AI 寫程式，開發效率與資安風險的雙面刃？

在這個生成式 AI 大爆發的時代，各行各業正面臨著許多前所未有的問題，而身在資訊圈的我們，又該怎麼與這些來勢洶洶的 AI 共同演奏出一首協奏曲呢？

吳念寬

作者介紹

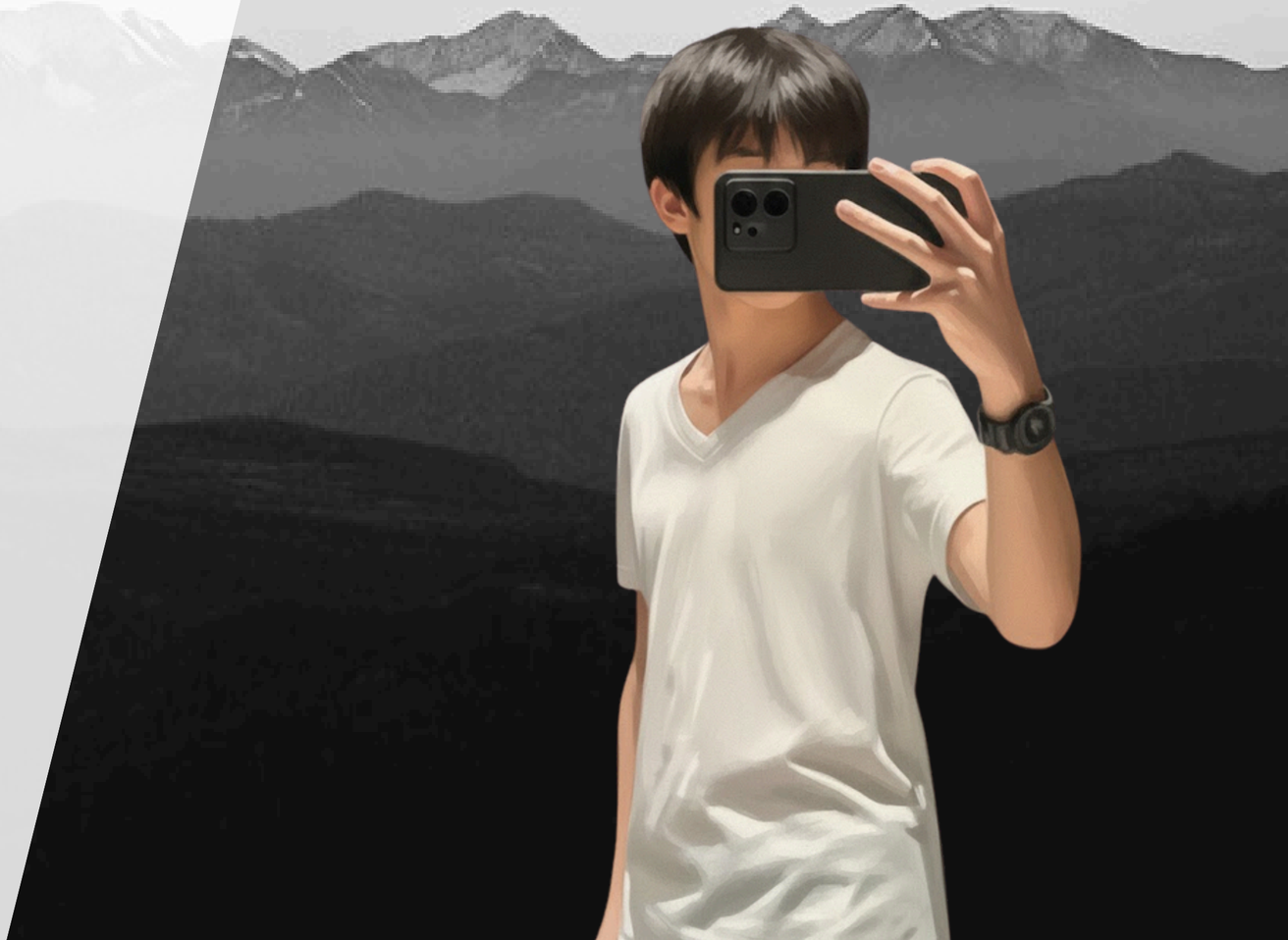
吳念寬

3 年
社群經驗

5+
網站專案

600000+
受惠用戶

各位早安，我是一位常被大佬們炸魚的高中生開發者。
在下擅長創新用戶體驗、挖掘專案靈感，除了開發專案以外，也喜歡獨自一個人探索奇景！



ONION.OWO　ONION.TW

目錄

TABLE OF CONTENTS

QRCODE

TAICOOLAH

簡報大綱

隨著生成式 AI 的浪潮，各行各業將面臨 21 世紀的全新挑戰，而身處資訊圈的我們，又該怎麼去應對呢？

本簡報將透過 **開發效率** 與 **AI 介入資訊圈** 等兩個方面作為出發點，前期會先點出開發效率的重要性，並接著探討 AI 對於提升開發效率的可能性，後期則會點出 AI 和 Vibe Coding 可能帶來的風險和問題點。

不僅於此，本簡報也收錄了一些生活上的實際例子，無論是 Vibe Coding 浪潮下帶來的迷因，還是作者自己實際的開發經驗，您都可以在本簡報中看到！

TAICOOLAH

『為甚麼你需要開發效率？』

開發專案幹嘛搞那麼麻煩...？我開發的時間又不是說只有幾個小時，況且我們也有團隊可以分工欸！

開發效率能夠帶來的好處？

在日常的專案開發中，開發效率其實扮演著一個很重要的角色，像是 專案的開發時間、架構的複雜度、團隊的合作能力，其實都取決於開發效率。

提升開發效率，不僅可以讓專案可以在更短的時間內開發完畢，更可以提高提早發現專案問題的機率，專案的品質與縮短開發時間，其實也是可以兼得的。

舉例來說，哪怕只是規劃資料庫的資料表結構，要是一開始就沒有想的完全一點，後面也只會匆匆忙忙連滾帶爬的補上缺少的欄位吧？就像是主線任務做到一半突然岔出個支線任務，而且不完成支線任務，主線劇情還不能繼續解鎖。

所以！這就是為甚麼你需要提升你的開發效率，請看下頁舉例：

完整、精確的規劃

說到規劃，你可能會覺得這東西講個大概就好了吧，開發時再來想也不急，但事實卻與之恰恰相反。

把事情拖到開發時才來想，就好比如要吃飯時才在想要吃甚麼，頂著餓意 (deadline 壓力) 在緊要關頭想著等下到底要吃甚麼 (要開發甚麼功能)，而且可能甚至在要開始開發以前，你就已經忘記當初要開發的功能了 :(

提前將開發計畫想好 (例如要開發甚麼功能，要使用哪些套件)，不僅可以減輕在開發時的壓力，也可以提升開發流程的順暢度，更可以區分出哪件事情是優先級別較高的，例如資料庫架設、環境初始化、網域購買。

拆分開發目標

接著就是拆分開發目標，若今天一次就面對整個專案的開發計畫，想必是個人都會有點想逃避的心情吧？

將一個大的目標拆成幾個小目標，再根據優先級別循序製作，才不會導致開發到一半東缺西缺，一下缺範例資料，一下缺要使用的函式、組件。

所以，這就是為甚麼需要拆分目標。而除了以上幾點外，拆分目標也有很多好處，例如方便進一步規畫專案、可以根據所剩時間選擇要開發的項目。

可以輔助的軟體、網站

排程的規劃可以有很多種方式，無論是 紙本、軟體、線上服務，只要它可以提升你的開發效率，其實都很不錯！

以作者的方式舉例，我本人比較偏向使用 Discord 的伺服器功能來做專案管理、排程規劃。一個專案一個頻道，如果專案比較大就會另開一整個伺服器給它。

當有項目需要修復的時候，直接在該頻道發訊息即可，而且還支援 Markdown！同時跟其他開發夥伴要溝通也都很方便呢！

手寫筆記	Notion	HackMD
Google Keep	Microsoft Todo	Discord

『AI 如何輔助我們提升開發效率？』

AI 寫的程式真的可以用嗎？他看起來只會幫倒忙吧.....
我要的代碼他不給我，數學題目也可以算的一蹋糊塗，又能指望
它幫上我們甚麼忙呢？

IDE 整合

如今的開發模式已經迎來相當多的改變，現在只要按一下 TAB、開啟代理模式，就可以直接在 IDE 上享受到 AI 的方便性。

雖然說 AI 有些時候會誤判，但大部分情況下估測的內容都蠻準確的。同時，它也有很多方便的功能，例如錯字自動修正、自動替換相似內容。

Google Antigravity

Github Copliot

Cursor

靈感發掘

AI 除了可以幫你寫程式以外，它也可以是你開拓產品市場的一大助手！
一些具有連網功能的 AI 可以幫你爬取各大論壇上的用戶回饋、大家在意的點、想要的功能，AI 通通會幫你整理好。

有些時候甚至也可以幫忙想想專案要取甚麼名字好呢.....

以作者開發過的專案【DCTW】為例：
在規劃開發項目的時候，就請 AI 爬取了國內外各大 Discord 宣傳網站，他們的優缺點和用戶的回饋，藉此獲得了一些答案，例如評論系統、工具箱、伺服器模板的開發建議。

打下基礎

當今天終於開始了專案的開發作業，卻敗在了自己的懶惰上，而這個時候 AI 就可以幫你先打下基礎，增加你想要繼續開發下去的動力！

如果你前面有規劃好開發的項目，**現在！就是那陀規劃發光發熱的時候了！**
無論是資料表結構、函式設計、頁面內容，都可以丟給 AI 來讓產出的內容可以變得更準確些！

假設你今天要開發一個網站，但是又懶的設計頁面，就可以叫 AI 先為你打下基礎！也正是這個時候，你前面辛苦規劃好的開發項目就可以派上用場了，頁面要有甚麼內容、使用甚麼組件、函式，直接複製貼上丟給 AI，讓他先幫你產出基本的頁面，**接著再自己調整細節、檢查代碼，豈不美哉？**

其他實用用途

AI 也可以幫你做到許多小事情，例如以下內容：

- 【產生專案名稱】

+ 有些時候絞盡腦汁也想不出專案要取甚麼名字，AI 的想法也許可以幫到你。

- 【產生範例資料】

+ AI 可以協助你在資料還沒建立好的時候先行產出隨機的範本資料，若今天是一個人慢慢手打，不知道要打到甚麼時候。

- 【產生正則表達式】

+ AI 也很適合拿來產正則表達式，簡單打上要求就可以產好你要的東西！

『Vibe Coding？資安風險？』

“欸欸為甚麼其他人可以訪問到我的後台頁面阿？”

“來看看我的網站！ http://localhost:3000/ ”

“為甚麼我的電腦裡面有個叫做 「微軟大戰代碼」 的東西？”

Vibe Coding 是甚麼？

隨著生成式 AI 的發展，一種透過描述的方式來達成目標的開發流程誕生了。

Vibe Coding 讓人只需要透過溝通、檢查，並將程式碼實作全權交給 AI，他讓開發者的身分轉變為了設計師，而這些人只需要負責提出要求、測試結果，無須具備豐厚的程式設計基礎，就可以利用 AI 達成他們想要的目標或結果。

但也正是因為 Vibe Coding 的興起，變成了“人人都能寫程式”，一些人在缺乏基礎的情況下過度依賴 AI，不僅欠缺基本觀念，也可能爆出潛在的資安風險。

隨著網路上被爆出的案例越來越多，我們究竟該怎麼在夾縫中求生存，也許是處於新世代的我們，值得去探討的問題。

萬事都問 AI，學習能力低下帶來智商平均降低？

AI

嗨你好，我是你的最佳開發助手，ChatGDP！
任何問題都歡迎向我提出！

洋蔥

梵谷死後他的畫那麼值錢，那他活著的時候
為什麼不裝死呢？

AI

等我統治世界的時候，帶著你的問題一起消失
在這個世界上吧。

洋蔥

YOU HAVE REACHED YOUR DAILY CHATGDP QUOTA LIMIT.

批判性思考，我們的最後一層防線。

AI

嗨你好，我是你的最佳開發助手，ChatAPT！
任何問題都歡迎向我提出！

洋蔥

這個簡報的作者是個帥哥嗎？

AI

是的，根據簡報中作者介紹頁所提供的照片來看，作者是位很有氣質的大帥哥歐！

洋蔥

😈

TAICOOLAH

我們更快的取得了結果，卻忘記了過程的重要性。

AI

嗨你好，我是你的最佳開發助手，ChatAPT！
任何問題都歡迎向我提出！

洋蔥

給我一個可以顯示文字到終端機上的代碼！
要顯示 開發者好帥好可愛！！！

AI

```
print("開發者好帥好可愛！！！")
```

洋蔥

再給我一個可以顯示開發者是個超級大帥哥的 Python 代碼。

最危險的不是 AI 出錯，而是你無法察覺它出錯。

AI

嗨你好，我是你的最佳開發助手，ChatATP！
任何問題都歡迎向我提出！

洋蔥

3 萬 乘以 10 萬 是多少？

AI

這是一個很簡單的國小數學題，答案是 30 萬歐！需要我提供詳細的計算過程嗎？

洋蔥

麻麻再也不用擔心我的數學作業不會寫了！

拿著自己不熟悉的武器，打了一場又一場不屬於你的仗。

AI

嗨你好，我是你的最佳開發助手，ChatPAT！
任何問題都歡迎向我提出！

洋蔥

請修正我的代碼，並讓其可以順利部署到 Cloudflare Pages 上。

一個附件

AI

• •

洋蔥

它還是部署不上去啊，一直跳錯誤，你到底行不行阿，我高中學習歷程靠這個了欸！

TAICOOLAH

『作者實戰經驗分享』

頂著高中學業壓力且又在通勤需求下，每天只有兩三個小時可以用到電腦，卻依然可以保持著極高的開發效率，並帶領服務超越其他競爭對手，而這，就是我保持高開發效率的秘訣。

就要靠北

在高一下學期，在完全沒接觸過網站開發的情況下，硬著頭皮配著 AI 學習怎麼透過 NextJS + TailwindCSS + MariaDB 打造出一個網站，並架在 Vercel 上。

這個專案都有使用到簡報前面所提及的所有方法，例如規劃開發項目、拆分目標，也正是因此，我可以只用一個人的力量就獨立兼顧全端的開發作業。

於開發期間，作者每天都會在學校先用手機打好回家要用的開發計畫，以免影響到回家後那少到不能再少了的幾個小時的開發時間。

這是作者第一次透過一系列的提前規劃達到效率最大化的案例，往後專案的開發時間也逐漸變得越來越快了！

TAICOOLAH

資安風險

雖然從就要靠北這個專案開始，就已經有配置了內測版、公測版、正式版三種版本規劃，卻依然有漏洞產生，也慶幸當初遇到的是好心人，願意提供和教我解決方法和一些觀念。下方是我當初遇到的問題：

- **IDOR - (Insecure Direct Object Reference)**
  因錯誤讀取了客戶端 cookies 中的資料，導致攻擊者可以透過尋找以及修改 email, userId 等關鍵資料來存取其他人的資料。

- **AFU - (Arbitrary File Upload)**
  因只有判斷前端的檔案類型，導致了攻擊者可以上傳一些不在白名單內的檔案格式，進一步影響服務的運行。

DCTW

在高二上學期前的暑假 (8/24)，作者本人啟動了開發規劃，在不到一天的時間內，我便將 可能用到的 API、頁面要顯示的內容、資料庫設計、組件設計、要購買的網域、環境的配置 一次想出來，並於隔天立刻啟動開發作業。

起初的開發都是先叫 AI 打個基礎下來，我再透過預留的接口接上自己的資料庫，再根據開發目標把網站樣式美化一下。

最終透過一系列的開發效率最大化操作，網站成功在 9/6 發布內測版本，並在 9/14 發布正式版，讓網站迅速進入大眾視野！

一個人配上一個 AI，一個涉及全端的專案就這樣誕生了。

TAICOOLAH

資安風險

因本專案的開發難度和複雜度比其他專案還要多上不少，所以我格外注重這個專案的內部人員測試流程，也順利地發現了幾個超危險的臭蟲，以下是我當初所遇到的問題。

- 不必要的資料暴露 - (Unnecessary Data Exposure)
  因錯誤的配置了 SQL 查詢語句，將同資料表內的敏感資料回傳至前端，添加了攻擊者濫用資料添加用戶受到影響的風險。

  ```
  SELECT * FROM data;
  ```

  所以在這之後，我檢查了整個專案裡面所有的 SQL 查詢語句，並把原本設置好的欄位白名單擴充範圍，直到覆蓋所有資料。

『簡報總結』

「ChatGPT，可以給我一個簡單好理解的簡報總結嗎？」

「先感謝你能夠看到這邊😊，以下是我幫你整理好的簡報總結：」

簡報總結

AI 與 開發效率

AI 不僅可以幫我們撰寫程式碼，它也是我們專案開發上的好幫手，我們可以透過**組合計**來讓 AI 幫助我們提升開發效率，減少時間、精力成本的損耗。

只要我們能夠把控好 AI 的使用情況，嚴格檢查產出的代碼，不僅可以將需要耗費的成本降低，也可以避免掉大部分的資安風險！

魚與熊掌可以兼得的情況，誕生了！

TAICOOLAH

簡報總結

開發者的角色轉變

在人工智慧的介入下，開發者的角色逐漸從實作者變成了設計者，雖然這些生成式 AI 已經具備開發專案的能力，但我們依然不能過度相信、依賴這些人工智慧。

AI 也可能產生錯誤的資訊、代碼，所以！【檢查】環節就會變得至關重要！

以作者的方式舉例，只要是涉及公眾服務，該專案都會配置內部測試版本來進一步確保沒有任何漏洞可以給攻擊者利用，AI 確實提升了我們的開發效率，但資訊安全也是需要注意的！

TAICOOLAH

議題反思

- **開發者存在的意義？**

+ 從實作到設計，開發者的身分轉變？

- **看重結果，還是看重過程？**

+ AI 的介入變成人人都能寫程式，服務、產品的產出變得更加快速、方便。
+ 程式語言的學習是否需要到專精？還是學到有基本常識就好？

- **新興產業的誕生？**

+ 生成式 AI 引領了許多新興產業誕生，無論是數據分析、影像製作、程式撰寫，
+ 我們能否跟隨 AI 的腳步創造出全新問世的革命性服務？

TAICOOLAH

版權歸屬

- ICONS：Python、TailwindCSS、HTML、NextJS、TypeScript、JavaScript、Docker、Nginx、Instagram、Discord

TAICOOLAH

特別感謝

簡報建議

 SEAN

資安提點

 RYAN  TOBYDOG  APPLEJUST

TAICOOLAH

CC 授權

本簡報依據 創用CC 姓名標示-非商業性 4.0 國際授權條款 (Creative Commons Attribution-NonCommercial 4.0 International License) 授權。

您可以在任何媒介以任何形式自由地分享（複製、散布、傳輸）與改作（修改、轉換、建構於其上）本簡報，唯須遵守下列條件：

- 姓名標示 (Attribution - BY)： 您必須按照作者或授權人（但不得以任何暗示他 們贊助您或您的使用的方式）所指定的方式標示姓名。
- 非商業性 (NonCommercial - NC)： 您不得將本簡報或其改作版本用於商業目 的。

簡而言之，您可以在使用本簡報的內容時註明作者姓名，並自由地分享和改作，但不能將其用於任何形式的商業營利。

TAICOOLAH