WordPress Security

&

Hardening Action Plan

- By WP Hacked Help

The 10-Point WP Hardening Checklist is going to help you level up your WordPress security. Over-the-shoulder, walk through tutorial that show you how to lock out 99.9% of all hack attempts on your WordPress site.

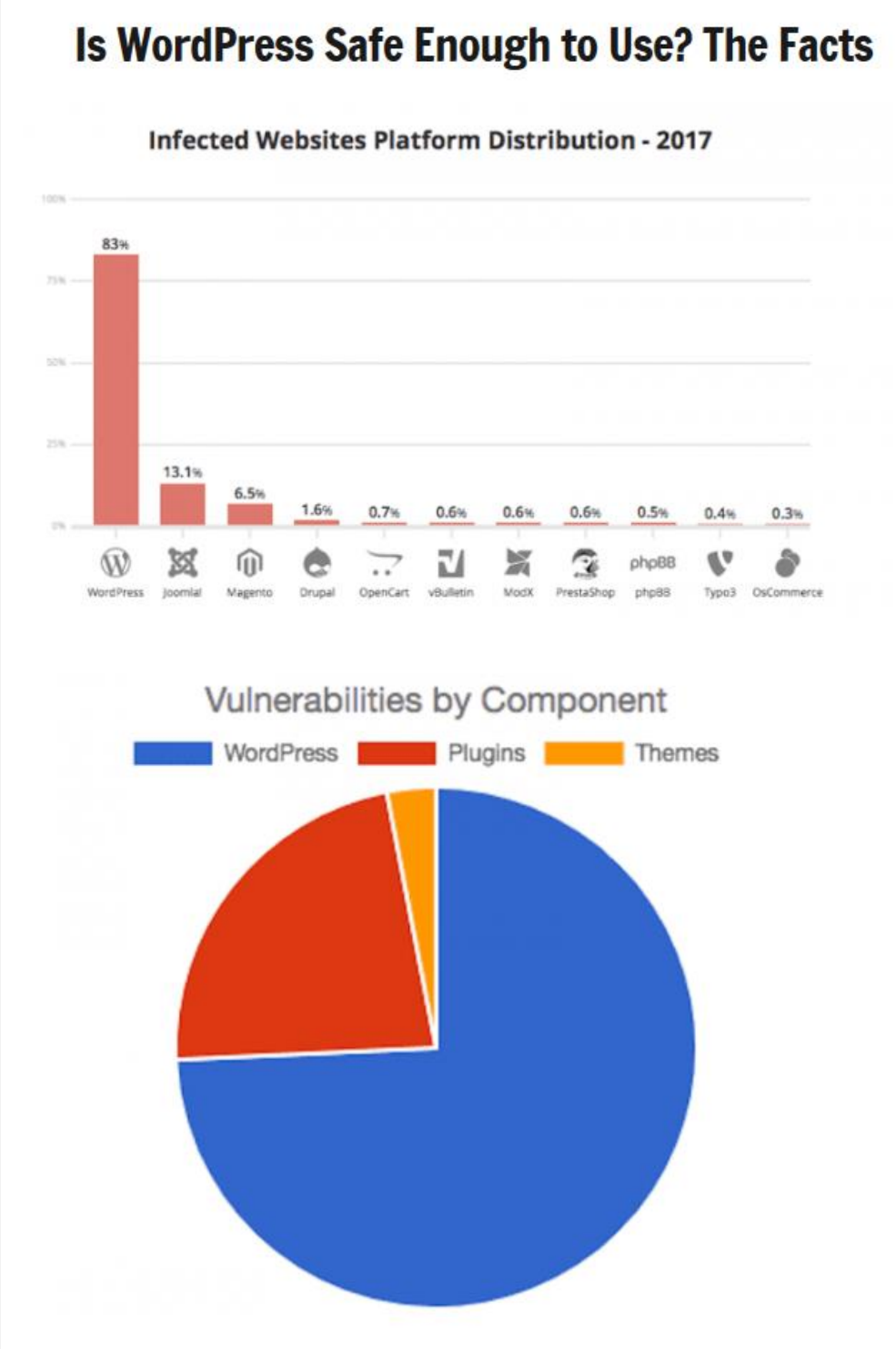
43% of Wordpress-attacks are aimed at small businesses sites. Every day 230,000 samples of malware are produced. There is a wordpress-attack after every 1 minute. The businesses have to pay a considerable cost for hacking and other cyber-crimes. A Juniper Research study has estimated that cybercrimes will cost businesses $2 trillion in 2019.

Hearing these statistics might give you the impression that WordPress is an inherently insecure platform. But your impression would be incorrect. WordPress is actually quite secure. The team at WP Hacked Help takes security very seriously and have a well-defined process for managing potential vulnerabilities.

Most of those hacks could have been prevented with some basic WordPress security tips and tricks.

The attacks that were more sophisticated could have been stopped with advanced WordPress security. And, let's face it, some of them could not have been stopped.

People have hacked into the Pentagon, the CIA, NASA and countless other 'secret' and 'secure' government agencies around the world.



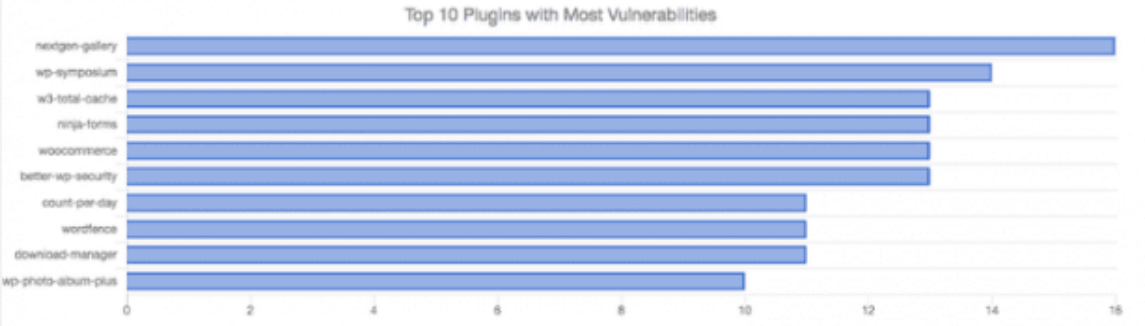
How Can Hackers Get into Your WordPress Site?

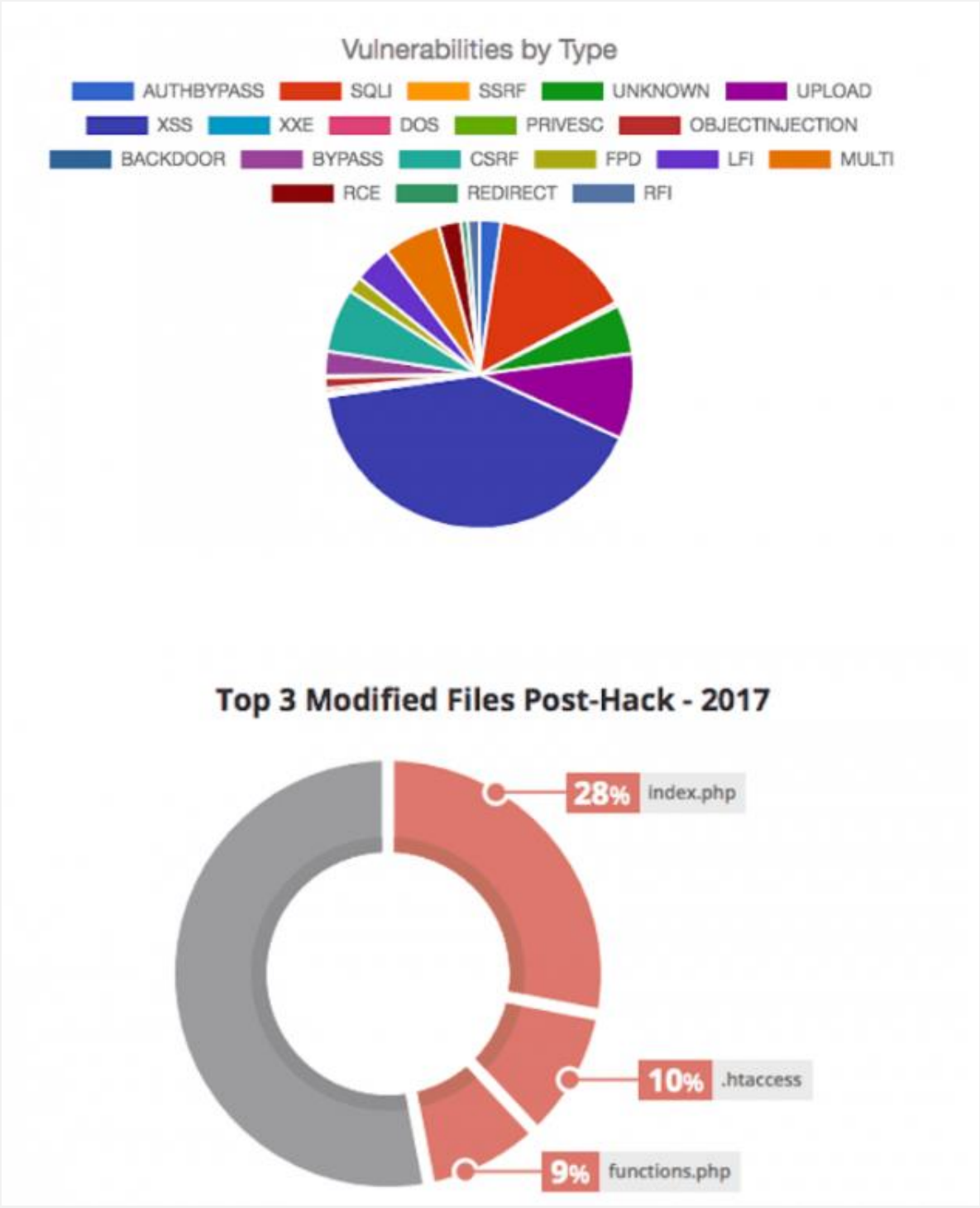
To the layperson, "spam" and "malware" may be the easiest ways to describe a WordPress security breach.

As a developer, you understand that hackers get much more creative than that. Because of the variety of ways in which they attack or infect a website and the location through which they're able to get inside, there are over a dozen types of WordPress threats you should be aware of.

Number of vulnerabilities detected in the latest core updates:

Plugins frequently been afflicted with security vulnerabilities:





- *SQL Injection*
- *Cross-site Scripting - **Wordpress XSS***
- *Forgery*
- *Phishing*
- *Remote File Inclusion*
- *File Upload*
- *Path Traversal*
- ***WordPress Malware Redirect***
- ***Brute Force Attack***
- *Distributed Denial of Service - **WordPress DDOS attack***

If a hacker REALLY wants to get into your site, they will probably find a way. Luckily, situations like that are few and far between until you become a major authority in the world.

When it comes to WordPress, the truth is, **your site just needs to be more secure than the average.** There are so many WordPress sites that are insecure that if a hacker encounters any sort of difficulty getting into your website they'll simply move on to the next one rather that bother hacking yours.

Again, you don't need to make your site unhackable, you just need to make it harder to hack than the others.

Remember the premise of the old joke: "I don't need to outrun the bear, I just need to outrun you." Same thing with hackers. You just need to be a little better prepared than the other websites.

On that note, let's start with some basic wordpress security tips for your site so that you can have some peace of mind.

Keep an eye on your site's performance

You should be checking your website's load speed at least once a week. A sudden slow down on your website can be an indicator that it's infected with malware or has been hacked.

Most brick-and-mortar business owners rarely check their websites, which means they could be down for an extended period without them knowing about it. So an uptime monitoring service can be important if you're in that boat.

Pingdom (https://www.pingdom.com/) is a great tool that can help you with both starting at $15 or less per month.

Install security plugins

Installing security plugins that monitor your site files is a smart move. There are two major ones that we use and recommend: WordFence and Sucuri.

WordFence does things like scan site files for changes on a regular schedule, limits login attempts with wrong usernames or passwords, keeps track of IP addresses that are using your website in suspicious ways. Some hosts don't like you using WordFence (particularly WP Engine) because that plugin can be a server resource hog. There is a free and premium version of this plugin.

Sucuri is a primo security plugin that scans your websites directly for malware. They also have a firewall that will filter out suspicious traffic before it even reaches your website. If you are infected with malware they'll also clean it up for you. They have a free and premium version, but all the cool stuff all comes with the paid version.

Scan Your WordPress site on regular basis.

Check and **scan WordPress for malware** detection using the best professional tools. Use multiple malware checkers: online site check tools as well as on-site malware scanners. Scan your site thoroughly by first identifying the malicious hacks on the site like Wordpress malware redirect. This scan helps in discovering and identifying the infected files.

Once you have done an indepth scan for malware in wordpress theme and identified the malicious files , remove these. Review WordPress front-end, back-end, source-code, file-system, themes, plugins, updates, configurations and settings to discover the source of attack.

You can use this Advanced Wordpress scanner by WP Hacked Help.

Their Deep Scanning **WordPress malware scanner** detects viruses and trojans hidden deep within the server and their WordPress experts **cleans it up**. It is important for you to know the security gaps and what exactly needs to be done to clean up your site. Read our indepth guide to remove malware from wordpress site.

Don't keep ZIP backups on your server

It is important that you backup your website and database regularly if you are regularly adding new content to your site. Some backup plugins will save the backups inside the WordPress directory. Bad move.

Hacking scripts can easily access those ZIP files and insert malware into them. Then, if for any reason you need restore your site, you'll be restoring a hacked version of your website.

That's why it's best to have the backups either emailed to you or stored in the cloud with Dropbox, Google Drive, Amazon S3 or another cloud service provider.

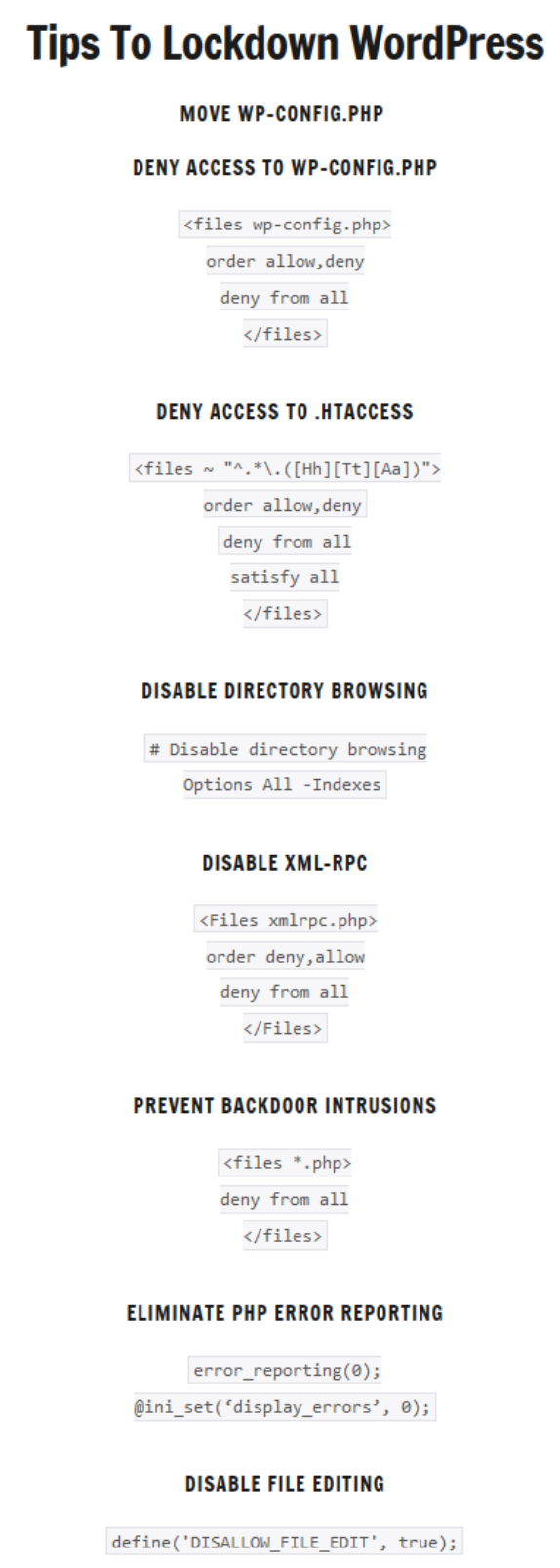
Delete the install.php and upgrade.php files

These two files allow special access to server resources and are only required for installation or upgrading your WordPress site. So you can delete them once your site is installed or updated.

These files may reappear after you update your WordPress core files, so you'll have to delete them after everyupdate.

Lockdown directory access

There are two directories within your WordPress folder hierarchy that **never** need to be accessed by the public: wp-admin and wp-includes. It is always a good idea to restrict access to these directories using your .htaccess file.



Tips To Lockdown WordPress

MOVE WP-CONFIG.PHP

DENY ACCESS TO WP-CONFIG.PHP

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

DENY ACCESS TO .HTACCESS

```
<files ~ "^.*\.([Hh][Tt][Aa])">
order allow,deny
deny from all
satisfy all
</files>
```

DISABLE DIRECTORY BROWSING

```
# Disable directory browsing
Options All -Indexes
```

DISABLE XML-RPC

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

PREVENT BACKDOOR INTRUSIONS

```
<files *.php>
deny from all
</files>
```

ELIMINATE PHP ERROR REPORTING

```
error_reporting(0);
@ini_set('display_errors', 0);
```

DISABLE FILE EDITING

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

Protect your wp-config.php file

The wp-config.php file is one of the most important files in your WordPress installation. If it's not protected it's relatively easy for to access for a hacker to access and see your database credentials. They can use those database credentials and the file itself to wreak all kinds of havoc on your website.

There are two main ways to protect it. The one you choose will depend on your hosting account. If your website is on an Apache server you can use the .htaccess file to protect your wp-config.php file.

The second option is only useful if you are using a dedicated host and you have access to folders above the root of your website. If you do, you can move the wp-config.php file out of the public folders to the folder above the root.

Block too many failed logins

Too many failed login attempts in a short amount of time is an indication that someone is trying to guess a username and password combination that will give them access to your site. This is called a Wordpress brute force attack.

You can block people that have failed to login a certain number of times using the Wordfence plugin and the Limit Login Attempts plugin (https://www.youtube.com/watch?v=s3z3eseY9E4).

Move the login page to a different URL

Brute force attacks are often carried out using automated tools. These tools look for the WordPress login page in the usual places: YourDomain.com/wp- login.php or YourDomain.com/wp-admin. If there's no login page there they have no choice but to move on. That's why moving the login page do a different URL is so handy.

There's a handy plugin called Move Login (https://en-ca.wordpress.org/plugins/sf-move-login/) that will help you do just that. You can choose the slug for the login page to be anything you want. Now when the automated tools scan WordPress sites for login pages to brute force, your site will be invisible.

Hide WordPress version

Every WordPress core update includes security patches. When an update is released information about the patches and the vulnerabilities they fix are published online. Hackers know that most people don't update their websites right away AND the hackers now know the exact vulnerabilities that exist in previous versions of WordPress. This is what we call 'low-hanging' fruit.

To make matters worse every WordPress site publishes the version number of the WordPress core files in the source code. Using automated tools hackers can scan your site, find the version number and attempt to hack in using the known Wordpress security vulnerabilities .

That is why it's so important to update your WordPress core files as soon as updates become available. It's also a good reason to remove the WordPress version number from your source code.

Remove/disguise login error messages

When you enter an incorrect username and password combination into a WordPress login page the error messages give you hints about what you got wrong.

For example, if you enter an incorrect username AND an incorrect password the error message says "Error: The username or password you entered is incorrect".

However, if you enter the correct username but an incorrect password the error messages says" Error: The password you entered is incorrect".

That's bad for business. If you're a hacker, you now know that you have a valid username and you just need to crack the password. For that reason it's much better to keep the first error message all the time, "Error: The username or password you entered is incorrect".

Conclusion

WordPress powers nearly 22% of all websites on the internet, which is huge and it means that the WordPress community will probably be around for a long time to come. It also means that WordPress is a huge target for hackers.

Unfortunately, most webmasters don't care or don't know that they should be securing their websites. Sooner or later they will be hacked and it will hurt their business. Even by just browsing through this document you are doing more than the vast majority of webmasters, so good work!

Now it's time to take this to the next level. I've created a step-by-step tutorial action plan to harden your website substantially more than most people are doing. By following this action plan you will no longer be 'low-hanging fruit'. Any would-be hackers will probably (not always) move on to another site that *is* low-hanging fruit and leave yours alone.

IMPORTANT:

If you are at all concerned about the security of your website, then you NEED to read this right now.

Why?

Because most people want to secure their website, but they're unsure of the exact steps, even with the above checklist in hand. Every day that goes by an unsecured site is more likely to be hacked.

That's why I created a special step-by-step WordPress security for beginners tutorial series detailing exactly how I secure every site that I'm responsible for quickly and easily.

It is very difficult to get all the correct answers by cruising YouTube, forums and websites, it's much easier when it's all distilled into an actionable set of tutorials:

That's exactly what the WP Security Action Plan is all about.

And if you act quickly, you can get this entire plan implemented on your site for just $99 . Contact us here to know more

If you're serious about hardening your WordPress site, then this is the first step.

Scan Your Website Now >>>

Ref's: Resources For Further Reading (InDepth)

Importance Of WordPress Security - Tips to secure your site in 2019

Ultimate WordPress Security Checklist 2019

Best wordpress malware-scanners in 2019

WordPress Troubleshooting Tips (Errors)

How To Fix WordPress Upload Failed To Write File To Disk Error?

Fix "Are You Sure You Want to Do This" & Logout Error in WordPress

How to Track (Monitor) User Activity in WordPress?

WordPress HTTP Image Upload Error

HTTP 503 Service Unavailable Error

WordPress Stuck in Maintenance Mode

Parse Error: Syntax Error Unexpected WordPress

"This Account Has Been Suspended"

WordPress Not Sending Email, WP Mail SMTP Not Working

WordPress Security / Management Checklists

WordPress Malware Checklist

WordPres Maintainence Checklist

WordPress Security Guide For Beginners - OPEN.EDU