Keep your site up to date:

WordPress core files, plugins, themes should be latest. you can get an update notifier plugin for your site which will notify you through email for an update.

Choose strong passwords. There are tools available to generate strong passwords. Change passwords frequently.

Choose trusted plugins and themes.

Choose plugins that are hosted in the Wordpress Plugin Directory.

Check out the plugins ratings and reviews.

Check out are they actively developing or not.

Check plugins description and installation steps.

Remove unused plugins, files, folders and themes.

Go to plugins and remove/delete unused, inactivated plugins.

Copy the .htaccess code file data and pate it in webserver .htaccess file above everything, will make website more secure and user would not be able to read readme files etc.

Wordpress allows admins to directly make changes to thmes, which is useful but can be risky as any admin can make changes. To disable editing directly in wordpress admin panel in wp-config.php file add this line.

define(`DISALLOW_FILE_EDIT`, true);

Just above the comment which says /*that's all, stop editing, happy blogging*/

Now there will be no option of edit theme or plugin directly in dash board.

New user Default role must be subscriber.

Wp-config file contains all the sensitive information like passwords etc so its necessary to keep it safe. There are 2 methods to keep it safe

1) **Restricting access via .htaccess file**

Copy this code

```
# PROTECT WP-CONFIG
<Files wp-config.php>

  # Apache < 2.3
  <IfModule !mod_authz_core.c>
    Order allow,deny
    Deny from all
```

```
    Satisfy All
  </IfModule>

  # Apache >= 2.3
  <IfModule mod_authz_core.c>
    Require all denied
  </IfModule>

</Files>
```

And paste it in root director of your .htaccess file. Add the code any where before wordpress rules are mentioned. If your site don't have .htaccess file make one. upload it.

Now if you try to open the wp-config file in the browser. It would say you don't have permission to do so.

2) R**estricting access via file permissions.**

You can give permissions through web server. check the permission number in front of .htaccess file in file manager. If it is 644 it means it allows access to wordpress file but deny access to all outside files. May be on your server this number is encrypted then you can go to online converter and decrypt it e.g www.onlineconversion.com/html_chmod_calculator.htmand check the code number by checking diff options.

Configure authentication keys:

In wp-config file, there are authentication keys. freshly installed wordpress does not show keys. To generate them go to the link mentioned in wordpress wp-config file above key area, generate keys and paste them

in define key area (remove all the built-in key code and paste the new generated one) . Just save the file now wordpress will save all your data super secure.

Customize the database prefix:

Wordpress database prefix is always wp_ , which is on risk of spams and hackers, you can change this prefix to something unique. to change it, during installation process, before submitting the installation page, open wp-config file and scroll to the line which says:

$table_prefix = 'wp_';

Change this to another thing.

Begin this prefix with wp_

Then put any random alpha numeric characters like s3CUr3

End with _

e.g wp_s3CUr3_

Then continue with the installation process.

This increase security immensely.

Set proper file permission:

Wordpress file permission default number is 644 and for directories it is 755. You can check it on web server. Alternatively, you can install

File Permission & Size Check plugin. You can then go to tools and then Run file Check and check the file number. After checking you should delete that plugin.

Prevent Directory Listing

Many web host disable directory listing by default as it is the first think attackers see before destroying your site. make sure it is disable.

Copy this code

DISABLE DIRECTORY VIEWS

Options –Indexes

And paste it in your .htaccess file in web server.

Now your directories will not be visible in browser

e.g yoursiteaddress/directory/

No directory listing will appear now.

You can put an index.html file in your directory folder of web server

Like this

```
<!DOCTYPE html>
<html>
  <head>
    <meta charset="UTF-8">
    <title>No Access</title>
  </head>
  <body>
    <h1>Directory Views Disabled!</h1>
  </body>
</html>
```

Now if anyone would try to see your directory listing in browser, he will get message, like that:

“Directory Views Disabled”

Remove version number:

Exposing Version numbers can be risky and hackers can attack your site. Version members are exposed by default in WordPress. To disable them open functions.php file

Copy the below code:

```
// remove version from head
remove_action('wp_head', 'wp_generator');

// remove version from rss
add_filter('the_generator', '__return_empty_string');

// remove version from scripts and styles
function shapeSpace_remove_version_scripts_styles($src) {
   if (strpos($src, 'ver=')) {
      $src = remove_query_arg('ver', $src);
   }
   return $src;
}
add_filter('style_loader_src',
'shapeSpace_remove_version_scripts_styles', 9999);
add_filter('script_loader_src',
'shapeSpace_remove_version_scripts_styles', 9999);
```

And paste it in the end of functions.php file.

Now version numbers will not be displayed.

Disable Error code:

If errors are displayed in browsers to public, its risk to security.

Open the wp-config file and scroll down to this line

Define('wp_debug', true);

Define('wp_debug_log', true);

Define('wp_debug_display', true);

Just make these true values to false.

Fight Comment Spam:

Install a plugin to fight through spam messages. Antispam Bee is a good plugin for that purpose. Through this plugin, you can even block some countries or specific languages to comment on your site.

Secure your Login Page:

You can secure your login page by limiting login attempts through a plugin. **Cyber limit login attempts** is a great plugin.

Stop User Enumeration:

User enumeration is a term when hackers can know your user id.

They can know the real user ids by writing siteurl/author/user-6

Or siteurl/?author=1

They would be able to see your registered real user ids so one way to avoid this is in dashboard go to users and edit user names with something different. it will not display in page but hackers can still see in url so to stop it install a plugin. One great one is "**Stop User Enumeration".**

Monitor admin users:

"activity log" is a great plugin to monitor user activities.

Implement a firewall:

BBQ is a good plugin to block bad queries. Hackers are in search of weak points through automated scripts.

Block Access:

WP-ban is a great plugin. It can ban on basis of IP address or user agents etc. You can get IP n user agent from webserver. In plugin setting block it.

Monitoring File Change:

Website File Changes Monitor is a great plugin for this purpose. It will detect new changes in any file.

Stop file hotlinking:

Hotlinking means when someone use your content e.g image etc without your permission. To stop that use this code:

```
# STOP HOTLINKING (METHOD 1)
<IfModule mod_rewrite.c>
   RewriteCond %{HTTP_REFERER} !^$
   RewriteCond %{HTTP_REFERER} !^http(s)?://([^.]+\.)?example\.com [NC]
   RewriteRule \.(gif|jpe?g?|png)$ - [NC,F,L]
</IfModule>
# STOP HOTLINKING (METHOD 2)
<IfModule mod_rewrite.c>
   RewriteCond %{HTTP_REFERER} !^$
   RewriteCond %{HTTP_REFERER} !^http(s)?://([^.]+\.)?example\.com [NC]
   RewriteCond %{REQUEST_FILENAME} !hotlink.gif [NC]
   RewriteRule \.(gif|jpe?g?|png)$ /hotlink.gif [NC,R,L]
</IfModule>
```

And paste it before any wp rules are mentioned in your .htaccess file.

Before posting change example.com to ur site url and .com to your top level domain. Replace hotlink.gif with ur image name.

Protect the installation page:

Go to wp-admin directory and open the install.php file. There are three methods to remove it after installation.

Method 1: delete file after installing wordpress.

Go to your webserver and rename this file with install_backup. And delete the origional.

Method 2: deny access via your site's .htaccess file

This method is more reliable. Copy the blank.htaccess.zip folder and paste it into wp-admin directory. next copy this code:

```
# SECURE INSTALL PAGE
<Files install.php>

  # Apache < 2.3
  <IfModule !mod_authz_core.c>
    Order allow,deny
    Deny from all
    Satisfy All
  </IfModule>

  # Apache >= 2.3
  <IfModule mod_authz_core.c>
```

```
    Require all denied
  </IfModule>

</Files>
```

And put it in .htaccess file on webserver.

Method 3: replace the file with something more useful.

Rename install.php with intall_backup and put in wp-admin directory.

Replace the install code with this code:

```
<?php
  /*
    WordPress install.php replacement page
    @ https://perishablepress.com/important-security-fix-for-wordpress/

    Place in /wp-admin/ directory
  */

  header('HTTP/1.1 503 Service Temporarily Unavailable');
  header('Status: 503 Service Temporarily Unavailable');
  header('Retry-After: 3600'); // 3600 seconds = 60 minutes

  mail('your-email@example.com', 'Database Error', 'There is a problem with the database!');
```

```
?>
<!DOCTYPE html>
<html>
  <head>
    <meta charset="UTF-8">
    <title>Site offline for maintenance</title>
  </head>
  <body>
    <h1>We'll be right back..</h1>
    <p>The site is currently offline for maintenance.</p>
  </body>
</html>
```

Paste all this code in installation .php , customize email address to urs.

Stop automated spam:

```
# BLOCK SPAM
<IfModule mod_rewrite.c>
  RewriteEngine On
  RewriteCond %{REQUEST_METHOD} POST
  RewriteCond %{HTTP_USER_AGENT} ^$ [OR]
  RewriteCond %{HTTP_REFERER} !example.com [NC]
  RewriteCond %{REQUEST_URI} /wp-comments-post\.php [NC]
  RewriteRule .* - [F,L]
</IfModule>
```

Copy this code and put in .htaccess file.

Change website to yours instead of example.com

Detect and block bad bots:

Paste this code in .htaccess file of your web server.

 # BLOCK BAD BOTS

<IfModule mod_rewrite.c>

RewriteCond %{HTTP_USER_AGENT}
(360Spider|acapbot|acoonbot|alexibot|asterias|attackbot|backdorbot|becomebot|binlar|blackwidow|blekkobot|blexbot|blowfish|bullseye|bunnys|butterfly|careerbot|casper|checkpriv|cheesebot|cherrypick|chinaclaw|choppy|clshttp|cmsworld|copernic|copyrightcheck|cosmos|crescent|cy_cho|datacha|demon|diavol|discobot|dittospyder|dotbot|dotnetdotcom|dumbot|emailcollector|emailsiphon|emailwolf|extract|eyenetie|feedfinder|flaming|flashget|flicky|foobot|g00g1e|getright|gigabot|go-ahead-
got|gozilla|grabnet|grafula|harvest|heritrix|httrack|icarus6j|jetbot|jetcar|jikespider|kmccrew|leechftp|libweb|linkextractor|linkscan|linkwalker|loader|miner|majestic|mechanize|morfeus|moveoverbot|netmechanic|netspider|nicerspro|nikto|ninja|nutch|octopus|pagegrabber|planetwork|postrank|proximic|purebot|pycurl|python|queryn|queryseeker|radian6|radiation|realdownload|rogerbot|scooter|seekerspider|semalt|siclab|sindice|sistrix|sitebot|siteexplorer|sitesnagger|skygrid|smartdownload|snoopy|sosospider|spankbot|spbot|sqlmap|stackrambler|stripper|sucker|surftbot|sux0r|suzukacz|suzuran|takeout|teleport|telesoft|true_robots|turingos|turnit|vampire|vikspider|voideye|webleacher|

webreaper|webstripper|webvac|webviewer|webwhacker|winhttp|wwwoffle|woxbot|xaldon|xxxyy|yamanalab|yioopbot|youda|zeus|zmeu|zune|zyborg) [NC]

RewriteRule .* - [F,L]

</IfModule>

Firewall your site:

Paste this in .htcacces file before wordpress rules

```
# 6G FIREWALL/BLACKLIST
# @ https://perishablepress.com/6g/

# 6G:[QUERY STRINGS]
<IfModule mod_rewrite.c>
  RewriteEngine On
  RewriteCond %{QUERY_STRING} (eval\() [NC,OR]
  RewriteCond %{QUERY_STRING} (127\.0\.0\.1) [NC,OR]
  RewriteCond %{QUERY_STRING} ([a-z0-9]{2000}) [NC,OR]
  RewriteCond %{QUERY_STRING} (javascript:)(.*)(;) [NC,OR]
  RewriteCond %{QUERY_STRING} (base64_encode)(.*)(\() [NC,OR]
  RewriteCond %{QUERY_STRING} (GLOBALS|REQUEST)(=|\[|%) [NC,OR]
  RewriteCond %{QUERY_STRING} (<|%3C)(.*)script(.*)(>|%3) [NC,OR]
  RewriteCond %{QUERY_STRING} (\\|\.\.\.|\.\./|~|`|<|>|\|) [NC,OR]
```

```
  RewriteCond %{QUERY_STRING} (boot\.ini|etc/passwd|self/environ) [NC,OR]
  RewriteCond %{QUERY_STRING} (thumbs?(_editor|open)?|tim(thumb)?)\.php [NC,OR]
  RewriteCond %{QUERY_STRING} (\'|\")(.*)(drop|insert|md5|select|union) [NC]
  RewriteRule .* - [F]
</IfModule>

# 6G:[REQUEST METHOD]
<IfModule mod_rewrite.c>
  RewriteCond %{REQUEST_METHOD} ^(connect|debug|delete|move|put|trace|track) [NC]
  RewriteRule .* - [F]
</IfModule>

# 6G:[REFERRERS]
<IfModule mod_rewrite.c>
  RewriteCond %{HTTP_REFERER} ([a-z0-9]{2000}) [NC,OR]
  RewriteCond %{HTTP_REFERER} (semalt.com|todaperfeita) [NC]
  RewriteRule .* - [F]
</IfModule>

# 6G:[REQUEST STRINGS]
```

```
<IfModule mod_alias.c>
  RedirectMatch 403 (?i)([a-z0-9]{2000})
  RedirectMatch 403 (?i)(https?|ftp|php):/
  RedirectMatch 403 (?i)(base64_encode)(.*)(\()
  RedirectMatch 403 (?i)(=\\\'|=\\%27|/\\\'/?)\.
  RedirectMatch 403 (?i)/(\$(\&)?|\*|\"|\.|,|&|&amp;?)/?$
  RedirectMatch 403 (?i)(\{0\}|\(/\(|\.\.\.|\+\+\+|\\\"\\\")
  RedirectMatch 403 (?i)(~|`|<|>|:|;|,|%|\\|\s|\{|\}|\[|\]|\|)
  RedirectMatch 403 (?i)/(=|\$&|_mm|cgi-|etc/passwd|muieblack)
  RedirectMatch 403
(?i)(&pws=0|_vti_|\(null\)|\{\$itemURL\}|echo(.*)kae|etc/passwd|eval\(|self/
environ)
  RedirectMatch 403
(?i)\.(aspx?|bash|bak?|cfg|cgi|dll|exe|git|hg|ini|jsp|log|mdb|out|sql|svn|swp|
tar|rar|rdf)$
  RedirectMatch 403 (?i)/(^$|(wp-
)?config|mobiquo|phpinfo|shell|sqlpatch|thumb|thumb_editor|thumbope
n|timthumb|webshell)\.php
</IfModule>

# 6G:[USER AGENTS]
<IfModule mod_setenvif.c>
  SetEnvIfNoCase User-Agent ([a-z0-9]{2000}) bad_bot
  SetEnvIfNoCase User-Agent
(archive.org|binlar|casper|checkpriv|choppy|clshttp|cmsworld|diavol|dotb
```

```
ot|extract|feedfinder|flicky|g00g1e|harvest|heritrix|httrack|kmccrew|loader
|miner|nikto|nutch|planetwork|postrank|purebot|pycurl|python|seekerspi
der|siclab|skygrid|sqlmap|sucker|turnit|vikspider|winhttp|xxxyy|youda|zm
eu|zune) bad_bot

   # Apache < 2.3
   <IfModule !mod_authz_core.c>
      Order Allow,Deny
      Allow from all
      Deny from env=bad_bot
   </IfModule>

   # Apache >= 2.3
   <IfModule mod_authz_core.c>
      <RequireAll>
         Require all Granted
         Require not env bad_bot
      </RequireAll>
   </IfModule>
</IfModule>

# 6G:[BAD IPS]
<Limit GET HEAD OPTIONS POST PUT>
   Order Allow,Deny
```

```
    Allow from All
    # uncomment/edit/repeat next line to block IPs
    # Deny from 123.456.789
</Limit>
```

Control Proxy access:

First Method:

Copy the wpninja 5.06 htaccess-code.txt.

Paste this code in .htaccess file on web server.

Second Method:

Copy this code in the end of function.php file.

```
// block proxy visits @ http://m0n.co/01
function shapeSpace_block_proxy_visits() {
    if (@fsockopen($_SERVER['REMOTE_ADDR'], 80, $errstr, $errno, 1)) {
        die('Proxy access not allowed');
    }
}
add_action('after_setup_theme', 'shapeSpace_block_proxy_visits');
```

Control Admin Access:

Copy this code:

```
# SECURE WP-ADMIN
<FilesMatch ".*">

    # Apache < 2.3
```

```
  <IfModule !mod_authz_core.c>
    Order Deny,Allow
    Deny from all
    Allow from 123.456.789.000
  </IfModule>

  # Apache >= 2.3
  <IfModule mod_authz_core.c>
    Require ip 123.123.123.000
  </IfModule>

</FilesMatch>
```

And put it in .htaccess file. If you don't have any .htaccess file(in wp-admin directory), create one. Then paste this above code. Change IP address to your own. YOur Ip addess can be found on google just search what is my IP? Upload file in server.

Also to put more security to login page, which is wp-login page in root directory. Go to .htaccess file of root directory. If it does not have any create 1 and then paste this code:

```
# SECURE LOGIN PAGE
<Files wp-login.php>

  # Apache < 2.3
  <IfModule !mod_authz_core.c>
    Order Deny,Allow
```

```
    Deny from all
    Allow from 123.123.123.000
  </IfModule>

  # Apache >= 2.3
  <IfModule mod_authz_core.c>
    Require ip 123.123.123.000
  </IfModule>

</Files>
```

Don’t forget to change IP addresses to your own.

Find and report vulnerabilities:

In wordpress dash board, you can go to tools and check your site health.

Never check anyone can register option in settings.

Display name should not be same as user name.

Limit the number of admins.

Check all the .htaccess files.

Choose a good host.

Further security techniques

- **Monitor errors.**
- **Respond to incidents**
- **Don’t modify core files**
- **Work with a clean computer**
- **Use https**

- **Use sftps**
- **Write secure code**
- **Explore plugins.**