Orange Tsai

蔡政達的漏洞研究、台灣駭客社群與國際揭露工作

Orange Tsai，本名蔡政達，是台灣資安公司戴夫寇爾（DEVCORE）的首席資安研究員，也是 CHROOT 資安社群的核心成員。他的工作，是找出軟體原本不該允許、卻實際做得到的事情，再把發現整理成廠商能修補、同行能檢驗的研究。讓他受到國際注意的成果，包括企業 VPN、微軟 Exchange 郵件伺服器、Apache 網頁伺服器，以及 Microsoft Edge 瀏覽器的漏洞。這些東西多半不在使用者眼前，卻負責企業通訊、遠端工作和網站運轉。[1, 2]

他的職涯從台灣高中生的自學與駭客競賽起步，穿過輔大的學生社團、跨校戰隊和本地資安公司，逐漸進入國際漏洞通報、技術會議與產品安全研究的網絡。一路上，競賽選手、顧問、研究者、講者與作者幾種角色交疊。螢幕上一次成功的示範，可能只花幾秒；它背後則有幾個月的閱讀與失敗、同事互補的專長，以及找到問題後仍未結束的協調工作。

讀他的文章，會發現一種特別的反差：技術對象愈來愈重大，文字卻仍保留早年部落格的表情符號、自嘲和興奮。2010 年他寫上大學的消息，才說完高興，下一段已經轉去討論自己為什麼解不出一道題。十多年後，他寫獲獎研究，仍會交代最初嫌棄某個發現沒有用、暫時把它擱下的經過。這些紀錄讓人看見，成果不是從已知答案倒推的一條直線。[3, 4]

高中生、輔大社團與台科大，2007–2013

蔡政達在 2021 年回顧自己的養成時，把一則 2007 年底的駭客新聞列為轉折：電視上的人物讓他開始嚮往這種能力。之後他主動聯繫翁浩正（Allen Own），以高中生身分每週前往輔仁大學的 NISRA 學習；2009 年拿到 HITCON Wargame 冠軍，也讓這個興趣第一次帶來明顯的同儕認可。[5]

NISRA 是輔大資工學生在 2007 年發起的自學團體。它留下的歷史不是一份完整課表，而是寒假特訓、社群講座、比賽與跨校隊伍的活動紀錄。2010 年有「台科大分舵」，2011 年同名隊伍在金盾獎拿下冠軍。這種命名帶著玩笑，卻也準確描述知識怎麼流動：加入的門檻不完全由學籍決定，學長、社團與共同解題，把原本分散在不同學校的人接在一起。[6]

2010 年 4 月 6 日，蔡政達在部落格同時記下升學與講課的壓力。他正在申請台科大不分系及市北教資科，準備到中研院 OSSF 講課，又擔心自己的高中學分。他剛借到一本漏洞分析的書，覺得其中的思考方式非常好玩。這篇短日記裡，進入專業社群和順利高中畢業，還是兩件並行、未必互相配合的事。[7]

5 月，他寫下台科大備取錄取。緊接著的內容是：同一道練習題，在自己的伺服器上為何得到不同結果？最後發現是編譯器版本及保護機制的差異。這不是後來成名後整理的勵志故事，而是當時留下的小紀錄。大學錄取很重要；使他繼續寫下去的，仍是兩個環境之間那個尚未解釋的不同。[8]

到 2013 年，PyCon Taiwan 的講者介紹已把他列為研究網站與 Windows 安全的大學生，講題是從駭客的角度看 Django。對他而言，會議不是完成學業後才取得的資格。當學生的同時，他已在學習把自己理解的技術說給開發者聽。[9]

CHROOT、HITCON 與跨校戰隊

這個成長環境還有一層較早的歷史。CHROOT 在 2004 年形成，成員後來辦起台灣駭客年會 HITCON。早期活動介紹直接回應「駭客等於犯罪者」的社會印象，希望提供公開的技術交流場所。這不是說社群消除了所有界線問題，而是它試著建立一種可以教、可以辯論、可以共同評價的實踐。[10]

CTF，亦即 Capture the Flag，是這套世界的重要活動：在限定環境中解題、突破主辦者設計的限制，取得稱為 flag 的通關證明。它與真實企業入侵不同，規則和授權範圍由比賽事先設定。也正因為場地被框起來，參賽者可以集中追問奇特問題，而不必把任何陌生網站都當成試驗品。

Orange 在 2017 年的訪談中描述，HITCON 戰隊結合了 CHROOT、台大的 217、交大的 Bamboofox 與中央大學等不同群體。那是當時的組成，並非一支永遠固定的名單。它讓資安人才的地圖超過單一明星：有人熟悉記憶體與系統，有人擅長密碼、逆向工程或網站。全隊的能力來自分工，也來自解不出來時能把問題交給誰。[11]

他在 2025 年的《Phrack》回憶中，估計自己參加過兩百多場 CTF，並記得與隊友在教室通宵、在賽後探索陌生城市。國際競賽的履歷之外，還有一段共同生活的經驗。[12]

他的 PHP 長文也把競賽題目和產品研究接在一起。從這種編排可以看出，CTF 留下的成果不只有名次：它也保存了可供後來研究重新使用的技術問題。[13]

在 DEVCORE，把研究變成工作

目前公開的早期資料，至少可以確認：2015 年 HITCON 的講師介紹已列他為 DEVCORE 資安顧問。當年的企業課程由他教授網站安全相關技術，社群場次則談網站攻防中容易被忽略的特殊行為。這時他已同時面對兩種聽眾：需要學會方法的企業學員，以及會追問新意和細節的同行。[14, 15]

DEVCORE 提供紅隊演練、滲透測試、產品安全研究與教育訓練。紅隊演練是在授權的目標與限制內，模擬對手能如何達成指定目的；產品研究則可以跨越單一客戶，檢視很多組織共同依賴的軟硬體。依公司的研究部門介紹，研究成果也會回流到演練能力。這個組織安排，使深入研究和商業服務之間有了通道。[16]

對 Orange 的職涯來說，公司提供的不只是名片上的頭銜。企業研究經常要取得設備、建置測試環境、支付長期人力，又不保證每個月都有足以發表的成果。從公開業務與研究的並存，可以理解這種職位如何被容納；但公司沒有公開他的薪資、個別研究成本或各業務的補貼比例，不能把得獎金額當成他的年收入。

他在 Bug Bounty Forum 的問答中，甚至把漏洞獎勵計畫稱為嗜好，說自己更喜歡研究：研究卡住，或碰到某種有趣設計時，才可能轉去找適合的獎勵計畫。這是那次訪談的自我描述，不宜套用為每一年的工時表，卻能修正一個常見誤解：他的日常不是不停掃描網站、用漏洞件數換獎金。[17]

授權界線也是在這段過程中變得具體。他曾公開承認，年輕時對實際服務的試探，雖然事後回報，仍造成企業困擾；進入公司後，也意識到這可能連累同事與公司聲譽。他在 2021 年談這件事時明確不鼓勵效法。這段反省值得保留，因為它使今天的「白帽」身分不只是一個替早年行為自動免責的標籤。[18]

Facebook 與 GitHub：從網站表面走進產品內部，2016–2017

2016 年，Orange 發表了研究 Facebook 所使用檔案傳輸系統的文章。真正的對象不是動態消息頁面，而是企業採購的第三方產品。他注意到先前漏洞公告透露的程式線索，接著研究產品內部，最後把發現通報 Facebook 與供應商。公開時間表顯示，他在 2 月通報，依 Facebook 要求暫緩文章，直到 4 月調查完成後才發表。[19]

這個案例裡最重要的職業動作，是在「知名網站」背後辨認出實際運作的產品。使用者看到的是一個品牌；研究者要拆開的，則是一組採購、整合與維護關係。一家企業可以把主要網站做得很好，仍必須面對外部軟體帶進來的風險。Orange 後來愈來愈常研究企業共同使用的基礎產品，這種視角在此已經清楚。

2017 年的 GitHub Enterprise 研究進一步顯示他的長處。成果不是找到一個單獨、明顯致命的錯誤，而是把四項問題串成能在伺服器執行程式的路徑。其中涉及不同元件對同一段資料的處理，以及網站替使用者向其他服務發出請求的能力。這類問題的困難，在於單看一個環節，危害可能有限；連起來才看得出信任如何被逐步借用。[20]

可以把這種研究想成追蹤一份文件在機構裡流轉：第一個窗口確認了一項條件，第二個窗口卻以為所有條件都已確認；最後拿到的權限，超過最初那次確認應該允許的範圍。研究者必須逐段驗證這些交接，找出權限從哪裡開始超出預期。

這也是 Orange 第一次為 Black Hat USA 與 DEF CON 準備正式英語演講的時期。他在文章開頭說，為兩場發表準備了數月。對外呈現一條簡潔的研究脈絡，需要另一套勞動：把反覆繞路的過程重整，讓不曾陪他讀程式的人，也能理解為什麼這些小問題會連成大問題。[21]

和 Meh Chang 研究 VPN，2018–2019

VPN 原本用來讓員工安全地連回企業。這使它成為一個特殊研究對象：它站在外部網路與內部工作環境的交界，而人們往往正因為信任它的保護功能，才讓它站在那裡。

Orange 與同事 Meh Chang 合作研究企業 SSL VPN。以兩人公開的 Pulse Secure 紀錄為例，工作從 2018 年 12 月開始，前兩個月沒有得到結果；2019 年 3 月才找到突破，3 月通報，4 月供應商推出修補。這和他們研究另一家產品時很快得到成果的經驗形成對照。同一批研究者、同一類產品，時間成本仍可能非常不同。[22]

成果把幾個較小的問題連接起來，影響到企業入口設備的安全。比技術勝利更難處理的，是何時公開。兩人在文章裡交代，團隊曾為了讓使用者有時間更新而延後細節；但修補推出後，其他人也會開始研究差異、發表自己的發現。研究者能選擇自己的時間表，卻無法控制所有人同步等待。[23]

從這裡開始，Orange 研究的利害關係更鮮明。漏洞通報是改善安全的一環，漏洞知識本身卻也能被攻擊者使用。研究、修補、部署與公開之間，每一個時間差都有不同承擔者：原廠要改程式，企業要安排更新，研究者要維持可驗證的成果，又不能假裝世界會停下來等自己。

Exchange：研究完成之後的危機，2020–2021

微軟 Exchange 是企業自行架設郵件系統時使用的產品。Orange 在 2020 年已研究這套系統，2021 年 1 月通報後來被稱為 ProxyLogon 的漏洞。就他的原始技術說明來看，核心問題涉及前端與後端之間的代理及信任關係：外部請求如何被系統內部接手，而接手後又被當成什麼身分。[24]

這是多年企業軟體演變留下的複雜環境。新版本必須支援舊有功能，模組與服務必須互相交談。對正常使用者來說，這些細節應該被藏起來；研究者卻必須重新畫出它們的關係，尋找不同部分對身分、位置或權限的理解在哪裡分岔。

2021 年 3 月 2 日，微軟緊急推出更新，並公開說明有攻擊者正在利用 Exchange 漏洞。微軟最初的公告將已觀察到的特定攻擊歸於 HAFNIUM，後續又指出其他組織也在利用相關漏洞。這是惡意攻擊的紀錄，不能與向微軟通報問題的 Orange 混為一談。[25, 26]

但這個區分當時並未始終保住。3 月 18 日的 iThome 專訪記載，他和公司遭遇把研究者當成攻擊者的報導。Orange 說，一個多星期裡，他和主管每天只睡三、四小時，醒來就查看問題、回覆詢問。這個階段的工作已不是安靜分析軟體，而是處理誤解、釐清時序，以及在全球事故中說明自己究竟做了什麼。[27]

外界對攻擊工具如何流出有過猜測，但現有這些材料不足以據此判定洩漏責任。可以確認的是，通報、原廠修補、惡意利用及公開研究，是不同事件。把它們壓成「他找到了洞，所以他導致災情」，既忽略其他攻擊者可能獨立發現問題，也抹去防禦者獲得修補所需的研究工作。

同年他還發表 ProxyShell 等 Exchange 研究。名稱相近不代表是同一條漏洞鏈，也不能把所有修補日期合為一次。研究持續往系統架構深處走，卻已不能只按技術難度衡量成敗：一次發現可能同時使他得到國際聲譽，並帶來他無法獨自控制的公共後果。[28]

工作檯上的選題、同事與失敗

理解這份工作，最好先放下「每天找到多少漏洞」的想像。他的一篇 Jenkins 研究說明，自己會先根據產品用途、框架與可能影響，挑出值得深挖的部分。Jenkins 是協助軟體建置與交付的工具，往往能接觸程式碼與部署流程；因此，某個看似只是管理介面的問題，可能有超過頁面本身的影響。選題已包含對企業運作的判斷。[29]

而找到可疑之處後，工作未必立即前進。他在公開問答中提到的資訊來源包括 RSS、社群動態與程式碼分享平台；與其囤積固定測試字串，更重要的是理解特定環境為何產生某種行為。這是一種需要持續更新的閱讀工作。新框架、舊公告、別人的失敗和一段不尋常的程式，可能在很久以後才產生關聯。[30]

2023 年，他和 Angelboy 共同發表的 Pwn2Own 經驗談，則把研究的後勤攤開：如何選目標，如何取得設備，真實硬體與模擬環境有什麼差別，以及競賽規則怎麼影響準備。產品運送、版本變動、漏

洞是否已被別人找到，都可能改變一項成果的比賽價值。報名一個目標，並不等於到了現場只剩按下按鈕。[31]

兩人在簡報裡還用角色扮演遊戲比喻研究員的不同專長。玩笑背後是很實際的配置：Orange 的網站與邏輯研究，可以和擅長底層利用、裝置分析或其他領域的同事互補。現在的研究團隊也包括 splitline、HexRabbit 等其他研究者；具體專案仍須看署名，不能把每件成果都算成 Orange 個人作品。[32, 33]

他自己也持續當學生。2025 年分享 OSEE 高階安全認證考試經驗時，他以網站研究者的身分自嘲，承認自己對某些記憶體利用問題不如同事熟悉。文章同時提到研究、管理行政和準備考試相互擠壓。他寫了熬夜應試的狼狽，也提醒睡眠的重要。這些細節顯示，已有國際名聲的人仍有能力邊界，工作也不會自動替學習騰出完整空檔。[34]

Apache：讀懂模組之間的誤會，2024

2024 年的 Confusion Attacks，是 Orange 研究方法相當成熟的例子。Apache HTTP Server 是老牌網頁伺服器，由多個模組一起處理請求。他追查的不是某位開發者忘記檢查一個欄位，而是不同模組對共享資料的意義有不同理解：同一個欄位，在某處被當成一種東西，交給下一處時卻變成另一種。[35]

若用日常語言說，這像一張多年沿用的表格：不同單位都能讀它，各自也有熟悉的工作慣例，直到有人刻意構造一份讓各方理解不一致的內容，才暴露出整個流程沒有共同定義。每個模組各自運作合理，仍可能在組合時產生問題。

Apache 的官方安全公告確認了他回報的多項漏洞，以及 2024 年 7 月推出的相關修補。公告還特別提醒某些舊設定需要調整。這是成熟軟體修補的難處：使用者可能多年來都依賴原有行為，一旦把不安全的假設改掉，正常系統也得配合遷移。漏洞研究因此會碰到軟體維護的歷史負擔，不只是揭露一個孤立錯字。[36]

發表這項研究的同時，他還交代了另一種與程式碼無關的障礙：依他 2024 年的說法，自 2022 年起赴美所需的旅行許可一直不順，當年的簽證流程也未能讓他及時成行，最後以預錄方式參與 Black Hat USA。這是當時的個人紀錄，不能推定為今日仍有效的限制。它提醒我們，台灣研究者即使已被國際會議認可，能否親自到場仍受另一套行政條件影響。[37]

WorstFit：全球化軟體中的字元轉換，2024–2025

和 splitline 合作的 WorstFit，從 Windows 長期保留的字元轉換機制切入。現代軟體使用 Unicode，舊介面仍可能依賴不同語系的編碼。為了相容，系統有時會把無法直接表示的字元，轉成它認為最接近的形式。麻煩出在安全檢查與轉換不一定發生於同一層：前面認為普通的文字，後面可能讀成具有特殊意義的內容。[38]

這件事和 Orange 先前研究解析器差異的興趣相連，但多出一個容易被英語中心的技術想像漏掉的條件：語言環境本身。相同程式在不同系統編碼下，行為未必一樣。因此，單一測試環境裡的安全結論，不能不加條件地搬到所有使用者身上。

兩人的文章也明確回溯早年研究者對相關編碼問題的討論。WorstFit 的價值在於重新梳理、擴展並驗證這類行為如何出現在現代軟體鏈中，而不是宣稱此前沒有人想過字元轉換的風險。這也是成熟研究與競賽捷報的差別：新意需要把前人的工作交代清楚，才能說明自己究竟往前推了哪一步。[39]

講給開發者聽，也把舊知識留下來

Orange 的公開工作始終有兩種語氣：向專家交付足夠細節，也替不熟悉漏洞研究的人建立理解入口。2023 年回到 WebConf，他設定的目標很小：四十五分鐘不可能把所有防禦方法教完，只希望開發者下次碰到相似情況時，腦中能出現一個警告。[40]

這場演講把十年間的變化放在一起：網站架構增加代理與快取，框架承擔更多工作，資料經過愈來愈多次轉譯，原本分開的應用又被串接。從這些趨勢看，他的研究興趣並不只是偏愛稀奇技巧，而是追著開發方式的改變走。當系統把複雜度移到下一層，研究者也得往下一層讀。[41]

2025 年，他花半年寫作《Phrack》文章，在咖啡廳附近散步時繼續思考取捨。這次要完成的，已超過單項研究報告：他還得決定多年累積的經驗，哪些值得留下。[42]

2026 年的 Edge，以及團隊成績的尺度

2026 年 10 月，Orange 公開了他在 Pwn2Own Berlin 使用的 Microsoft Edge 研究。這次選擇的路徑以邏輯問題為主，沒有依賴記憶體毀損。完整說明把幾項漏洞與既有系統功能串在一起；其中一個早期發現，曾因看似用途有限而被他放在筆記裡。它的價值是在後續找到能連接的部分後，才變得清楚。[43]

這個案例延續了他從伺服器走向瀏覽器時仍保留的思考：追問資料和權限在交接後變成什麼，而不只問某一段程式會不會當掉。瀏覽器、網頁內容與作業系統之間本來就有多道界線；研究的證明責任，是讓每一次跨越都能被重現和檢查。它不是把過去的網站技巧原封不動搬過來，而是把已形成的問題意識，帶進另一個龐大的系統。

主辦方公布的結果確認，Edge 項目得到 17.5 萬美元與 17.5 分；隔天 Orange 的 Exchange 項目另得 20 萬美元與 20 分。最終 DEVCORE 以 50.5 分、合計 50.5 萬美元取得團隊冠軍，其中包含其他成員的成果。這些是賽事公布的獎金和團隊成績，不是他的個人實領或固定收入。[44, 45, 46]

他把 Edge 文章取了帶挑釁意味的名字，強調這次是手工完成、沒有使用 AI。這可視為他對該項研究過程的自我定位；它並不能證明 AI 無法做資安研究，更不能推出他在所有工作上拒絕 AI。前一年他已坦白說明用語言模型協助翻譯。把兩件事並讀，比替他製造一個全盤反對 AI 的形象，更接近公開紀錄。[47, 48]

截至 2026 年 11 月，Orange 仍以 DEVCORE 首席資安研究員身分工作，持續發表、講課與合作。他的個人網站把早年的短日記與長篇研究放在同一份檔案裡：升學、練習題、第一次英語發表、共同研究的時序、考試失敗風險，以及一項暫時看不出用途的小發現。這份職涯最具體的連續性，就留在那些尚不知道結果時寫下的材料中。[49]

延伸閱讀

第一次讀 Orange，可以先讀 2010 年的〈Note〉和 2021 年的生涯演講報導，認識這個人；再讀 2023 年 WebConf 回顧，掌握他如何向開發者說明問題。想理解研究實際怎麼展開，GitHub、Pulse Secure 與 Apache 三篇原始文章分別呈現漏洞組合、團隊時序與架構分析。它們含有專門技術細節，適合依自己的背景選讀，並遵守授權測試範圍。[50], [51], [52], [53], [54], [55]

本文依截至 2026 年 11 月 4 日可公開查閱的資料撰寫。早年經歷與工作感受多來自本人回憶；獎項、修補與現職則盡量用主辦方、軟體供應者及機構資料交叉核對。未據公開紀錄補寫私人生活、精確到職日期或個人收入。

來源

1. CYBERSEC 2021，〈Orange Tsai〉，官方講者資料，確認中文姓名、職務與社群身分。原頁。↩
2. Orange Tsai，〈About〉，個人介紹，查閱於 2026-11-04；研究與獎項列表須區分個人及團隊。原頁。↩
3. Orange Tsai，〈爽〉，2010-05-12，當時的錄取及解題紀錄。原文。↩
4. Orange Tsai，〈The Last Proof of Human Craft: Forging a Microsoft Edge Full Chain with Logic Bugs Only!〉，2026-10-28，第一手研究回顧。原文。↩
5. 翁芊儒，〈14 年玩成全球頂尖駭客，戴夫寇爾首席資安研究員親身分享 5 階段心路轉折〉，iThome，2021-05-25，報導本人演講；童年及心境屬回憶性敘述。原文。↩
6. NISRA，〈關於 NISRA〉，官方簡介與活動年表；部分歷屆幹部年份尚未確定，本文未據此推定 Orange 任職年份。原頁。↩
7. Orange Tsai，〈Note〉，2010-04-06，升學與 OSSF 講課準備紀錄。原文。↩
8. Orange Tsai，〈爽〉，2010-05-12，當時的錄取及解題紀錄。原文。↩
9. PyCon Taiwan 2013，官方講者頁，〈駭客看 Django〉及蔡政達介紹。原頁。↩
10. HIT 2005，〈Introduction〉，CHROOT 與初屆年會的自我介紹；屬主辦方歷史陳述。存檔原頁。↩
11. SSD Secure Disclosure technical team，〈Know your community — Orange Tsai〉，2017-01-01，人物訪談。本文採其社群與研究敘述，未將缺乏交叉核對的學位介紹納入正文。原文。↩
12. Orange Tsai，〈The Art of PHP — My CTF Journey and Untold Stories!〉繁中版，2025-08-27，為《Phrack》撰寫的技術與生涯回顧，含寫作及翻譯說明。原文。↩
13. Orange Tsai，〈The Art of PHP — My CTF Journey and Untold Stories!〉繁中版，2025-08-27，為《Phrack》撰寫的技術與生涯回顧，含寫作及翻譯說明。原文。↩
14. HITCON 2015，企業教育訓練官方介紹，講師與課程資料。原頁。↩

15. HITCON 2015 Community，〈Web Hacking 中的奇技淫巧〉，官方議程。原頁。↩
16. DEVCORE，〈Research Overview〉，現行研究部門與服務說明，查閱於 2026-11-04；商業安排為公司自述，非財務揭露。原頁。↩
17. Bug Bounty Forum，〈AMA with @orange_8361〉，未標示可靠發布日期，本文不把其中當時的習慣當成現行作息。原文。↩
18. 翁芊儒，〈14 年玩成全球頂尖駭客，戴夫寇爾首席資安研究員親身分享 5 階段心路轉折〉，iThome，2021-05-25，報導本人演講；童年及心境屬回憶性敘述。原文。↩
19. Orange Tsai，〈滲透 Facebook 的思路與發現〉，DEVCORE，2016-04-21；本文採產品研究與通報時序，未將文中第三方活動的身分判斷視為已定案。原文。↩
20. Orange Tsai，〈How I Chained 4 vulnerabilities on GitHub Enterprise, From SSRF Execution Chain to RCE!〉，2017-07-28，第一手技術與發表準備紀錄。原文。↩
21. Orange Tsai，〈How I Chained 4 vulnerabilities on GitHub Enterprise, From SSRF Execution Chain to RCE!〉，2017-07-28，第一手技術與發表準備紀錄。原文。↩
22. Orange Tsai、Meh Chang，〈Attacking SSL VPN — Part 3: The Golden Pulse Secure SSL VPN RCE Chain〉，2019-09-02，聯合研究、揭露與修補時間表。原文。↩
23. Orange Tsai、Meh Chang，〈Attacking SSL VPN — Part 3: The Golden Pulse Secure SSL VPN RCE Chain〉，2019-09-02，聯合研究、揭露與修補時間表。原文。↩
24. Orange Tsai，〈ProxyLogon: A New Attack Surface on Microsoft Exchange Server! (Part 1)〉，2021-08-06；研究者提供的架構分析與各漏洞鏈時間表。原文。↩
25. Microsoft，〈HAFNIUM targeting Exchange Servers with 0-day exploits〉，2021-03-02，官方攻擊觀察與修補公告；威脅歸因為微軟判斷。原文。↩
26. Microsoft，〈Analyzing attacks taking advantage of the Exchange Server vulnerabilities〉，2021-03-25，後續觀察。原文。↩
27. 黃彥棻，〈專訪戴夫寇爾首席資安研究員 Orange Tsai：微軟 Exchange 漏洞研究與通報歷程大公開〉，iThome，2021-03-18；事件中的本人及公司說法，本文未採未定案的洩漏責任推測。原文。↩
28. Orange Tsai，〈ProxyLogon: A New Attack Surface on Microsoft Exchange Server! (Part 1)〉，2021-08-06；研究者提供的架構分析與各漏洞鏈時間表。原文。↩
29. Orange Tsai，〈Hacking Jenkins Part 1 — Play with Dynamic Routing〉，DEVCORE，2019-01-16，選題與程式分析說明。原文。↩
30. Bug Bounty Forum，〈AMA with @orange_8361〉，未標示可靠發布日期，本文不把其中當時的習慣當成現行作息。原文。↩
31. Orange Tsai、Angelboy，〈From Zero to Hero：從零開始的 Pwn2Own 奪冠之路〉，DEVCORE Conference，2023-03-11，聯合演講投影片。PDF。↩
32. Orange Tsai、Angelboy，〈From Zero to Hero：從零開始的 Pwn2Own 奪冠之路〉，DEVCORE Conference，2023-03-11，聯合演講投影片。PDF。↩
33. DEVCORE，〈Our Team〉，現行人員與職務介紹，查閱於 2026-11-04。原頁。↩

34. Orange Tsai，〈從 Web 狗的視角看 OSEE：從 0.1 開始的 Advanced Windows Exploitation 考試〉，2025-07-02，應試與工作安排的第一手敘述。原文。↩

35. Orange Tsai，〈Confusion Attacks: Exploiting Hidden Semantic Ambiguity in Apache HTTP Server!〉，2024-08-09；技術分析及當年旅行許可情況。原文。↩

36. Apache HTTP Server Project，〈Apache HTTP Server 2.4 vulnerabilities〉，官方安全公告；參見 2.4.60（2024-07-01）相關條目及研究者致謝。原頁。↩

37. Orange Tsai，〈Confusion Attacks: Exploiting Hidden Semantic Ambiguity in Apache HTTP Server!〉，2024-08-09；技術分析及當年旅行許可情況。原文。↩

38. Orange Tsai、splitline，〈WorstFit: Unveiling Hidden Transformers in Windows ANSI!〉，2025-01-10，源於 2024 年 Black Hat Europe 的合作研究。原文。↩

39. Orange Tsai、splitline，〈WorstFit: Unveiling Hidden Transformers in Windows ANSI!〉，2025-01-10，源於 2024 年 Black Hat Europe 的合作研究。原文。↩

40. Orange Tsai，〈從 2013 到 2023：Web Security 十年之進化與趨勢！〉，2023-08-12，演講目的與分類為作者觀點。原文。↩

41. Orange Tsai，〈從 2013 到 2023：Web Security 十年之進化與趨勢！〉，2023-08-12，演講目的與分類為作者觀點。原文。↩

42. Orange Tsai，〈The Art of PHP — My CTF Journey and Untold Stories!〉繁中版，2025-08-27，為《Phrack》撰寫的技術與生涯回顧，含寫作及翻譯說明。原文。↩

43. Orange Tsai，〈The Last Proof of Human Craft: Forging a Microsoft Edge Full Chain with Logic Bugs Only!〉，2026-10-28，第一手研究回顧。原文。↩

44. Dustin Childs，〈Pwn2Own Berlin 2026 — Day One Results〉，Zero Day Initiative，頁面標示 2026-05-14，Edge 項目官方結果；網址路徑日期與顯示日期不同。原文。↩

45. Dustin Childs，〈Pwn2Own Berlin 2026 — Day Two Results〉，Zero Day Initiative，2026-05-15。原文。↩

46. Dustin Childs，〈Pwn2Own Berlin 2026 — Day Three Results and Master of Pwn〉，Zero Day Initiative，2026-05-16，最終團隊成績。原文。↩

47. Orange Tsai，〈The Last Proof of Human Craft: Forging a Microsoft Edge Full Chain with Logic Bugs Only!〉，2026-10-28，第一手研究回顧。原文。↩

48. Orange Tsai，〈The Art of PHP — My CTF Journey and Untold Stories!〉繁中版，2025-08-27，為《Phrack》撰寫的技術與生涯回顧，含寫作及翻譯說明。原文。↩

49. Orange Tsai，〈About〉，個人介紹，查閱於 2026-11-04；研究與獎項列表須區分個人及團隊。原頁。↩

50. Orange Tsai，〈Note〉，2010-04-06，升學與 OSSF 講課準備紀錄。原文。↩

51. 翁芊儒，〈14 年玩成全球頂尖駭客，戴夫寇爾首席資安研究員親身分享 5 階段心路轉折〉，iThome，2021-05-25，報導本人演講；童年及心境屬回憶性敘述。原文。↩

52. Orange Tsai，〈從 2013 到 2023：Web Security 十年之進化與趨勢！〉，2023-08-12，演講目的與分類為作者觀點。原文。↩

53. Orange Tsai，〈How I Chained 4 vulnerabilities on GitHub Enterprise, From SSRF Execution Chain to RCE!〉，2017-07-28，第一手技術與發表準備紀錄。原文。↩

54. Orange Tsai、Meh Chang，〈Attacking SSL VPN — Part 3: The Golden Pulse Secure SSL VPN RCE Chain〉，2019-09-02，聯合研究、揭露與修補時間表。原文。↩

55. Orange Tsai，〈Confusion Attacks: Exploiting Hidden Semantic Ambiguity in Apache HTTP Server!〉，2024-08-09；技術分析及當年旅行許可情況。原文。↩