KAELITH SECURITY GUIDE

Self-XSS 防護

不要讓控制台變成攻擊入口

整理控制台貼碼風險、前後端權限邊界、使用者提示、後端驗證與事件處理流程。

分類	閱讀時間	適用對象	版本日期
瀏覽器安全	7–9 分鐘	網站維護者、後台使用者、內容更新人員、高權限帳號使用者	2026-06-19

文件摘要

整理控制台貼碼風險、前後端權限邊界、使用者提示、後端驗證與事件處理流程。

使用範圍與維護原則

攻擊者通常不需要突破瀏覽器限制，而是誘導使用者打開開發者工具，把陌生指令貼進控制台。只要使用者當下已登入網站，指令就可能讀取頁面資料、呼叫前端可用功能或引導後續詐騙流程。

防護重點不是封鎖所有開發者工具，而是讓敏感操作必須經由伺服器端重新驗證，並讓使用者知道官方不會要求貼上控制台指令。

風險等級

中高

建議檢查頻率

每季檢查一次；若有主機、DNS、信箱或人員異動，應額外盤點。

02 / 攻擊情境

假教學與假客服最容易讓人降低戒心。

Self-XSS 常被包裝成官方教學或客服協助流程，要求使用者不要重新整理、不要中斷流程，甚至要求截圖確認。

如果任何人要求貼上陌生指令、複製 Cookie、輸入備援碼或在控制台執行程式碼，都應視為高風險行為。

項目	說明
誘導理由	領獎、修復帳號、解除限制、客服協助除錯
要求動作	開發者工具、控制台貼碼、複製 Cookie、提供備援碼
可能結果	帳號接管、權限濫用、資料外洩、後續詐騙

03 / 維護控管

敏感動作不能只靠前端按鈕控制。

前端顯示或隱藏按鈕只能改善使用體驗，不能作為權限判斷。涉及付款、權限、資料匯出、信箱或登入安全的操作，必須由伺服器重新檢查權限。

維護階段應檢查是否具備 CSRF 防護、重新驗證、操作紀錄與風險提示，避免前端狀態被直接呼叫。

伺服器重新驗證

重要操作必須在後端檢查身份、權限、來源與操作條件。

提示策略

提醒官方不會要求貼控制台指令，但避免誇張彈窗干擾正常流程。

04 / 事件回應

已執行指令後，優先撤銷工作階段。

若已貼上並執行陌生指令，應立即登出所有裝置、變更密碼、撤銷不明授權、檢查帳號安全設定。

管理者應檢視近期登入、操作紀錄、資料異動紀錄與可疑授權，並確認是否需要暫停高風險功能。

1. 登出所有裝置並變更密碼。
2. 撤銷第三方授權與可疑工作階段。
3. 檢查近期操作、資料異動與高權限行為。
4. 通知服務管理者並保存可疑指令與來源。

維護檢核

維護檢查清單

以下項目可用於定期維護、權限盤點或事件回應前的初步確認。

- 官方說明是否明確表示不會要求使用者貼控制台指令。
- 敏感操作是否由伺服器端重新驗證權限。
- 重要操作是否有 CSRF 防護、重新驗證與操作紀錄。
- 管理後台是否降低把權限暴露在前端狀態中的機率。
- 是否有登出所有裝置、撤銷授權與檢查近期操作紀錄的流程。

本文件由 Kaelith 數位開發整理，供網站維護、帳號安全與日常風險控管參考。實際處理仍應依主機商、DNS 供應商、信箱服務與系統權限條件調整。