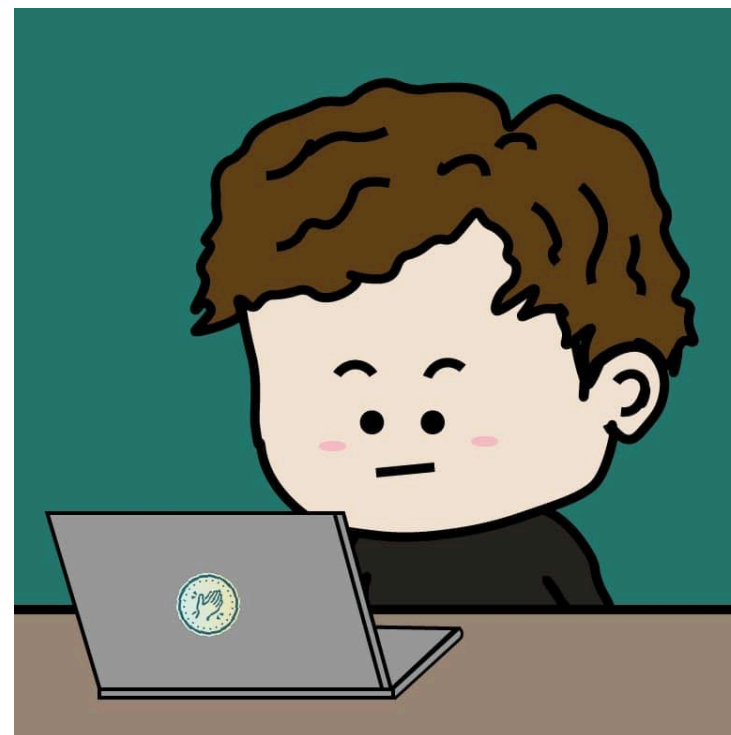


# 如何加強 WordPress 網站的安全性以保護 您的網站和使用者

Presented by: Nicholas Yau

# About Me

- 現職 Linux 資深系統工程師，
- (ISC)<sup>2</sup>網絡安全(Certified in Cybersecurity)認證。
- 開源軟件支持者
- 十年以上 WordPress 用家。
- 同時亦擔任多個香港IT社群的志工
  - Open Source Hong Kong 開源香港 擔任執行委員
  - PyCon Hong Kong 的志工
  - Hong Kong WordPress Meetup 的活動講者等
  - 近年亦有參與其他項目，如 LikeCoin、Tor Project 及 Nostr 等。



# 資訊安全鐵三角

## CIA Traid



# Confidentiality 機密性


- 指訊息不為其他不應獲得者獲得，保障訊息在對的人、對的時間、對的裝置和對的地點上被存取，用以維護用戶資訊的保密性
- 限制未經授權的資料之訪問與修改權
  - Authentication 驗證使用者合不合法
  - Authorization 使用者能做甚麼事情
  - Accounting 紀錄使用者做了甚麼事情


# Authentication 驗證使用者

- 使用者名稱的考慮
- 密碼的複雜性
- 雙重驗證 2FA
- 更改wp-admin到其他名稱

# Account Lockdown Policy

**Login Lockdown Options**

 Basic

 20/20

**Enable Login Lockdown Feature:** ☒ Check this if you want to enable the login lockdown feature and apply the settings below

**Allow Unlock Requests:** ☐ Check this if you want to allow users to generate an automated unlock request link which will unlock their account

**Max Login Attempts:**  Set the value for the maximum login retries before IP address is locked out

**Login Retry Time Period (min):**  If the maximum number of failed login attempts for a particular IP address occur within this time period the plug

**Time Length of Lockout (min):**  Set the length of time for which a particular IP address will be prevented from logging in

**Display Generic Error Message:** ☒ Check this if you want to show a generic error message when a login attempt fails

**Instantly Lockout Invalid Usernames:** ☐ Check this if you want to instantly lockout login attempts with usernames which do not exist on your system

**Instantly Lockout Specific Usernames:**

Insert one username per line. Existing usernames are not blocked even if present in the list.

**Notify By Email:** ☐ Check this if you want to receive an email when someone has been locked out due to maximum failed login attempts

Enter an email address

Save Settings

# Enable WP 2FA Settings

## WP 2FA Settings

Use the settings below to configure the properties of the two-factor authentication on your website and how users use it. If you have any questions send email at [support@melapress.com](mailto:support@melapress.com)

### Which 2FA methods can your users use?

When you uncheck any of the below 2FA methods it won't be available for your users to use. You can always change this later on from the plugin's settings page.

### Which of the below 2FA methods can users use?

#### Select the methods

#### Primary 2FA methods:

- ☒ One-time code via 2FA App (TOTP)
- ☐ One-time code via email (HOTP) - ensure email deliverability with the free plugin [WP Mail SMTP](#).

Allow user to specify the email address of choice

☐ Yes ☒ No

# Authorization 使用者權限


- WordPress 使用者權限
- 伺服器權限設定是否正確
  - 資料夾權限 775 or 755 (限制只有檔案owner或group內的用戶才可修改資料夾內容)
  - 檔案權限 644 (限制只有檔案的owner才可以修改)
  - 一些重要檔案，如wp-config.php，應該設定為640或600比較安全 (檔案內含資料庫密碼)



# Accounting 使用者權限

- 存留應有的活動紀錄並能歸責肇因。(Accountability and Accounting/Auditing)
- Example:  
透過 log(日誌), timestamp(時戳)...等紀錄，完成 5 種 W(When, Where, How, Who, Why)的資訊的保存，並能從其推論究因歸責後，對系統或服務進行修正與改善，以避免再次發生該問題。

# Monitor Login in Users & Failed logins

 **SUCURI** WP Plugin<sub>v1.8.39</sub>

[Feedback Survey](#)[Dashboard](#)[Firewall \(WAF\)](#)[Settings](#)

[All Users](#)[Admins](#)[Logged-in Users](#)[Failed Logins](#)

### Failed logins

This information will be used to determine if your site is being victim of [Password Guessing Brute Force Attacks](#). These logs will be accumulated and the plugin will send a report via email if there are more than **30** failed login attempts during the same hour, you can change this number from [here](#). **NOTE:** Some "Two-Factor Authentication" plugins do not follow the same rules that WordPress have to report failed login attempts, so you may not see all the attempts in this panel if you have one of these plugins installed.

Username	IP Address	Date/Time	Web Browser
nicholasyau	209.97.169.60	August 21, 2023 1:50 pm	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.108 Safari/537.36
nicholasyau	209.97.169.60	August 21, 2023 1:50 pm	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.108 Safari/537.36

# Integrity 完整性

- 確保修改資訊時是經授權的，所使用的資訊在傳送或儲存過程中，必需確保並能證明內容並未遭到竄改或偽造

# Using WordPress security plugin to check core files integrity

## WordPress Integrity

We inspect your WordPress installation and look for modifications on the core files as provided by WordPress.org. Files located in the root directory, wp-admin and wp-includes will be compared against the files distributed with v6.2.2; all files with inconsistencies will be listed here. Any changes might indicate a hack.








### Core WordPress Files Were Modified

We identified that some of your WordPress core files were modified. That might indicate a hack or a broken file on your installation. If you are experiencing other malware issues, please use a [Server Side Scanner](#).

[Review False Positives](#)


**PHP Version:** 8.1.18    **Version:** 6.2.2    **Running on:** cloudflare    **Redirects to:** https://nicholas.hk/

This information will be updated in 6 hours — [Refresh Malware Scan](#)

WordPress Integrity (5) ⓘ			
<input type="checkbox"/>	File Size	Modified At	File Path
<input type="checkbox"/>	 3B	June 15, 2023 12:27 am	.abc.html
<input type="checkbox"/>	 7.84K	May 13, 2023 11:41 pm	.htaccess_old
<input type="checkbox"/>	 0B	July 11, 2023 2:57 pm	cfapi.php ⓘ
<input type="checkbox"/>	 3.88K	July 11, 2023 2:55 pm	cloudflare_api.php
<input type="checkbox"/>	 32B	June 28, 2023 2:45 pm	test.php ⓘ

# Assign least privilege to non-admin user accounts

Toolbar

Language 

Name

Username

Role

First Name

ng site

Ad User

Ad Manager

Ad Admin

SEO Editor

SEO Manager

Shop manager

Customer

Subscriber

Contributor

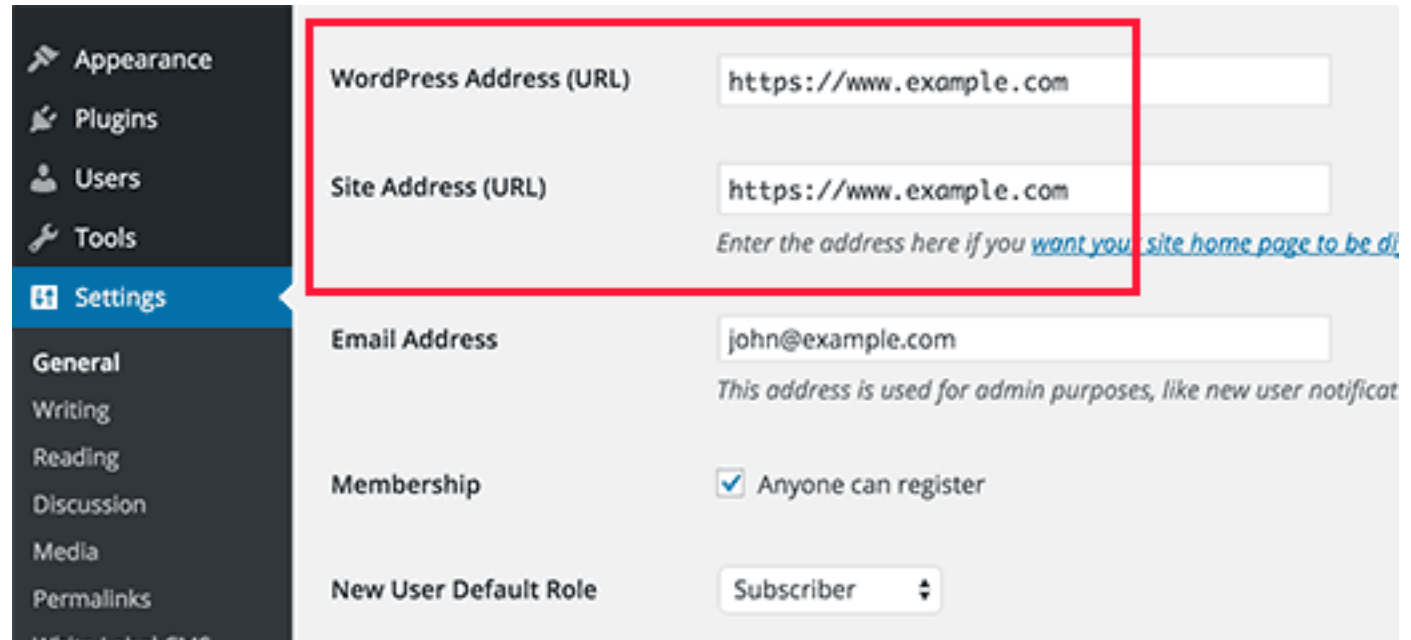
Author

✓ Editor

Administrator

— No role for this site —

Always use  
HTTPS to  
protect the  
data in transit



The screenshot shows the WordPress Settings interface. On the left is a dark sidebar with a menu containing 'Appearance', 'Plugins', 'Users', 'Tools', 'Settings' (highlighted in blue), 'General', 'Writing', 'Reading', 'Discussion', 'Media', 'Permalinks', and 'Writing Labels & CMS'. The main content area is light gray and contains several settings. A red rectangular box highlights the 'WordPress Address (URL)' and 'Site Address (URL)' fields, both of which contain the text 'https://www.example.com'. Below the 'Site Address (URL)' field is a small italicized note: 'Enter the address here if you [want your site home page to be different](#)'. Other visible settings include 'Email Address' with the value 'john@example.com' and a note 'This address is used for admin purposes, like new user notifications', 'Membership' with a checked checkbox for 'Anyone can register', and 'New User Default Role' set to 'Subscriber'.

WordPress Address (URL)	<input type="text" value="https://www.example.com"/>
Site Address (URL)	<input type="text" value="https://www.example.com"/> <small>Enter the address here if you <a href="#">want your site home page to be different</a></small>
Email Address	<input type="text" value="john@example.com"/> <small>This address is used for admin purposes, like new user notifications</small>
Membership	<input checked="" type="checkbox"/> Anyone can register
New User Default Role	<input type="text" value="Subscriber"/>

# Availability可用性

- 可用性就是讓一個系統處隨時可工作狀態，資訊服務不因任何因素而中斷/停止

# High Availability / Disaster Recovery concern

- 利用為雲端服務商建立高可用性架構HA (High Availability)
- 內容傳遞網路 ( Content Delivery Network - CDN )
- 網站及資料庫的備份和回復



# Plugin for WordPress Backup





## Last log message:

[Download most recently modified log file](#)

The backup succeeded and is now complete (Aug 15 10:18:42)

## Existing backups 4

More tasks: [Upload backup files](#) | [Rescan local folder for new backup sets](#) | [Rescan remote storage](#)

<input type="checkbox"/>	Backup date	Backup data (click to download)	Actions
<input type="checkbox"/>	Aug 15, 2023 10:17 	<a href="#">Database</a> <a href="#">Plugins</a> <a href="#">Themes</a> <a href="#">Uploads</a> <a href="#">Others</a>	<a href="#">Restore</a> <a href="#">Delete</a> <a href="#">View Log</a>
<input type="checkbox"/>	Aug 08, 2023 10:17 	<a href="#">Database</a> <a href="#">Plugins</a> <a href="#">Themes</a> <a href="#">Uploads</a> <a href="#">Others</a>	<a href="#">Restore</a> <a href="#">Delete</a> <a href="#">View Log</a>
<input type="checkbox"/>	Aug 01, 2023 10:19 	<a href="#">Database</a> <a href="#">Plugins</a> <a href="#">Themes</a> <a href="#">Uploads</a> <a href="#">Others</a>	<a href="#">Restore</a> <a href="#">Delete</a> <a href="#">View Log</a>
<input type="checkbox"/>	Jul 25, 2023 10:25 	<a href="#">Database</a> <a href="#">Plugins</a> <a href="#">Themes</a> <a href="#">Uploads</a> <a href="#">Others</a>	<a href="#">Restore</a> <a href="#">Delete</a> <a href="#">View Log</a>

Actions upon selected backups

[Delete](#)

[Select all](#)

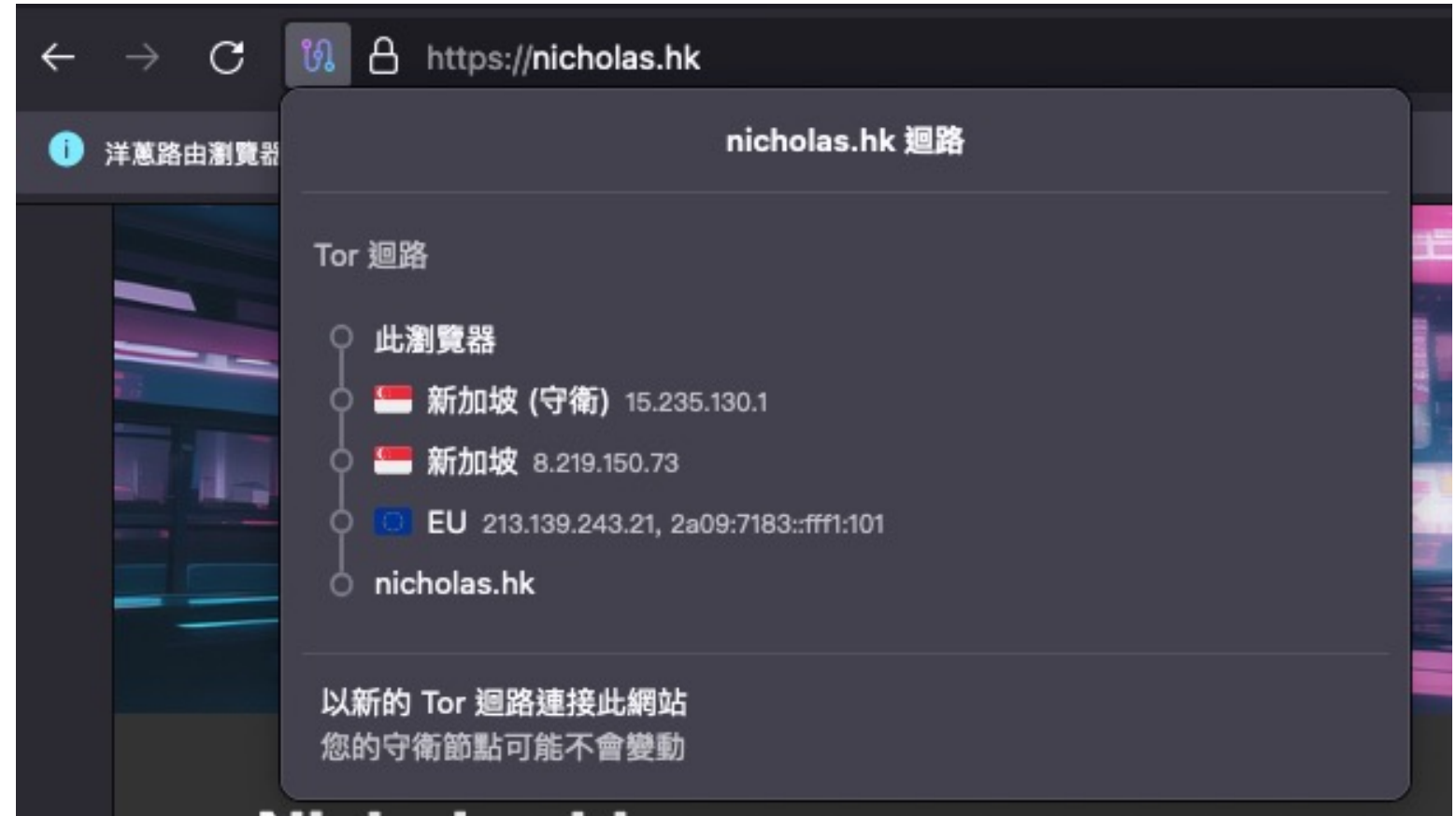
[Deselect](#)

*Use ctrl / cmd + press to select several items, or ctrl / cmd + shift + press to select all in between*

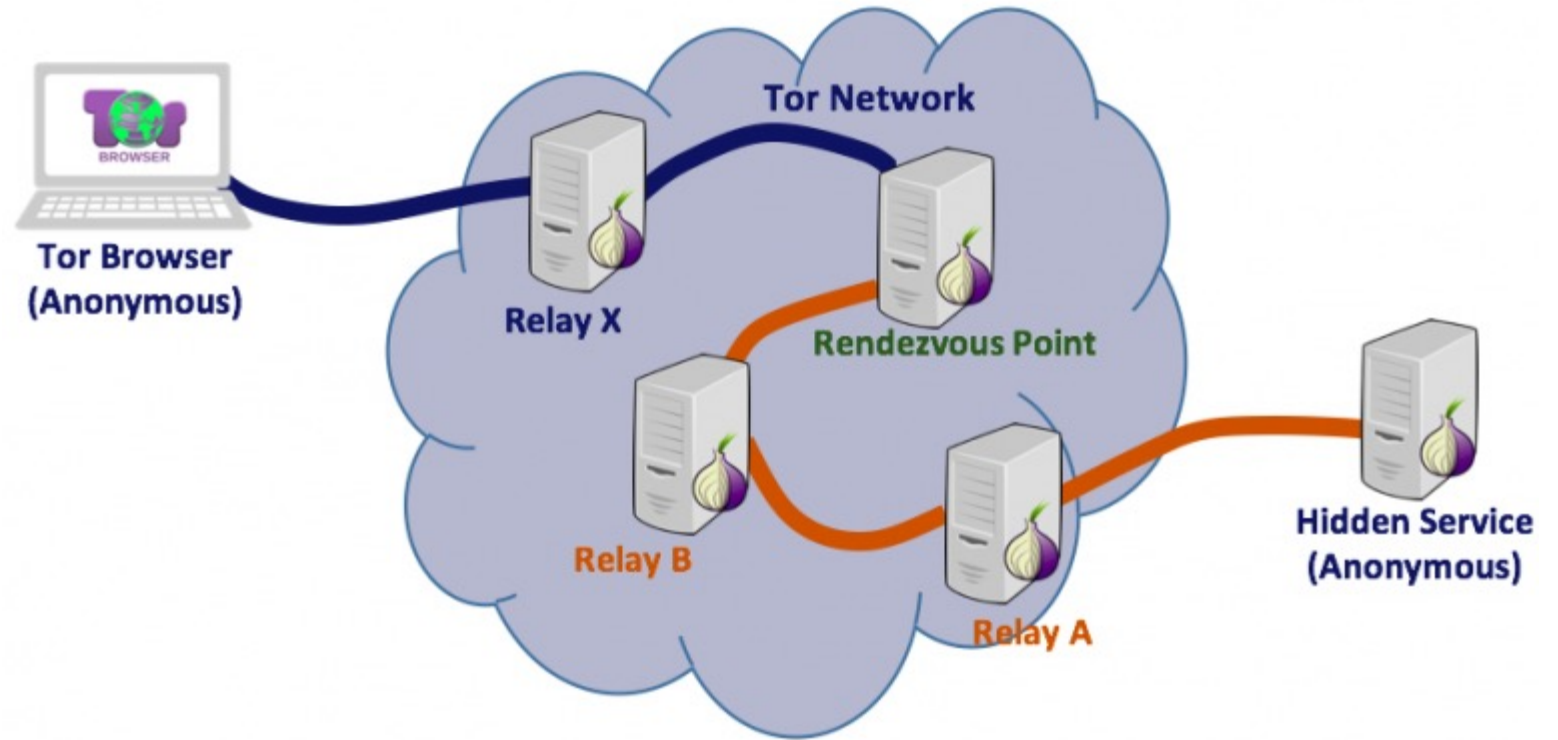
# How to be anonymous in Wordpress

- VPN?
- Tor Network

# Using Tor Browser to hide visitor IP address



Use Tor Hidden Service to create a website without exposing your IP address



# Example of Tor Hidden Network

## Submit documents to WikiLeaks ×

WikiLeaks publishes documents of political or historical importance that are censored or otherwise suppressed. We specialise in strategic global publishing and large archives.

The following is the address of our secure site where you can anonymously upload your documents to WikiLeaks editors. You can only access this submissions system through Tor. (See our [Tor tab](#) for more information.) We also advise you to read our [tips for sources](#) before submitting.

**<http://ibfckmpsmylhbfovflajicjgldsqpc75k5w454irzwlh7qifgglnbad.onion>**

If you cannot use Tor, or your submission is very large, or you have specific requirements, WikiLeaks provides several alternative methods. [Contact us](#) to discuss how to proceed.

[How to contact WikiLeaks?](#)[What is Tor?](#)[Tips for Sources](#)[After Submitting](#)

# Can WordPress Setup as a Hidden Service?

- Yes. But the site owner need full access to the server to setup the Tor Hidden Service
- Limitation: WordPress can only setup one Site Address, it's difficult to create a site with both registered domain name xxxx.com and xxxxxxxxxxxxxxxx.onion on the same WordPress site
- Another advantages of Hidden Service, there is no requirements for any fixed IP address or port forward setting for the website. Tor Network will help to connect your site to the hidden network.

# Q & A Session

