**Author**: Santhosh Tuppad
https://twitter.com/santhoshst | https://www.linkedin.com/in/santhosh-tuppad-338b7412/

# WordPress is cool, but it can also be cool for malicious evil hackers.

**Author**: Santhosh Tuppad
https://twitter.com/santhoshst | https://www.linkedin.com/in/santhosh-tuppad-338b7412/

# Local Risks that matter. Are you mitigating them or avoiding them?

- Do you have an antivirus (up-to-date)? (Kaspersky, Avast, Super Anti-Spyware, MalwareBytes.org or any other which does a great job)
- Are you doing a weekly scanning (full-scan) on the computer that you use for your work?
- If you use a public computer, do you trust them?
- There is no point in having great website security if your computer is infected by a keylogger.
- Are you leaving your cPanel session alive without logging out?
- Are you using a secure enough password on your cPanel?
- Is the FTP software that you are using secure enough? (For instance: WS_FTP has a security vulnerability) Read more at https://www.cvedetails.com/vulnerability-list/vendor_id-193/product_id-336/Ipswitch-Ws-Ftp-Server.html
- Is your WiFi protected? Are you using WPA2? If not, then I recommend it.
- Do you like to work from Coffee Shop or Starbucks? Maybe you don't want to log in to your bank account, WordPress site, cPanel, or anything that is sensitive and is of value to you.
- Maybe you can try using VPN software?
- I recommend using a work computer or bank account details on a computer which is only used for "safe-browsing" purposes. Do not mix torrents or websites which are really malware-prone with your work.
- In short, make your local environment safe and secure. It just takes awareness and following certain guidelines mentioned above.

# Is your hosting secure?

- Shared hosting: Usually unsafe if you are a reputed business and also it becomes easier for hackers to see your data when they hack into someone else's account.
- How credible is your hosting company? Maybe you can do some search on Google, ask questions, and do some research. WARNING: Avoid FAKE warning sites.
- Good web hosting = Pricing is gonna be a bit expensive. Bad Web Hosting = Very cheap and very vulnerable.

# WordPress Security - Are you doing these?

- Are you updating your WordPress timely?
- Maybe you can turn on auto-updates on your hosting control panel?
- Are you using WordPress hosting services?
- Are you using backup services and also some secure server settings on your cPanel?
- Maybe you want to look at https://wpengine.com/plans/ (Managed Hosting and Security plans) for your WordPress. [ Optional ].

**Author**: Santhosh Tuppad
https://twitter.com/santhoshst | https://www.linkedin.com/in/santhosh-tuppad-338b7412/

# Changing the configuration of your WordPress

- Change the settings of your WordPress because WordPress is open-source and black-hat hackers may be aware of certain naming conventions and try to gain access or try hacking using those default values. Change is for the better ;-)
- Modify the table prefix (change wp_ to something else).
- Change the "admin" username. Change it to something else which is not easy to guess by a human or brute force tool.
- Set a secure password. (Do not use the family name, dictionary name, 123456 sequences, or 123 at the end of the password).
- Security keys in WordPress to add a layer of security.
- I see some WordPress sites show the username as author/display name in articles or blog posts. In such a case, changing the "admin" default username to something else is a total waste. Doesn't make sense.

# WordPress Secure Installation

1. Create a new database with a "not so easy to guess" database name. (This is to change the table prefix of default WordPress which is wp_)
2. Go to MySQL in cPanel and create a new database. Create the database name something like, "r238ab991" this is hard to guess.
3. The next step is to create a strong username and strong password (I know it's hard, but you can try).
4. Use usernames like ew8292lkn320 and password as (maybe you can use password generators provided in your hosting. But, make sure they are more than 10 characters with better password rules). Look into the password strength meter as well if your hosting has one (But, beware of buggy ones. I can show 100/100 by using less than 6 characters as well ;-)).
5. Make sure you give "All Privileges" to the database user you created.
6. Download the latest WordPress files from http://wordpress.org/ website.
7. Open the wp-config-sample.php file with the text editor once you extract the compressed files or archive.
8. Replace the values with your database name, database user, and database password.
9. In the same file wp-config-sample.php, you will find a place to add secure keys. Generate the keys and use them. Your WordPress API to create these salt/keys.
10. Also, change the table prefix from wp_ to something else.
11. Change the wp-config-sample.php file to wp-config.php
12. Connect to FTP using FileZilla and transfer all the WordPress files to your server.
13. Once uploaded, go to your website in the web browser.
    [ You will see wp-admin/install.php Choose your language and continue ]
    1. In the username "DO NOT USE admin as USERNAME". Choose something obscure. For instance: ce897esc

2. Choose the password which is stronger. Longer the password, the better the password. Maybe you can use http://strongpasswordgenerator.com/ to generate a secure password with better entropy.
3. There is a setting called "Allow your website to be indexed by search engine". It is checked by default. You can uncheck it till you create a full-fledged website with all pages in place.
4. Once the installation is done, make sure you change your Display Name. You don't want your obscure username to be displayed as an author under every blog post. That's a hint for black-hat hackers to use the same username in the wp-admin login form. To change this, go to Users → Your Profile and go to the "Nickname" field. Change it to something else. It can be your name or full name or anything else. Then choose the Nickname as "Display name publicly as".

# Plugins to be installed on WordPress for better security

## [ *Be careful as some plugins may slow down your website* ]

- Limit login attempts
- Clef secure passwordless login
- All in one WP Security and Firewall
- Wordfence
- Limit IP addresses to login (whitelisting IP addresses)
- Hide the login page
- CAPTCHA on the login page (reCAPTCHA)
- Two-factor authentication
- .htpasswd (You need to enter this password and only then the server will authenticate you to show the login page. Extra layer for better security).
- Check the plugin's last updated date on the Wordpress.org plugins page.


- Also, look into the reviews and star rating for the specific plugin
- Add Google Authenticator on your Smartphone and then install the **Google Authenticator** plugin on your WordPress site.
- Some other easier plugins: Due 2 Factor Authentication and UNLOQ.io Authentication
- Create .htaccess and .htpasswd file to protect wp-login.php
- Also, password protect /wp-admin directory through cPanel
- Login errors that give hints to the black-hat hackers about valid usernames and invalid ones. (***Wordfence*** plugin has this option under "Options" to avoid this).
- Turn on "Automatic updates" for plugins

**Author**: Santhosh Tuppad
https://twitter.com/santhoshst | https://www.linkedin.com/in/santhosh-tuppad-338b7412/

# WP Updates Settings (To update the plugins always)

- Remove /readme.html from the File Manager. Also, remove the license.txt file from the web server.
- Change the permissions for files and folders for User, Group, and World. (Read Write Execute permissions). Never give 777 to directories.
- Move wp-config.php file from public_html or wwwroot folder to one level higher folder. This way we make sure it is a bit more secure as hackers cannot try to access it whatsoever unless they break into the cPanel or Control Panel of the hosting provider or they get access to FTP.
- Create a robots.txt file to secure your folders or sensitive files being indexed by search engine spiders

# Tools

- https://wpscan.org/
- https://securityheaders.io

# Blocking IP's (Malicious Activity)

- Block specific IP address
- Block entire network
- Block a narrow range of a network

# Plugin to avoid Brute-Force attack

- Jetpack by Wordpress.com
- Turn on the Brute Force Avoiding feature
- Also, Jetpack provides whitelist IP addresses (Just in case if you try to do invalid login attempts).
- Wordfence also has brute-force protection (Not sure at this point of time if that feature is in the commercial version or free version).

**Author**: Santhosh Tuppad
https://twitter.com/santhoshst | https://www.linkedin.com/in/santhosh-tuppad-338b7412/

# Summary / Quickview

- Take backup [ Regular ]
    - Full backups
    - Partial backups
- Run scheduled full scan on your local environment
- Use WiFi with WPA encryption
- Use secure FTP to transfer files from your computer to the server
- Maintain audit logs on your hosting environment
- Check your .htaccess files to see if it was modified by a hacker to have a redirect
- Check your plugins
- Check your users [ Maybe it was some other user who has admin access. Is it only you who is admin? If it's only you, was the password leaked or cracked? ]
- Use scanners like WP Scan http://wpscan.org/ and http://sucuri.net/
- Use the GOTMLS scan and run the scanner → Get off the maliciously loaded scripts
- Protect your privacy of whois information [ You don't want hackers to know the administrator's email address and hack it in order to compromise your hosting account ].
- Something fishy? Change all your passwords. WordPress, hosting account, .htaccess .htpasswd, salt keys in wp-config.php, Google Authenticator / 2 factor authentication etc.
- Use WP Security Audit Log to do automatic audits for your WordPress website.
- Use Wordfence to avoid brute-force attacks, live traffic analysis, use it for blocking IPs or networks for a specific time, and more features.
- You can also use https://hackertarget.com/wordpress-security-scan/ to scan your WordPress website.
- Block Bad Queries, Blackhole for bad bots, WPBruiser

**Counter-measures**

- Disabling author pages (http://example.com/?author=1 or 2 or 3...N)
  Add the following piece of code under the theme or child theme,

```
<?php
header("HTTP/1.1 301 Moved Permanently");
header("Location: /");
?>
```

This has to be in the authors.php file.

Also, you can use the Yoast plugin, but this edit in authors.php is better in my view.

- Setting up the HTTP headers using the HTTP headers plugin

  Plugin URL: https://wordpress.org/plugins/http-headers/

    - X-Frame-Options

- X-XSS-Protection
- X-Content-Type-Options
- X-UA-Compatible
- Strict-Transport-Security
- Public-Key-Pins
- Access-Control-Allow-Origin
- Access-Control-Allow-Credentials
- Access-Control-Max-Age
- Access-Control-Allow-Methods
- Access-Control-Allow-Headers
- Access-Control-Expose-Headers
- P3P
- Referrer-Policy