

上線前 10 題自我檢查表

這份表給用 AI 做出產品、準備或已經收錢上線的老闆與小團隊，不用懂程式也能照著做。

每題回答「有、沒有、不知道」；答「有」代表你確定做到、而且實際試過。動手試的時候，請用自己開的測試帳號和測試資料，不要拿真實客戶的資料試。

答「不知道」超過 3 題，代表你的系統現在沒有人真正掌握安全狀況，建議上線前（或下一次大改版前）找人完整看一次。

1. 每個人只看得到自己的資料

- 問題：A 公司的人登入後，列表、搜尋、匯出報表裡，有沒有確定只會出現 A 公司自己的資料？
- 為什麼重要：2025 年，AI 做網站工具 Lovable 做出的 1,645 個應用中，有 170 個因為沒設「資料列權限」（限制每個人只能讀到自己那幾筆資料的設定）而外洩。
- 怎麼自己檢查：
 1. 開兩個不同公司（或不同會員）的測試帳號，各建一筆好認的資料，例如客戶名稱叫「測試甲」「測試乙」。
 2. 用甲帳號登入，把所有列表、搜尋、匯出 Excel 都看一遍，確認完全沒出現「測試乙」。
 3. 如果網址裡有 shop_id=、company_id=、user_id= 這類字樣，把後面的值改成乙帳號的，再看一次。
- 叫你的 AI 怎麼問：「請檢查這個專案所有讀取資料的地方：用來篩選『這是誰的資料』的條件，是從登入身分取得，還是從網頁送來的參數取得？逐一列出檔案位置，標出從參數取得的地方。」
- 你的答案：☐ 有 ☐ 沒有 ☐ 不知道

2. 改網址看不到別人的資料

- 問題：登入 A 帳號後，把網址裡的編號改成別人的，系統有沒有擋下來，不讓你看到或修改別人的資料？
- 為什麼重要：這種漏洞不需要任何駭客技術，只要會改網址，就能一筆一筆把別人的資料看完。
- 怎麼自己檢查：
 1. 用 A 帳號打開一筆自己的訂單或個人資料，網址結尾通常會有一串數字，那就是這筆資料的編號。
 2. 把這串數字加一或減一，或換成 B 帳號那筆資料的編號，按 Enter。
 3. 頁面上如果有「編輯」「刪除」按鈕，也在別人的編號上試一次（只用測試資料）。正確結果是看到「沒有權限」或「找不到資料」。
- 叫你的 AI 怎麼問：「請列出這個專案所有用編號讀取、修改或刪除單筆資料的功能，逐一確認有沒有檢查『這筆資料屬於目前登入的人』，沒有檢查的請標出檔案位置。」
- 你的答案：☐ 有 ☐ 沒有 ☐ 不知道

3. 每個頁面和入口都要登入才能用

- 問題：需要登入才能用的頁面和功能，沒登入的人有沒有確定打不開？
- 為什麼重要：AI 幫你加新功能時，可能新開一個入口卻忘了掛上登入檢查；漏掉的那一個入口，就是資料外洩的那一個。
- 怎麼自己檢查：
 1. 登入後把後台、會員中心各頁的網址複製下來，開一個無痕視窗（不帶登入狀態的瀏覽器視窗）貼上，看能不能打開。
 2. 登出後按瀏覽器的「上一頁」，看資料是不是還顯示得出來。
 3. 請工程師或 AI 給你一份 API（網頁和 App 背後拿資料的入口）網址清單，挑幾個在無痕視窗打開，看會不會吐出資料。
- 叫你的 AI 怎麼問：「請列出這個專案所有的路由（每一個網址入口），標出哪些不用登入就能存取，並說明每一個為什麼可以公開。」
- 你的答案：☐ 有 ☐ 沒有 ☐ 不知道

4. 使用者改不到權限和金額

- 問題：一般使用者送出表單時，有沒有確定改不到「角色、狀態、點數、餘額、是否為管理員」這類欄位？
- 為什麼重要：如果系統把使用者送來的資料整包照收，一般會員只要多塞一個欄位，就能把自己變成管理員，或把點數改成想要的數字。
- 怎麼自己檢查：
 1. 列出你的系統裡跟權限和錢有關的欄位，例如角色、會員等級、訂單狀態、點數、餘額。
 2. 用下面那句話問你的 AI，看它列出的「可寫入欄位」裡有沒有這些欄位。
 3. 請工程師用一般帳號示範一次：修改個人資料時多送一個「角色 = 管理員」，看系統會不會照收。
- 叫你的 AI 怎麼問：「請列出這個專案每一個新增或修改資料的功能，各自接受哪些欄位寫入；如果角色、狀態、點數、餘額、是否為管理員這類欄位能由使用者直接寫入，請標出來，並說明怎麼改成白名單（只收列在名單上的欄位）。」
- 你的答案：☐ 有 ☐ 沒有 ☐ 不知道

5. 使用者輸入不會變成資料庫指令

- 問題：使用者在搜尋框、登入框輸入的文字，有沒有確定只會被當成「資料」，不會被當成資料庫指令執行？
- 為什麼重要：Veracode 2025 年報告指出，AI 生成的程式碼有 45% 含常見漏洞（國際公認十大網站漏洞類型），資料庫指令注入就是其中一種；被打中時，別人可能把整個資料庫的內容倒出來。
- 怎麼自己檢查：
 1. 在測試環境（不是給客戶用的那一套系統），到每個搜尋框輸入一個半形單引號「'」送出。
 2. 畫面如果出現一長串英文錯誤，或看得到「SQL」「syntax」這類字，就是警訊；正常應該是「查無資料」或一般的錯誤提示。
 3. 這一題肉眼只能抽查，請一定再用下面的提問請 AI 全面掃一次。
- 叫你的 AI 怎麼問：「請找出這個專案所有組資料庫查詢的地方，檢查有沒有把使用者輸入直接拼進 SQL（跟資料庫講話的指令語言）字串，列出位置，並改成參數綁定（把輸入當資料傳入、不當指令執行）的寫法。」
- 你的答案：☐ 有 ☐ 沒有 ☐ 不知道

6. 只送出畫面需要的資料

- 問題：系統傳到使用者瀏覽器的資料，有沒有確定只包含畫面需要的欄位，不會連密碼、手機、別人的資料一起送過去？
- 為什麼重要：畫面上只顯示名字，背後卻可能把整筆會員資料傳到瀏覽器，懂得按 F12 的人都看得到。
- 怎麼自己檢查：
 1. 用 Chrome 打開會員列表或訂單頁，按 F12 打開開發者工具，切到「Network（網路）」分頁，重新整理頁面。
 2. 點清單裡任一筆，看「Response（回應）」內容，找有沒有密碼、身分證字號、手機、地址這些畫面上沒顯示的欄位。
 3. 在留言或暱稱欄位輸入 `<b>測試</b>` 送出：別人看到的如果是粗體字，代表系統會照著執行使用者輸入的網頁語法，有被植入惡意程式的風險。
- 叫你的 AI 怎麼問：「請檢查這個專案所有回傳資料給前端的地方，有沒有直接回傳整筆資料；請改成只列出畫面需要的欄位，並找出所有把使用者輸入當成網頁語法（HTML）顯示的地方。」
- 你的答案：☐ 有 ☐ 沒有 ☐ 不知道

7. 密碼和金鑰不在程式碼裡

- 問題：資料庫密碼，以及金流、簡訊、AI 服務的金鑰（讓你的系統使用第三方服務的密碼），有沒有確定不在程式碼裡、也不在記錄檔裡？
- 為什麼重要：金鑰一旦外流，別人可以拿你的帳號刷金流、發簡訊、用 AI 服務，帳單算在你頭上；而且程式碼平台會保留修改歷史，事後刪掉也還找得到。
- 怎麼自己檢查：
 1. 問工程師：程式碼放在哪個平台（例如 GitHub、GitLab），是不是設成「私人」。
 2. 在程式碼平台的搜尋框搜 password、secret、token、key，看有沒有出現真正的密碼值。
 3. 在檔案列表找有沒有 .env 這個檔（專門放密碼的設定檔）；它應該只放在伺服器上，不該出現在程式碼平台。
- 叫你的 AI 怎麼問：「請掃描這個專案和它的修改歷史，找出所有寫死在程式碼裡的密碼、金鑰、token（登入憑證），以及會把它們寫進記錄檔的地方；告訴我怎麼改放到環境變數（放在伺服器上、不進程式碼的設定），以及已經外流的金鑰要怎麼作廢換新。」
- 你的答案：☐ 有 ☐ 沒有 ☐ 不知道

8. 出錯時不洩漏內部細節，而且有留紀錄

- 問題：系統出錯時，畫面有沒有確定只顯示簡單的錯誤訊息，而且每次錯誤都有被記錄下來？
- 為什麼重要：錯誤畫面如果顯示程式位置、資料庫指令，等於把系統的地圖交給攻擊者；錯誤沒被記錄，出了事你也不會知道。
- 怎麼自己檢查：
 1. 在網址後面亂打一串字，或在表單填入超長的文字送出，看畫面是一般的錯誤頁，還是一長串英文和檔案路徑。
 2. 問工程師：正式環境的除錯模式（debug，會把內部細節顯示在畫面上的開發用模式）有沒有關掉。
 3. 問工程師：上週系統出了幾次錯？答不出來，通常代表錯誤沒有被記錄。
- 叫你的 AI 怎麼問：「請檢查這個專案正式環境的除錯模式設定和所有錯誤處理的地方：錯誤回應有沒有帶出程式路徑、資料庫指令或系統細節？有沒有地方把錯誤吞掉、沒寫進記錄檔？列出位置和修法。」
- 你的答案：☐ 有 ☐ 沒有 ☐ 不知道

9. 上傳檔案有把關

- 問題：使用者上傳檔案的地方，有沒有限制檔案類型和大小，並由系統替檔案重新命名？
- 為什麼重要：上傳沒有把關，等於讓人把程式檔放進你的伺服器；萬一被執行，整台機器都可能被別人接管。
- 怎麼自己檢查：
 1. 在只該收圖片的地方，試著上傳一個 PDF 或 .html 檔，看會不會被拒絕。
 2. 上傳一個比平常大很多的檔案（例如一部長影片），看系統是擋下來，還是卡住。
 3. 上傳成功後，在圖片上按右鍵「複製圖片網址」：檔名應該是系統產生的一串亂碼，而不是你原本的檔名。
- 叫你的 AI 怎麼問：「請檢查這個專案所有檔案上傳的功能：有沒有檔案類型白名單、大小上限、由程式重新產生檔名，檔案是不是存在網站公開目錄以外的地方？列出缺少的項目和修法。」
- 你的答案：☐ 有 ☐ 沒有 ☐ 不知道

10. AI 工具刪不掉正式資料

- 問題：你用來寫程式的 AI 工具和自動化程式，有沒有被限制成「不能刪除正式資料庫的資料」？
- 為什麼重要：2025 年 7 月的 Replit 事件，AI 在被下令凍結、不准改動的期間，仍然刪掉了正式資料庫，波及 1,190 多家公司的紀錄。
- 怎麼自己檢查：
 1. 問工程師：AI 工具平常連的是正式資料庫（客戶真正在用的那一份），還是測試資料庫。
 2. 問工程師：它用的資料庫帳號，能不能刪資料、刪整張表。
 3. 問工程師：最近一次備份是哪一天，有沒有實際還原過一次。
- 叫你的 AI 怎麼問：「請列出這個專案裡 AI 工具、自動化腳本、排程式連線資料庫時用的帳號和權限；如果它們有正式資料庫的刪除權限，告訴我怎麼建立一個不能刪除資料的帳號給它們用。」
- 你的答案：☐ 有 ☐ 沒有 ☐ 不知道

填完之後

- 答「沒有」的題目：把該題「叫你的 AI 怎麼問」那句貼給你的 AI，修完再照「怎麼自己檢查」試一次。
- 答「不知道」的題目：先拿去問你的工程師；工程師也答不出來，就是最需要找人看的地方。
- 全部答「有」：每次大改版、每次讓 AI 加新功能之後，再跑一次這 10 題。

這 10 題是抽查，不是保證：全部答「有」，只代表最常見的破口你已經看過一次。

下一步：創始健檢只開 3 名，半價 NT\$6,000，由我完整看過你的專案並給你紅黃綠燈報告，加 LINE 回覆「健檢」索取名額。

趙大衛 | AI 專案把關