

NOTICE: You Do NOT Have the Right
to Reprint or Resell this Report!

You Also MAY NOT Give it Away,
Sell or Share the Content Herein.

If you obtained this report from anywhere other than the Warrior Forum you have a pirated copy.





ADVANCED Security Training



Published By:
PageOneTraffic Ltd.



Copyright © 2013 – PageOneTraffic Ltd. All Rights Reserved

No part of this consumer report may be reproduced or transmitted in any form without the written permission of the author.

Disclaimer

This report has been diligently researched and compiled with the intent to provide information for those wishing to learn about Wordpress security.

Throughout the making of this consumer report, every effort has been made to ensure the highest amount of accuracy and effectiveness for the techniques suggested by the author. The report may contain contextual, as well as, typographical mistakes.

No information provided in this report constitutes a warranty of any kind; nor shall readers of this report rely solely on any such information or advice. All content, products, and services are not to be considered as legal, medical, or professional advice and are to be used for personal use and information purposes only.

This report makes no warranties or guarantees express or implied, as to the results provided by the strategies, techniques, and advice presented in this report. The publishers of this report expressly disclaim any liability arising from any strategies, techniques, and advice presented in this report.

The purpose of this consumer report is to educate and guide. Neither the publisher nor the author warrant that the information contained within this consumer report is free of omissions or errors and is fully complete. Furthermore, neither the publisher nor the author shall have responsibility or liability to any entity or person as a result of any damage or loss alleged to be caused or caused indirectly or directly by this report.

Even if all steps mentioned are followed correctly and exactly as specified and stipulated in this guide and the accompanying videos, it is reasonable to assume that there is inherent risk in anything to do related to the topic covered.

You are advised to do your own due diligence before following any of the tasks mentioned in the guide and take proper precautions, such as: implementing recovery measures and creating backups before trying anything from this guide.

Introduction

This is a bonus training and is intended for those that have prior experience with Wordpress and have some understanding of coding. It is not recommended for a newbie. However, the material is easy to follow and laid out in a step-by-step format. If you are interested in trying the information I highly recommend that you back up your website before doing so.

Even for the advanced user I recommend that you always back up your site whenever making any changes to the code. If you want to sell this service to your clients go through the steps a few times on your own website. Once you feel comfortable in what you are doing continue to use this document as a checklist and code swipe file.

I have not expanded on some things as I am assuming that you have some familiarity with Wordpress. If not, inside of cpanel there are usually video tutorials that you can refer to. Use those instead of YouTube videos to ensure accuracy.

Module 1: Before You Begin

On your current installation of Wordpress, make sure all your settings are up-to-date. Ensure all plugins are updated to the most recent versions.

Note: Even official WP updates and plugin updates CAN break your WP site. It is highly recommended that you create a backup solution to your website.

I thought I would mention this.

One of the fastest and easiest ways to backup Wordpress is a really good tool called wptwin. At first glance the \$97 price tag seems a little high, but the amount of time and effort it saves you is worth way more than what it costs.

You can learn more about it by [clicking here](#)

Let's begin...

1. Update to the latest version of Wordpress and plugins (you can do this from within Wordpress).
2. Perform a server backup of the home directory and the database (do NOT use full backup from cPanel).

- a. Create a folder on your machine to keep the backup files
- b. Login to WHM/cPanel
- c. Locate the Files section
- d. Choose "Backups"
- e. Click on the Home Directory button and download the backup to a safe place - the directory on your machine.
- f. Click on the name of the database that you have your Wordpress tables in and download the backup to the same directory.

3. Perform a Wordpress backup

- a. Login to Wordpress using an administrator account
- b. Navigate to the tools section
- c. Click on Export and download the file

Module 2: Initiate File Security

1. Move wp-config.php file up one level into your home from public_html (or wwwroot)

The wp-config.php file contains the name of your database and database password. Wordpress allows you to move this up one level from your wwwroot to your home.

Substitute username for your actual username given to you by your host.

wwwroot (or public_html) -> **/home/username/public_html** <- Publicly accessible
Your home directory -> **/home/username/** <- Not publicly accessible

You can use the unix/linux mv (Move) command if your are familiar with the command line and have shell access.

mv /home/username/public_html/wp-config.php /home/username/wp-config.php

If you don't have shell access, you can easily use the cPanel File Manager to move the file as shown in the video for this module.

2. Change wp-config.php file permissions to 600

You are changing the permissions to read/write permissions for you alone. The default 644 gives read permissions to the public, which is very dangerous. Nobody needs to read your wp-config file.

If you have shell access, you can use the chmod command

```
chmod 600 wp-config.php
```

If you don't have shell access, I've already shown you how to do this in the cPanel File Manager.

3. Delete readme.html, wp-admin/install.php and wp-admin/install-helper.php files

Once again, if you have shell access, you can use the rm command:

```
rm -f readme.html wp-admin/install*.php
```

Otherwise, navigate to the file using the cPanel File Manager and delete these files. The readme.html gives away your version number for Wordpress, which you should hide. The other two can potentially cause havoc.

Note: Whenever you upgrade Wordpress, always check if it dropped a new readme.html file and ensure that you delete it.

4. Create 0 byte index.php file in wp-content/uploads

If you are in the shell you can use the touch command to create the file.

```
touch wp-content/uploads/index.php
```

Make sure that the permissions are set to 755.

```
chmod 755 wp-content/uploads/index.php
```

If you create the file through cPanel File Manager, it will automatically add the 755 permissions to it.

5. Set .htaccess to 644 (or 664)

This may already be set as a default for a .htaccess - if not, you know the drill.

6. (Optional - BUT Recommended) - Set `expose_php=Off` in `php.ini`

This is an optional step that may not be possible for everyone to do. Ask your web hosting provider if they can provide a separate `php.ini` for your website.

If you have a dedicated server, cloud server or VPS, then you can and should implement this by logging into the shell as root and then running the following commands.

Keep in mind this is not really protecting you, but it is additional information you can hide, which helps your security. Every little thing that you hide makes it that much more difficult to hack your website.

From the shell you can use the `locate` or `find` command.

`locate php.ini`

To find the correct ini file.

`php -i | grep 'Configuration File'`

Go to the directory to look inside the file

`cat php.ini | grep expose_php`

If you find, `expose_php = On`, then it is advisable to use an editor to set it to `Off`.

7. Add secret keys to `wp-config.php` file

Visit <https://api.wordpress.org/secret-key/1.1/> to get your keys.

Refresh the page to change the keys.

If you used `fantastico` to install Wordpress, these keys would already have been set. You can still change them if you like.

Module 3: Initiate Database Security

Database security is a tricky issue. You can easily get into trouble by messing up your database (and databases are easier to corrupt than you think).

So be extra careful when you do anything with databases.

Make sure you have it backed up (take another backup as a secondary backup ... it's that important).

That said, the steps to follow are not really that hard, because it involves copying and pasting stuff.

1. Generate random prefix

One of the best places online is <http://random.org/passwords>

There are other password generators, but this is what I use. You can use any of them.

2. Generate SQL for db prefix

The following SQL statement will generate all the table name change statements in the database. By default the prefix is wp_. The SQL statement runs through the system tables and creates SQL query strings.

```
SELECT CONCAT('RENAME TABLE ',TABLE_NAME, ' TO <prefix>',  
SUBSTRING(TABLE_NAME,3),';') FROM INFORMATION_SCHEMA.TABLES WHERE  
TABLE_SCHEMA='<schema>';
```

Before you start, copy the above to a text file and replace <prefix> with your prefix. So if your prefix is zzzzz and Wordpress database is yyyy, your statement will be

```
SELECT CONCAT('RENAME TABLE ',TABLE_NAME, ' TO zzzzz',  
SUBSTRING(TABLE_NAME,3),';') FROM INFORMATION_SCHEMA.TABLES WHERE  
TABLE_SCHEMA='yyyy';
```

3. Prepare SQL statement and execute on DB

- a. Login to cPanel
- b. Find the Databases section
- c. Open PHPMyAdmin
- d. Select the information_schema database (these are MySQL system tables)
- e. Select the SQL tab
- f. Copy/Paste the SQL statement and click the Go button. This will generate the SQL statements
- g. Click on "Print View (with full texts).
- h. Copy the generated SQL statements.
- i. Now select the Wordpress database (not information_schema)
- j. Run the SQL statements

4. Run other update statements

If you have done the above correctly your database prefixes would have changed. Now there are 2 other updates you need to run to make sure everything is fine. Not running these 2 updates may cause errors in the admin backend with access permissions that are broken.

```
UPDATE `<prefix>_usermeta` SET `meta_key` = REPLACE(
`meta_key` , 'wp_', '<prefix>_');
```

```
UPDATE `<prefix>_options` SET `option_name` =
'<prefix>_user_roles' WHERE `option_name`
='wp_user_roles' AND `blog_id` =0;
```

Copy these to a text file.

Replace <prefix> with the same prefix you used above.

Each statement should have updates. If there are no updates, then there were typos.

5. Update db_prefix in wp-config.php file

After you finish this your Wordpress site will not be accessible, because Wordpress is still trying to access the old prefix. This is a fairly simple fix. Just edit your wp_config.php file.

Make sure that the line that says:

\$table_prefix = 'wp_'

Now this is updated with the correct prefix information.

After you run this step your site should load fine.

Congratulations: Even just after following these steps your site will already be much more secure than a majority of Wordpress blogs. But let's take it to the next level.

Module 4: Configure Blog Settings

1. Set Permalinks to /%postname%/ (ANYTHING other than the default)

This is very easy. Perhaps you have already set it. Login to Wordpress as an administrator. Go down to the Settings section and click on permalinks.

Set permalinks to /%postname%/ or anything else you wish (remember not to use any of the default settings).

2. Configure syndication settings (General/Reading)

Go to Settings -> Reading

Change the max pages to show = 3

Change the syndication feeds to show = 3

For each article in feed, show Summary.

You DON'T want your entire blog being syndicated. It is much better to have partial content in the feed that links to the entire article on the blog.

3. Create a new admin user (use randomized username and password). Don't display username!

We are going to create a new username that cannot be guessed. (NOTE THIS DOWN - if you forget the username, you may not be able to get back in).

- a. Go to a password generator like <http://www.random.org/password> and create a string
- b. Prefix initials to text file (optional) and copy this to a text file, which you will maintain
- c. Generate a password and add special characters
- d. Login as admin
- e. Go to Users and add new user.
- f. Copy/Paste username and password and make sure you select an e-mail that you want to use with this username. You must remember and have access to this e-mail.
- g. MAKE SURE you select administrator as the Role

4. Logout and Login as new user and change display name

Make sure you go back in and select the new user you just created from the User Panel and scroll down to display name. Change the display name to a real name (don't forget this step, otherwise the prior step will be wasted).

5. Delete user 'admin'

You want to delete the user admin. Go to your users tab and you can delete the user admin using the Delete link right under the username or you can click the checkbox and select delete from the drop down.

As soon as you click delete Wordpress will ask you if you want to move any existing content to another username.

If you have content, attribute all of this to the new user.

If this is a blank Wordpress install then you can safely remove this user and it will remove the default posts, pages and links.

6. Add functions to current themes functions.php file

This step is important again for hiding information. If you ever change your theme, you will lose these changes and will have to implement them again in the new theme files.

There are two functions - `add_filter` and `explain_less_login_issues` that you need to add to the `functions.php` file of your theme.

Go to the Appearance section within your admin panel and click on Editor. This gives you the capability to edit php theme files within Wordpress. We will be disabling this functionality shortly as well.

On the right side under Templates locate the functions.php file.

Select the functions.php file and it will load into the editor.

Go to the bottom of this file.

Copy the following function code:

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

function explain_less_login_issues(){
    return '<strong>ERROR</strong>: Entered credentials are
incorrect.';}
    add_filter( 'login_errors', 'explain_less_login_issues' );
```

Now, paste it after the last line in the functions. php file.

[Note: If the file ends with ?> then paste it just before ?>](#)

Click on Update File.

7. Create blockbadqueries plugin - Install, activate

This is a really nice piece of code contributed by Perishable Press. It prevents bad queries to your Wordpress installation and adds protection against SQL injection attacks.

To install this plugin, you will have to create a file in your plugins directory called blockbadqueries.php.

Use the cPanel File Manager to navigate to the wp-content/plugins directory and create the File and name it blockbadqueries.php.

Use the Code Editor to edit this file and copy the following code (as seen on the next page):

```
<?php
/*
Plugin Name: Block Bad Queries
Plugin URI: http://perishablepress.com/press/2009/12/22/protect-wordpress-against-malicious-url-requests/
Description: Protect Wordpress Against Malicious URL Requests
Author URI: http://perishablepress.com/
Author: Perishable Press
Version: 1.0
*/
if (strpos($_SERVER['REQUEST_URI'], "eval(") ||
    strpos($_SERVER['REQUEST_URI'], "CONCAT") ||
    strpos($_SERVER['REQUEST_URI'], "UNION+SELECT") ||
    strpos($_SERVER['REQUEST_URI'], "base64"))
{
    @header("HTTP/1.1 400 Bad Request");
    @header("Status: 400 Bad Request");
    @header("Connection: Close");
    @exit;
}
?>
```

Alternatively, you can just create a text file on your desktop called blockbadqueries.php and copy the above code and then ftp it to the wp-content/plugins directory.

From the Wordpress admin panel go to plugins and locate this new plugin. Click the activate link to activate this plugin.

8. Add switches to the wp-config.php file

Now we are going to disable the php editor within Wordpress. To do this go to your wp-config.php file and open it with an editor. I recommend using the Code Editor in cPanel File Manager, because it is easy.

Go to the bottom of the file and add the following line:

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

This will disable the php editor available for themes and plugins. Even an administrator cannot edit the php files from within Wordpress.

Note: Some themes may break on this step, especially if they have weird licensing requests. Try and ask the Theme author if you have an issue. If your theme does have an issue then you can comment this line or change the switch to false temporarily.

To prevent Wordpress from returning debug information, you need to turn off WP_DEBUG, which can be done by adding another line. See as follows:

```
define('WP_DEBUG', false);
```

Now, save the file.

9. Change the wp-config.php file permissions to 400

After you have done these steps you do not need to leave the wp-config.php file editable. It can be read-only. To make it read-only change the permissions to 400.

If you ever need to edit it, such as changing the prefix again or editing settings or changing the database password, then you can change it back to 600 temporarily. After you are done, change it back to 400 again.

This causes some plugins (even some popular ones) to break. No plugin should really need to write to this file. My advice is avoid the plugins that require you to give permissions to write to the wp-config.php file.

If you still need the functionality, change permissions of wp-config to 600, but no higher. You may want to monitor your wp-config timestamp from then onwards.

What is Next?

These are things you can move on to after the website is secure and after you have taken backups of your secured site.

1. If possible try and use https/ssl with wp-login to avoid sending a plain text password over the wire

It is possible to use an “unsigned” SSL certificate privately for free to go to your blog over https. Ask your host if you can do this and try and protect your wp-admin directory. An unsigned ssl certificate will make your browser give you a scary warning, but you don’t need to worry about that.

Alternatively, if you have a static IP, you can restrict login using a .htaccess file by adding a few lines.

```
<limit GET>
order deny,allow
deny from all
allow from your.ip.add.ress
</limit>
```

You can restrict a single file using the File directive.

```
<Files wp-login.php>
order deny,allow
deny from all
allow from your.ip.add.ress
</Files>
```

2. Change passwords frequently

This goes without saying! You should be changing passwords at least once every month. Most people let this slip. Don't be like them!

3. Monitor changes -> wp file monitor plugin

This is a really cool plugin that lets you know if there have been any changes to your files. After everything is ready, the only things that should change on your site is content.

This plugin sends you an e-mail if it detects any changes on the server. Can be very useful to being alerted that there is a possible intrusion. Sometimes people can go for weeks and months without even knowing that their site has been infected.

4. Work on Performance Optimization

You should try and work on optimizing your site both for user experience, as well as, search engine rankings. Here is a product I recommended -> <http://www.warriorforum.com/warrior-special-offers-forum/407036-google-says-faster-websites-rank-higher-how-supercharge-your-blogs-speed-step-step-bonus.html>

5. Work on SEO strategies

Most people give way too much credence to SEO. There is something good there, but remember to please your audience first. That said, there are some basic things that you can do to your website for SEO. Almost everyone who is reading should have a fairly decent idea.

Remember, a search engine is just ONE traffic source and even the so-called 800-pound Gorilla only controls about 6-7% of total internet traffic - even after controlling over 70% of search traffic.

6. Content Syndication - RSS, Social Media, etc.

Content syndication strategies, such as social bookmarking, RSS distribution, Social Media linking, etc. help the world know about your website and the information it has. Some of these locations can send you tons of targeted traffic even if you are not ranked high in the search engines for your terms. Here is another recommended product I think you will like ->

<http://www.warriorforum.com/warrior-special-offers-forum/424534-0-00-per-link-authority-sites-auto-pilot.html>

7. Track Your Results

I've been harping on this point for some time now regarding Google Analytics. Personally, I've been behind the scenes and have built analytics solutions for 15 years (the stuff Google Analytics produces looks like kid stuff). Besides, why would anyone ever give out their data to a 3rd party who may use it against them.

Sales pages have high bounce rates on purpose. On a sales page, I want people to either buy or go away. In my opinion that is one of the best user experiences ever. Fast decision making. Who is a 3rd party to judge how my users feel about their experience. It is rumored that Google uses

the bounce rates as a negative element to your rankings, which is their prerogative. You as a business should not be exposing your data to a 3rd party except where necessary.

There is a much better and much more powerful solution, which is free and open source pointed out by Markus Allen - who is a very well known marketer in his own right.

It's called TraceWatch and you can get it from www.tracewatch.com.

If you have all your sites on the same server, you can get by with a single TraceWatch installation.

Extra Chapter

Lastly, you need to know how to do this so...

Restoring Your Wordpress Install

In your backup folder, you will have 2 files:

1. The Home Directory Backup
2. The Database Backup

Here is a step-by-step restore process:

1. Login to cPanel
2. Navigate to Files -> Backups
3. In the database restore section upload the database backup file (hint: it will have an ending of .sql.gz).
4. When you load this, it will restore your database.
5. However, the restore DOES NOT restore your database user (you will need to create a database user).
6. Click on Databases -> MySQL databases
7. Create a new user and password (use the best practices used above).
8. After the user is created, go down to the "Add User To Databases" section, select the user you just created and the database you just restored.
9. It will automatically ask you what privileges you should grant. Select all and give this user all privileges.
10. Once, you have done this go back to Files -> Backups and restore your home directory by selecting the home directory backup file.
11. After you have done this, your site still will not work till you do one final step...
12. Edit the new MySQL username and password in your wp-config.php file.
13. Your site should be back now.

If you want a shortcut to this process, then [wp-twin](#) is a good solution, but to be honest with you this step-by-step process is more secure.

As always, thank you for trusting us to bring you the best products in the market. I really appreciate you and want you to be successful. If you like this course leave a comment in the thread.

Remember the goal is to get in the front door and this is an angle that nobody is using. Once you are in you can begin to sell all types of services. Here are some to consider: SEO, Web Design, Mobile, FaceBook, Social Media, and Reputation Management. [\(Tip: Use security as a twist to stand out even if you're selling FaceBook marketing\).](#)

Recommended Upgrade

Local Lead Boss Software & SecureSCAN Pro Plugin

