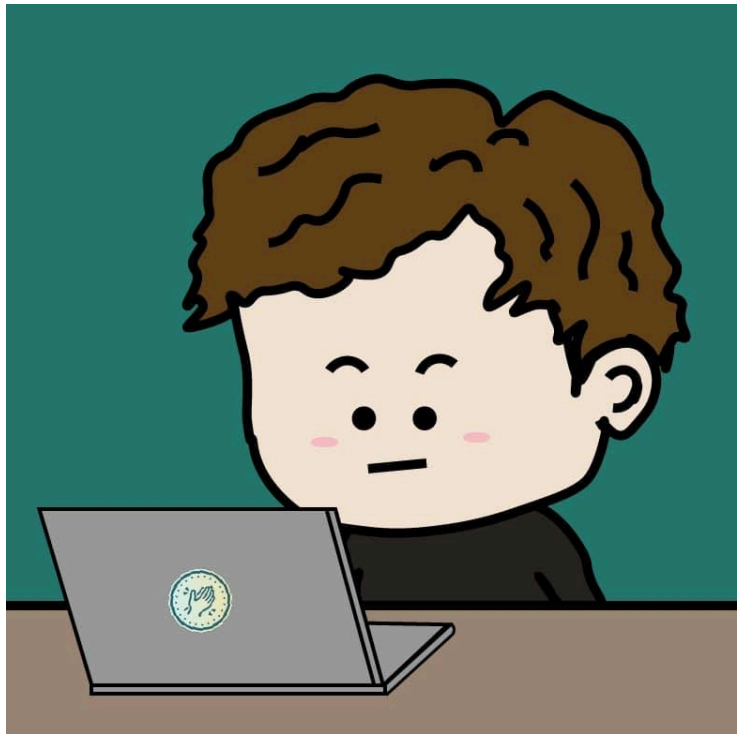
如何加強 WordPress 網站的安全性以保護您的網站和使用者

Presented by: Nicholas Yau

About Me

- 現職 Linux 資深系統工程師，
- (ISC)²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

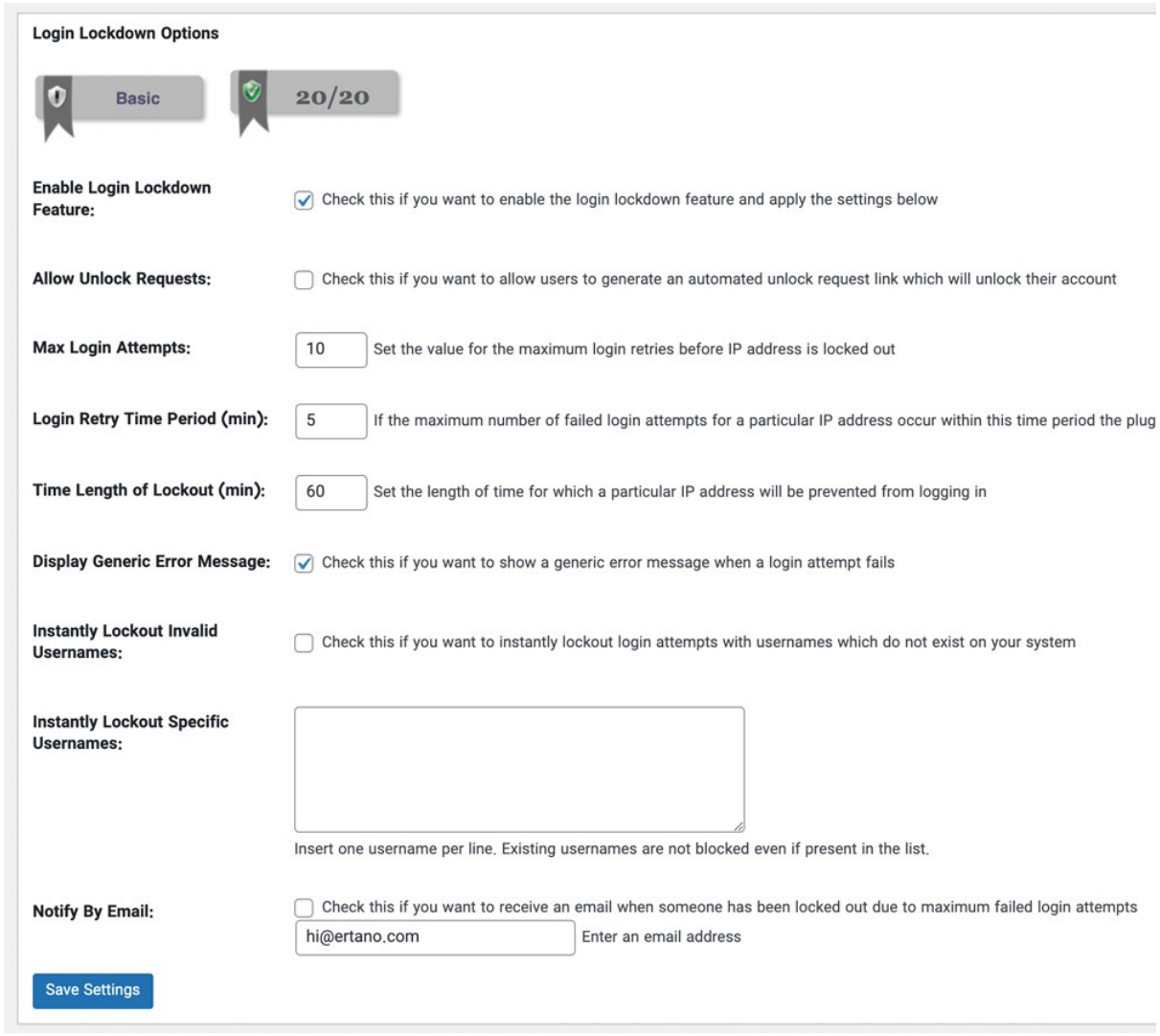
Confidentiality 機密性

- 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

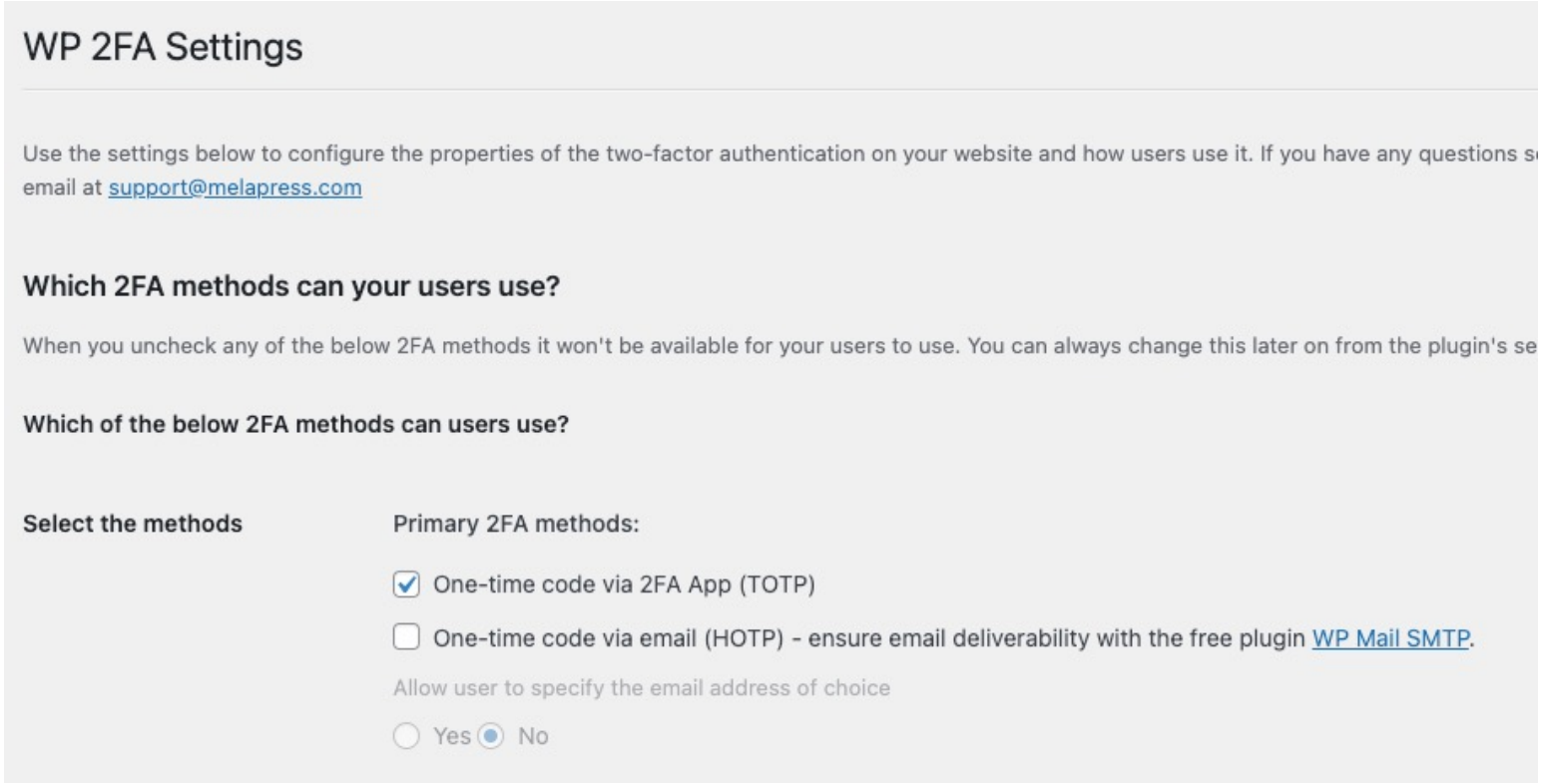
Authentication 驗證使用者

- 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



Enable WP 2FA Settings



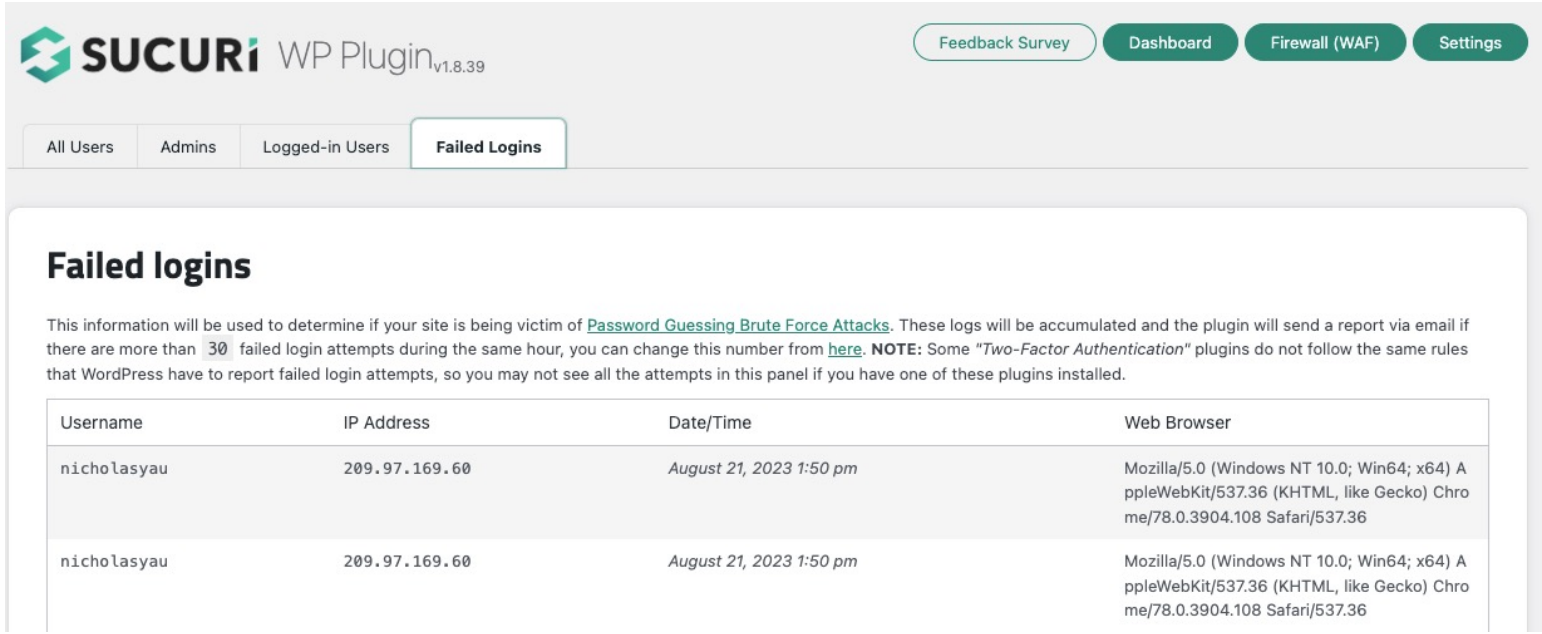
Authorization 使用者權限

- 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。

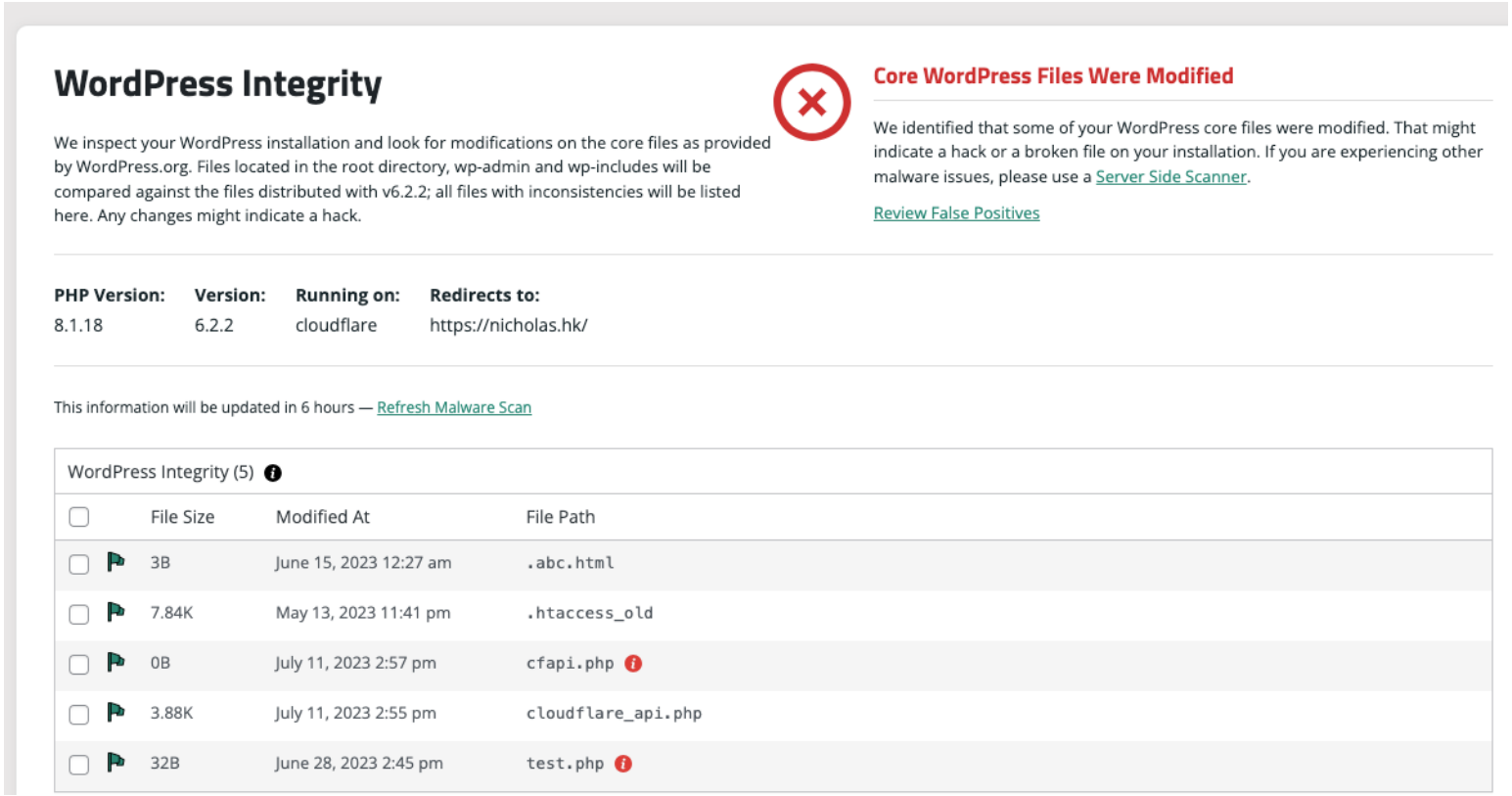
Monitor Login in Users & Failed logins



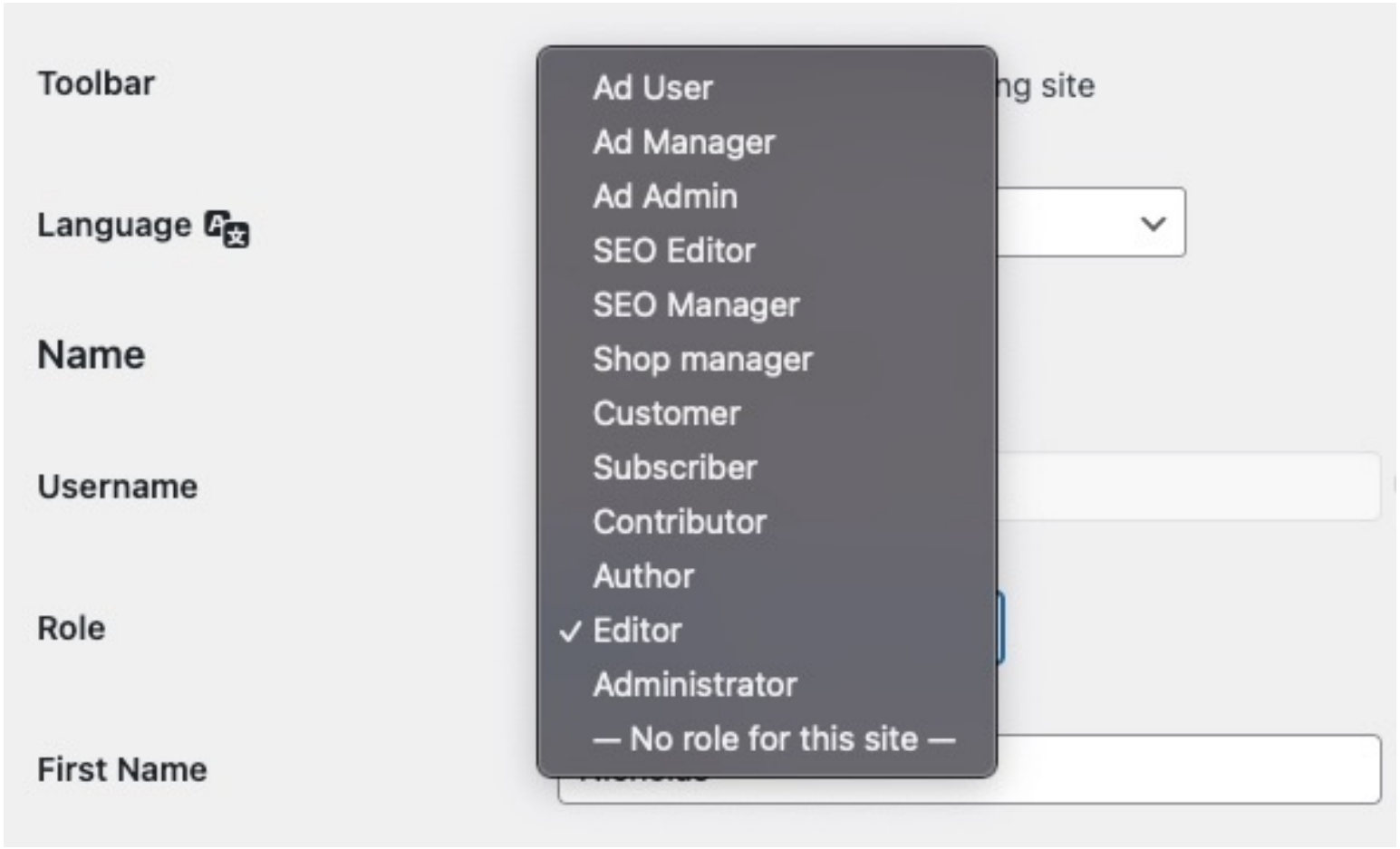
Integrity 完整性

- 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

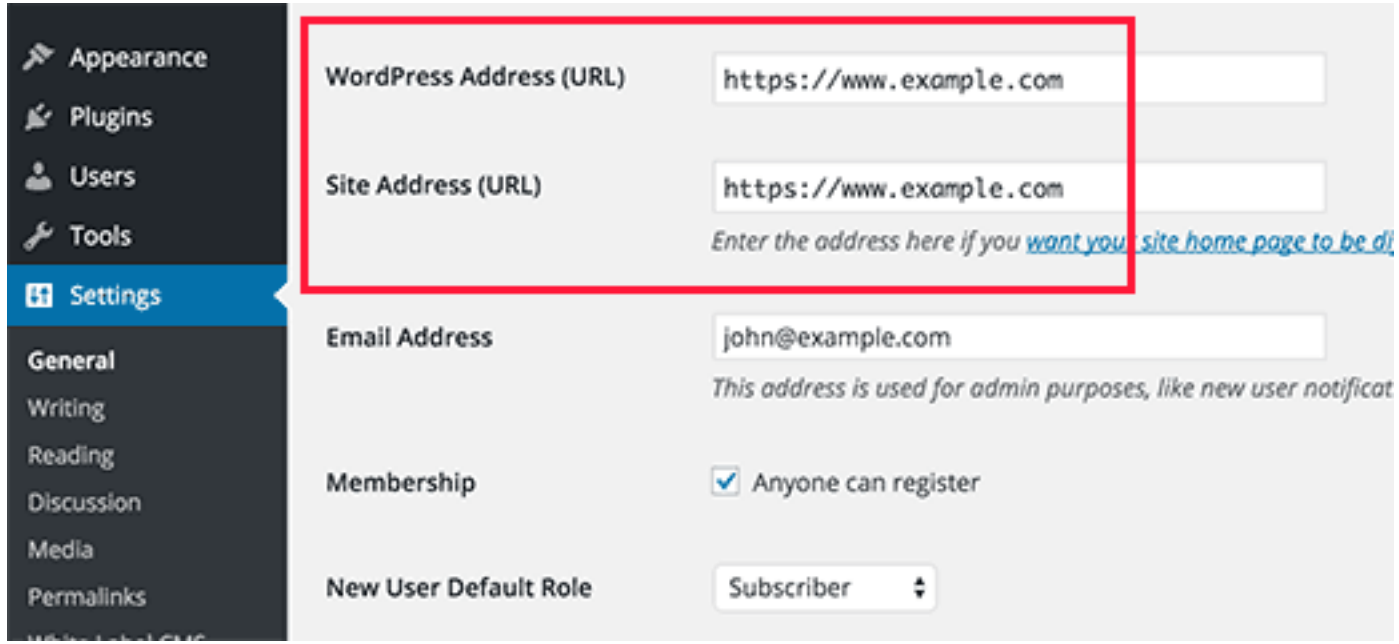
Using WordPress security plugin to check core files integrity



Assign least privilege to non-admin user accounts



Always use HTTPS to protect the data in transit



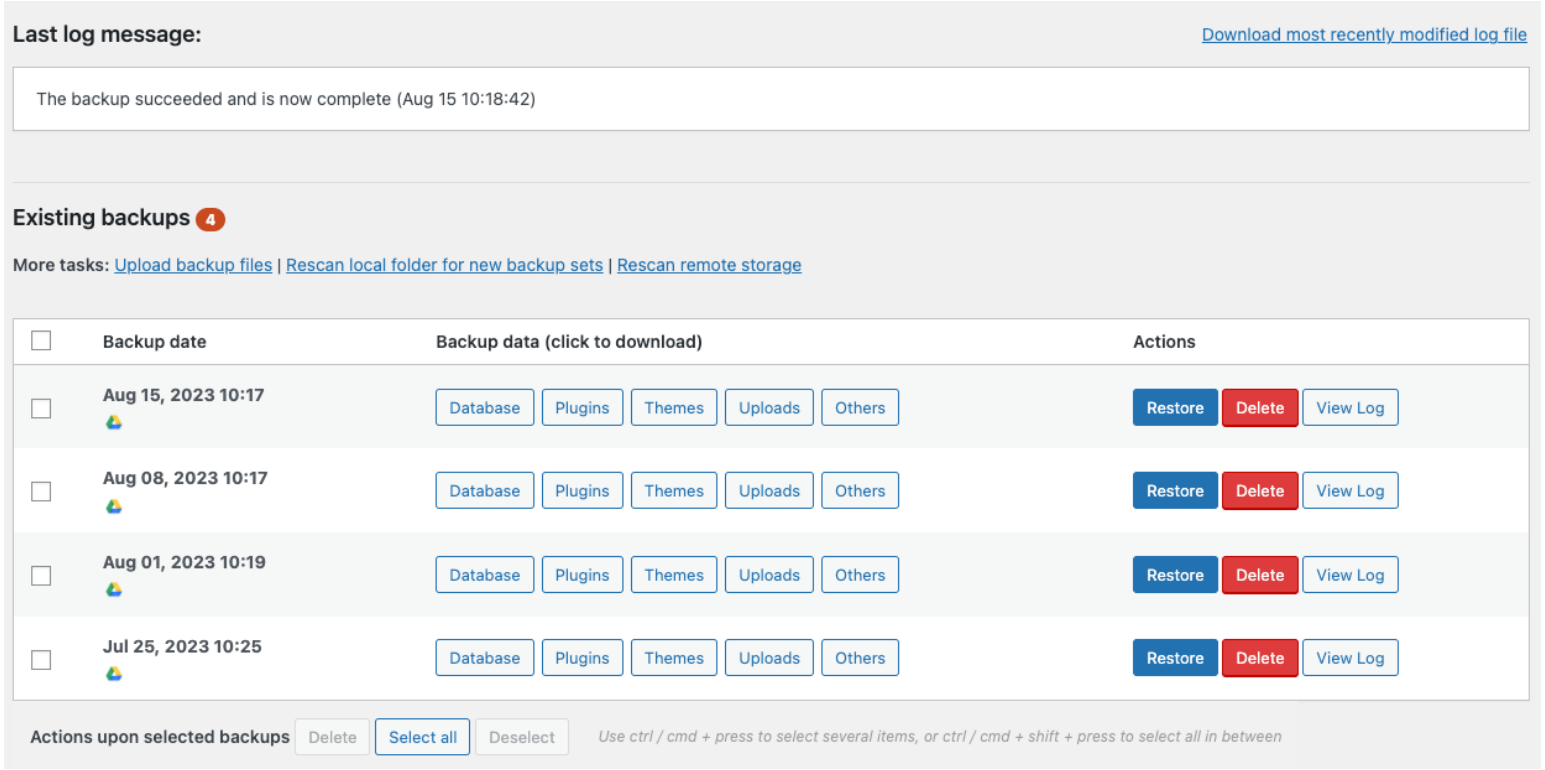
Availability可用性

- 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

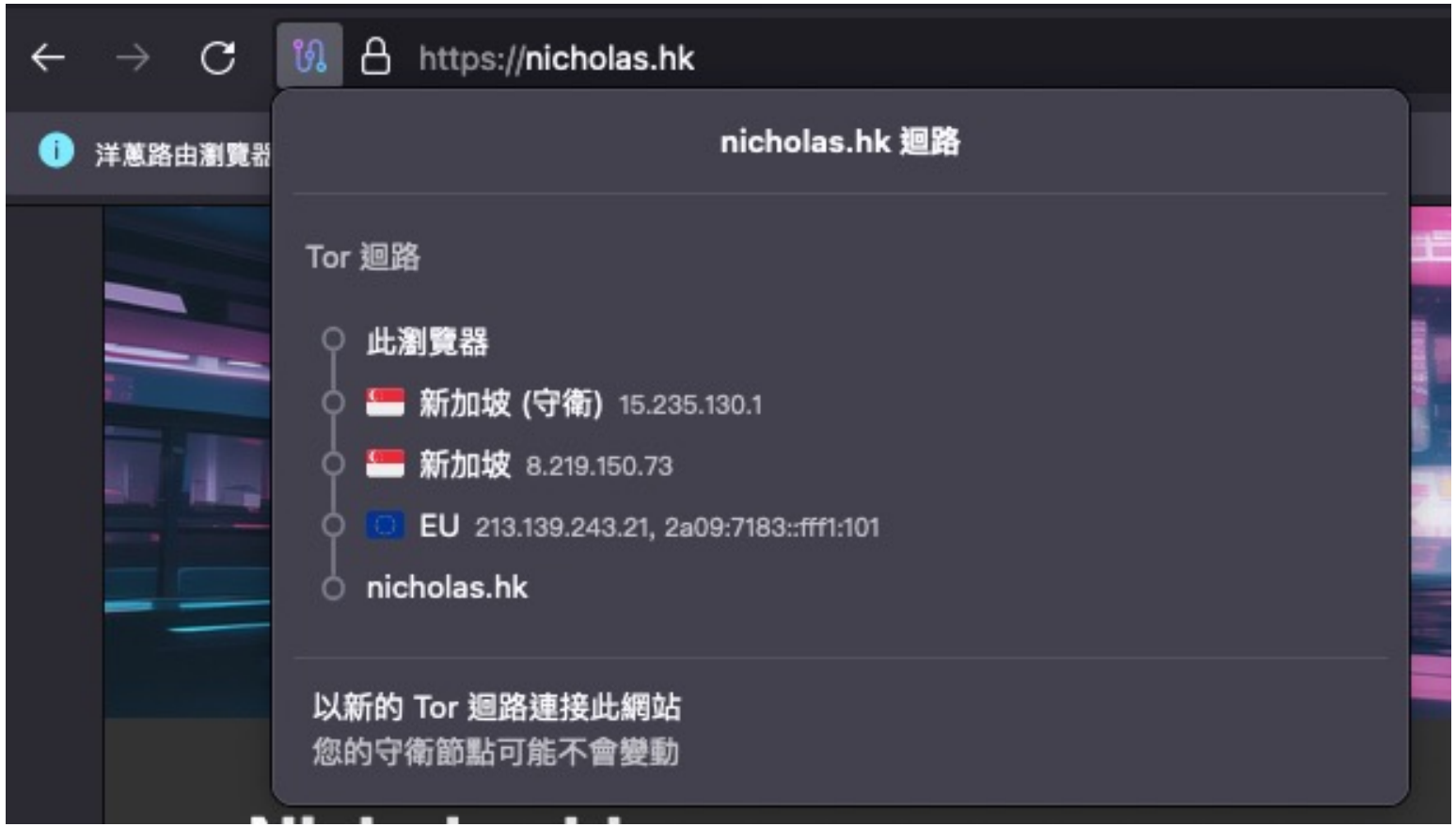
Plugin for WordPress Backup



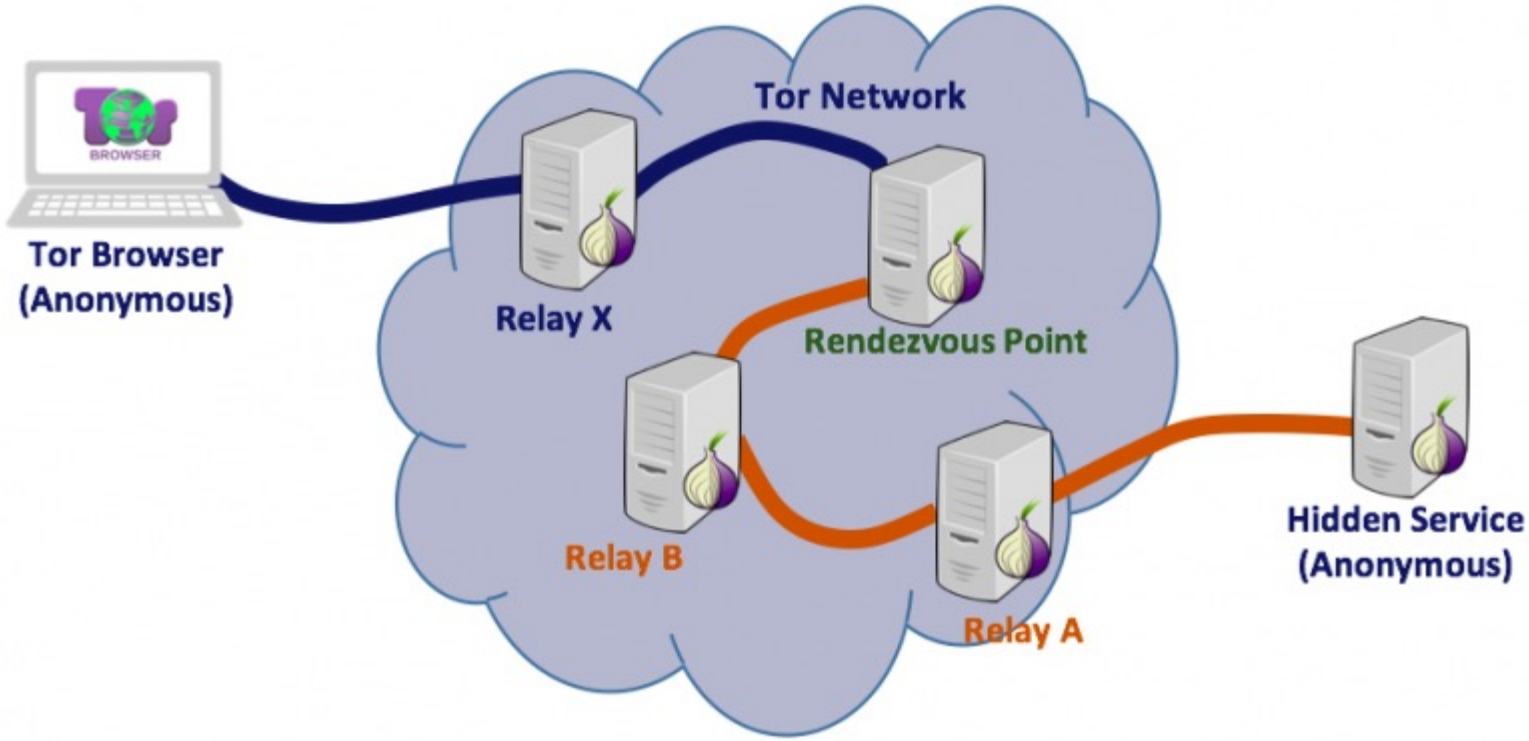
How to be anonymous in Wordpress

- VPN?
- Tor Network

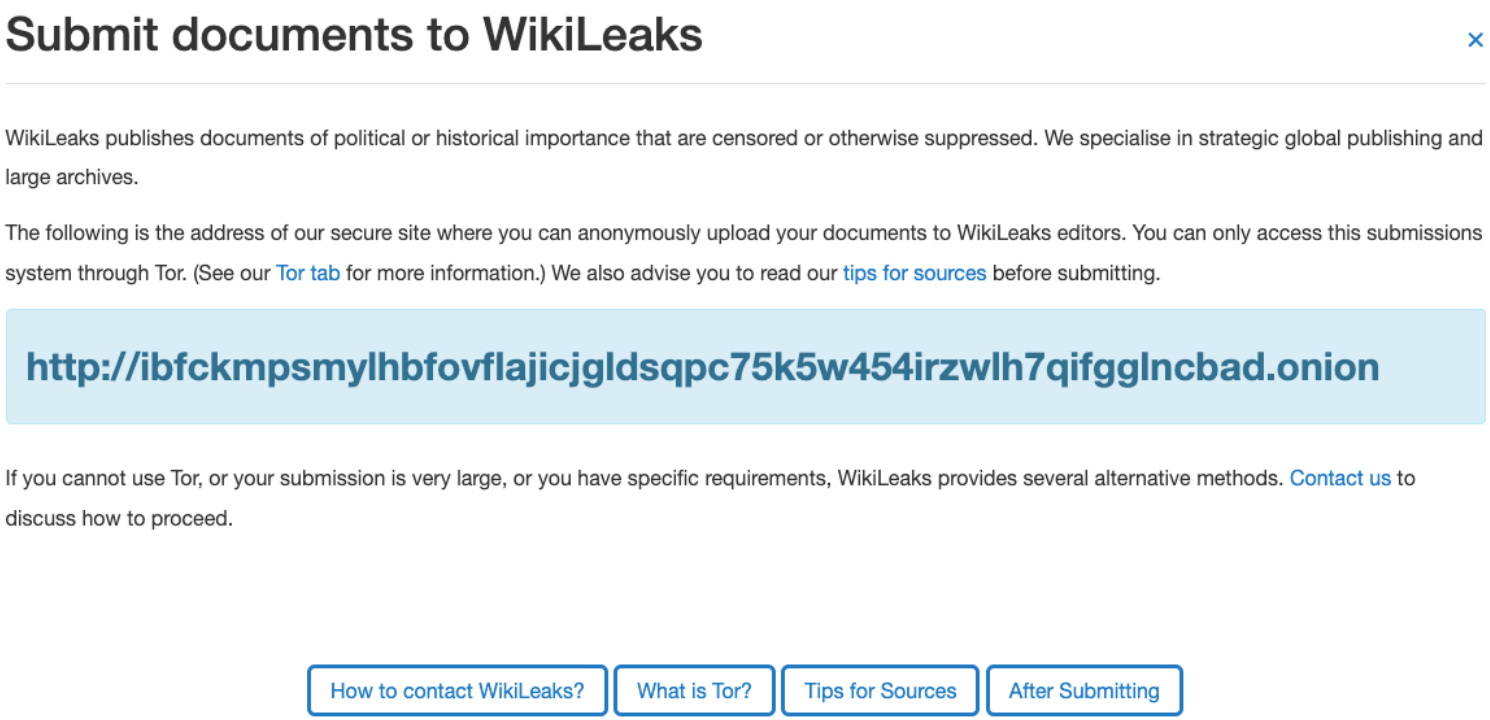
Using Tor Browser to hide visitor IP address



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



Example of Tor Hidden Network



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 xxxxxxxxxxxxxx.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