提升網絡安全意識及資訊科技應用能力分享會

Horace Ma
Head of Public Mission – Cybersecurity
2026.01

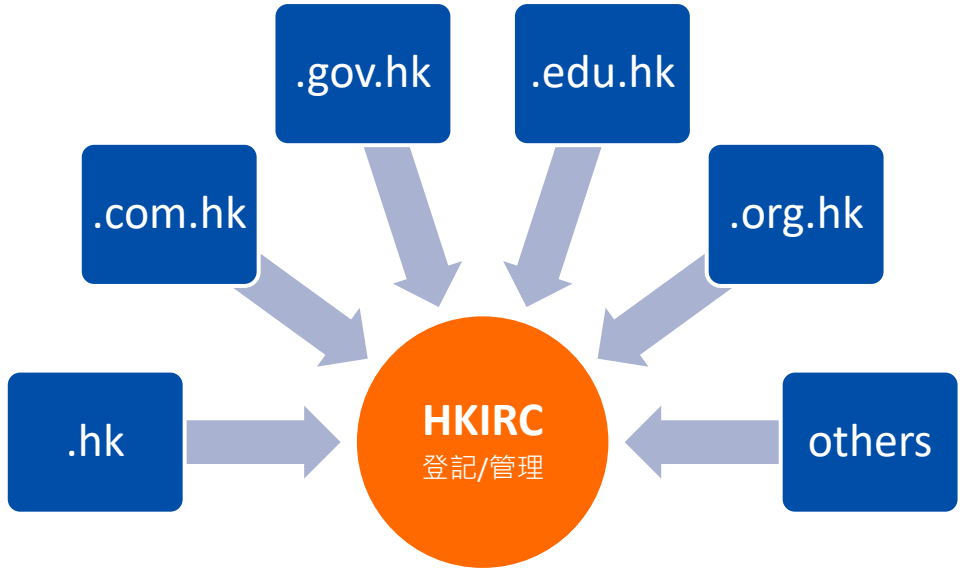
hkirc.hk

關於HKIRC

關於香港互聯網註冊管理有限公司

香港互聯網註冊管理有限公司 (HKIRC)

- 由香港特別行政區政府指定的一家非牟利及非法定機構，負責管理 .hk 國家代碼頂級域名 (ccTLD) 下的互聯網域名註冊
- **公共使命：**將香港推廣為一個包容、安全、創新及國際化的互聯網城市，並鼓勵使用互聯網及相關技術
- **網絡安全：**提供專業資源及協助，重點幫助企業、機構及學生提升其網絡安全水平，從而建立更安全的互聯網環境。



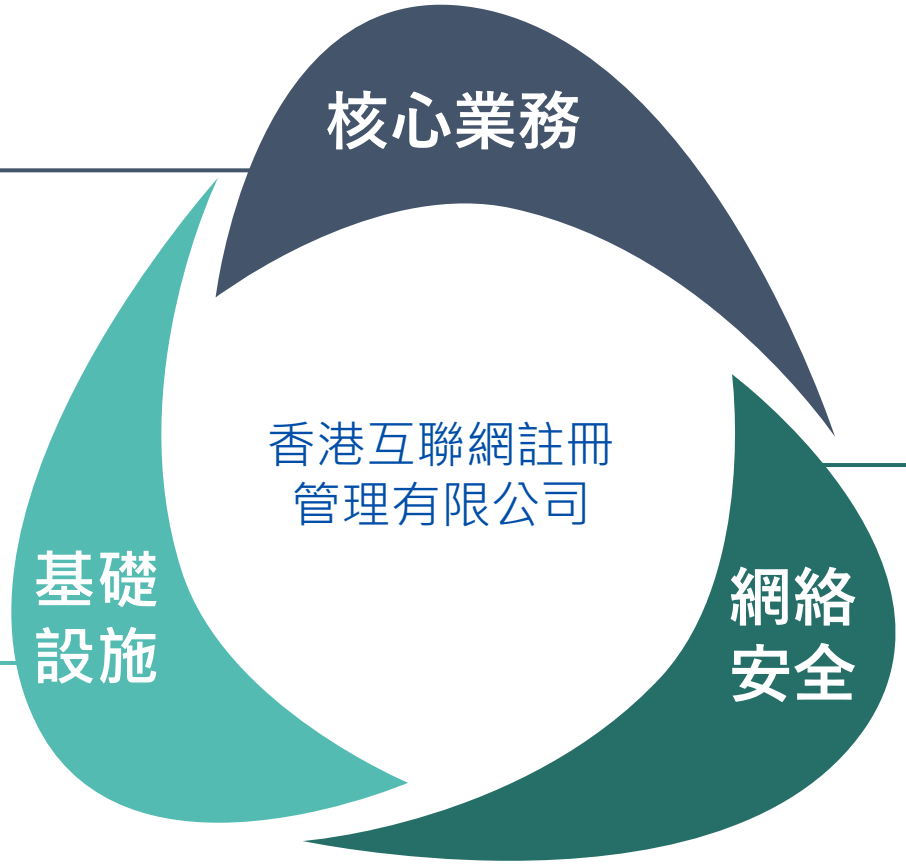
公司概覽

核心業務

- 在香港提供和維護可靠穩定的全天候DNS服務
- 監控和控制互聯網和功能變數名稱問題，如刪除網絡釣魚.hk網站、濫用和不當功能變數名稱
- 自給自足的營運模式，手頭儲備約2億港元

重要基礎設施

- 互聯網服務重要的基礎
- 支援香港大部分主要機構，包括政府部門、滙豐銀行、港鐵、所有大學等
- 採取最高的網絡安全標準規格



網絡安全服務

- 提升 .hk 域名使用者的網絡安全標準，如培訓和研討會
- 提供主動的網絡安全計畫，如中小企業網絡掃描、網絡安全資訊共用夥伴計劃、網絡安全員工培訓
- 與協會和不同持份者合作，將成功的計畫帶到不同的中小企

協助	培訓	25 年網絡釣魚演習：	送達
38,000+ 家香港中小企	400,000+ 名員工	300 機構、50,000 員工	網安警報 1M+ 條

公眾使命 – 網絡安全

透過定期掃描網站以識別潛在的安全弱點、持續監控系統環境中可能出現的威脅因素，有效應對各種技術漏洞，從而及時預防資料洩露事件發生，並全面確保整個系統的穩定性和完整性，進而提升整體資訊安全的防護水平。

- 網站漏掃
- 風險評估
- 顧問服務

技術層面

透過教育資源和專業指導，建立知識基礎並積極培養良好的網絡安全習慣，幫助有效識別諸如網絡釣魚等潛在風險，並逐步採用更安全的線上行為實踐，而無需具備深厚的技術專長即可達成。

員工層面

- 員工培訓
- 釣魚演練
- 威脅情報

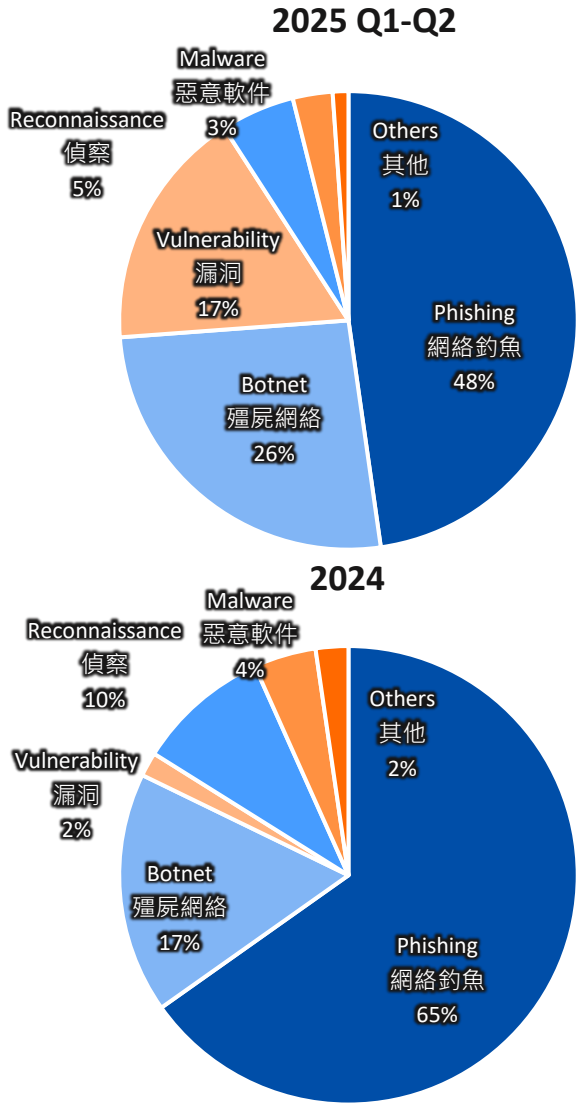
香港最新網路安全威脅

香港網絡攻擊及發展

- 針對香港的網絡威脅情報
  2025年第一季度至第二季度36萬相比 2024年44萬
  *數據來自香港警方網罪科

- 2025年網絡風險回顧與要點
  網絡釣魚 → 欺詐 Spoofing
  勒索軟件 → 存取權限販賣 Access sale
  漏洞→ 網站篡改 Defacement

- 香港的網路釣魚攻擊在2024年達到5年新高，同比增長108%。
- 2025 年Q1-Q2
  科技罪案發生16,262宗，損失金額30.48億港元



網絡釣魚 Phishing

什麼是網絡釣魚和欺詐？它如何影響我們？

網絡釣魚是什麼？

網絡釣魚是攻擊者假扮可信的人或機構，透過電郵、簡訊、社交媒體或假網站等方式，引誘你主動「上鉤」，輸入賬戶密碼、驗證碼或個人資料

什麼是欺詐 / 網絡詐騙

欺詐是利用各種詐騙手法，騙取金錢、賬戶或敏感資訊的行為。常結合網絡釣魚、假客服電話、假投資、假活動等方式進行

什麼是偽裝與冒充

偽裝與冒充是攻擊者把自己「包裝」成可信來源，
例如：仿冒電郵地址、來電號碼、網站網址、Logo 和版面，讓收件人以為訊息真的來自銀行、學校或常用服務

網絡釣魚如何利用偽裝與冒充

網絡釣魚通常結合偽裝與冒充，透過看似官方的電郵、簡訊、登入頁面或客服來電，誘使你放下戒心交出敏感資訊

影響層面:

- 個人賬戶與財務可能被盜用或轉走資金
- 公司系統與機密資料可能遭入侵和外洩
- 攻擊者可假冒客戶或供應商發送虛假付款指示
- 被竊取的賬戶可被用來發動更多釣魚與欺詐攻擊

案例研究：騙徒假冒NGO以虛假連結及網頁籌款

案例研究：利用災難新聞的偽冒 NGO 募款釣魚
受害機構： NGO遭偽冒
攻擊誘餌： 火災慘劇

詳細攻擊流程

1. **觸發點：利用公眾同情心與時事熱點**
   騙徒利用突發事件/災情製造緊急感，聲稱「立即捐款/協助」。
2. **偽冒身分：建立高像真度的釣魚據點**
   建立幾可亂真的假專頁/假網頁，盜用 NGO 名稱、標誌與文案，營造「官方」可信度。
3. **散播連結：釣魚訊息投放**
   透過社交平台貼文、群組訊息、私訊或短訊散播連結，誘導市民點擊。
4. **欺詐操作：偽造的捐款/登入頁面**
   假頁面引導受害者輸入個人/付款資料，或直接提供假收款方式（轉數快/銀行戶口）要求轉賬。
   騙取信用卡資料(包括CVV)/ FPS直接轉賬
5. **後果：雙重打擊**
   - 款項落入騙徒戶口（或資料被盜用作後續詐騙）
   - 真正 NGO 需要發澄清公告並承受信任受損。

更多案例

釣魚訊息 / 網站特徵

短訊或電郵內容前後矛盾、文法不通或拼字錯誤

電郵地址和網址的域名（domain）與官方域名有出入

網站未能轉換語言、部分按鈕或連結失效

電郵內有可疑連結、二維碼或附件

網址用上 .cc / .top / .vip /.today /.club等較冷門的延伸

在網站輸入不正確的帳戶或信用卡資料也能順利去到下一版面

安全貼士

不要開啟來歷不明的郵件或訊息

查看清楚寄件者的資料

切勿點擊可疑電郵或訊息內的超連結

切勿登入未經查證的網站

如網站要求提供個人或信用卡資料，應加倍小心

如懷疑受騙，應保存相關電郵或訊息，並儘快報警

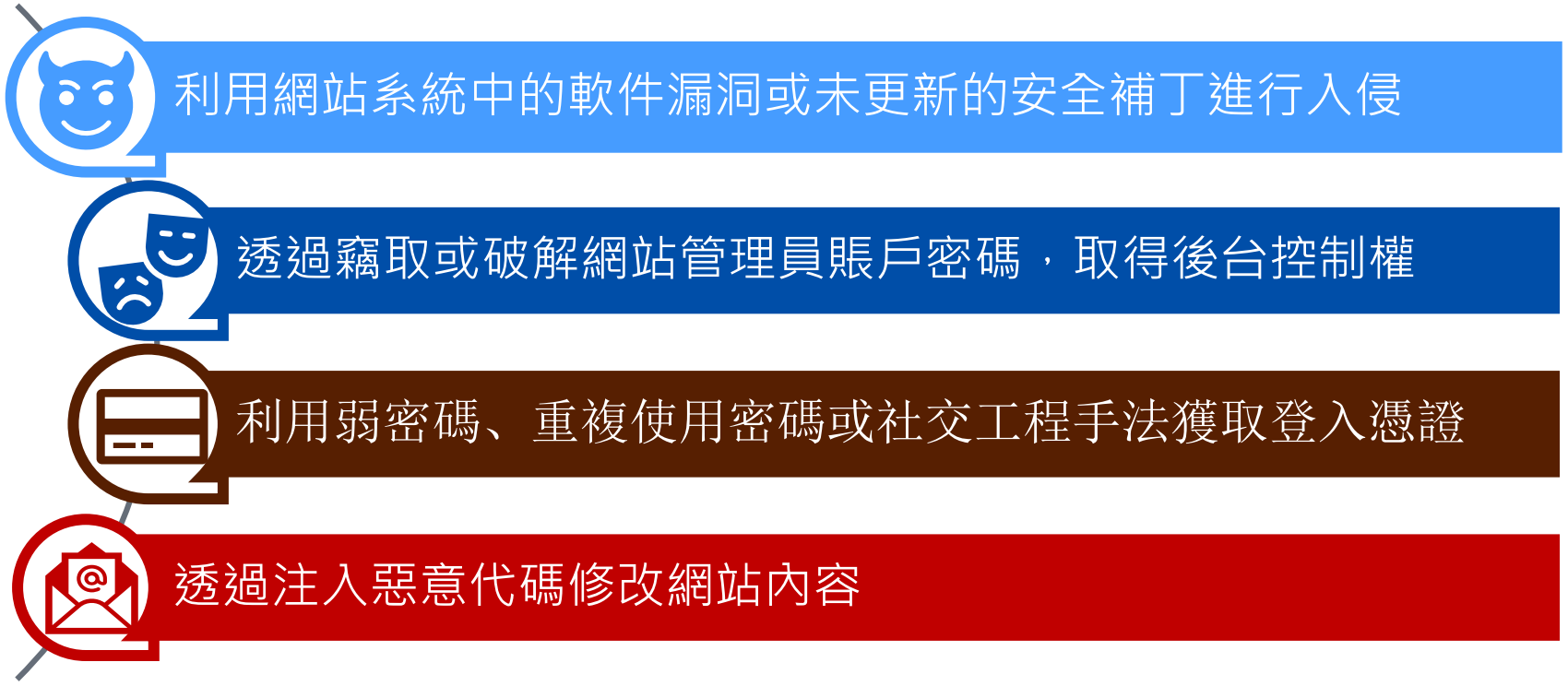
網路釣魚是什麼?

https://cyberhub.hk/index/#/tc/course/general-staff/1000am

網站篡改 Defacement

什麼是網站篡改？它如何影響我們？

損害品牌聲譽	用戶信任流失	潛在安全威脅	營運中斷	資料外洩風險
篡改內容可能包含污蔑信息、誤導客戶，破壞公司形象	用戶看到異常頁面會質疑網站安全性，可能停止使用服務	篡改網站可能植入木馬或病毒，危及訪客裝置安全	網站無法正常服務，直接影響業務	敏感資訊可能被竄改或盜取，造成法律與合規問題

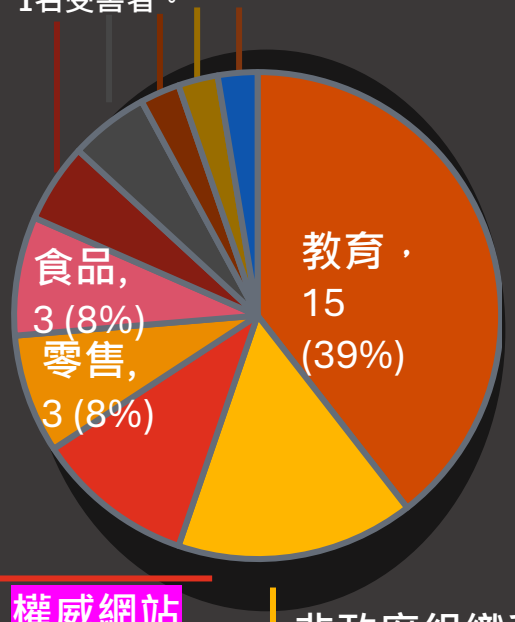


研究數據

香港網站面臨嚴重的網站篡改風險！僅在2025年1月至4月30日期間，PwC 就監控到38單網站篡改事件。

受害者分析

金融和酒店業業有2名受害者，而科技、專業服務和製造業有1名受害者。



數據來源: PwC

網站使用的技術

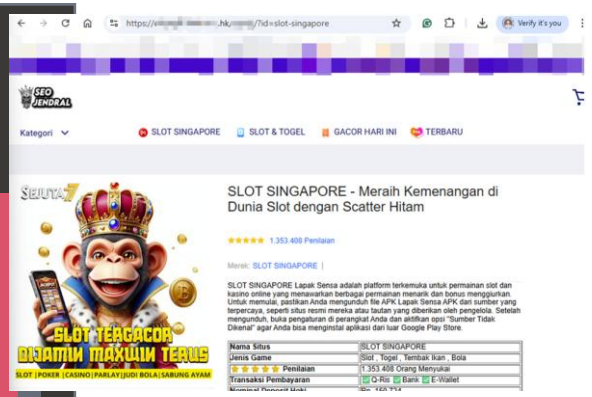
18 PHP	9 WordPress
4 Microsoft IIS	4 ASPX / ASP.NET
6 FTP	10 jQuery

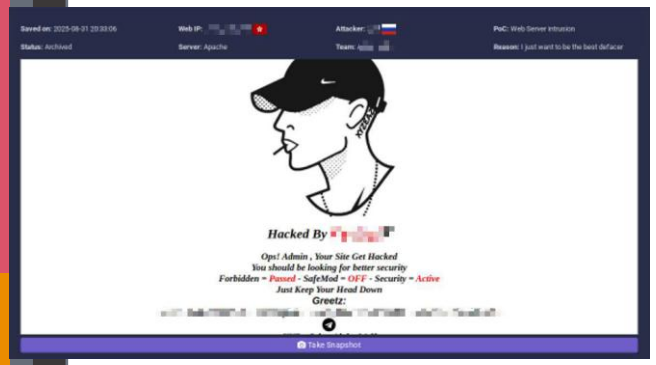
網站被篡改為.....

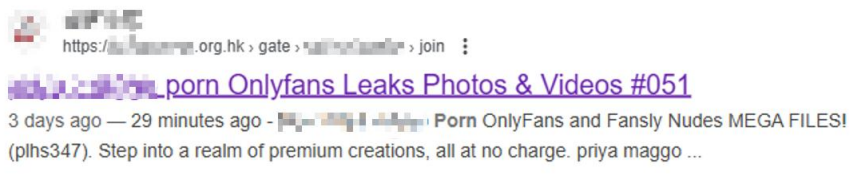
27 線上賭博網站

10 「純屬娛樂」或「灰色地帶」活動

1 成人內容







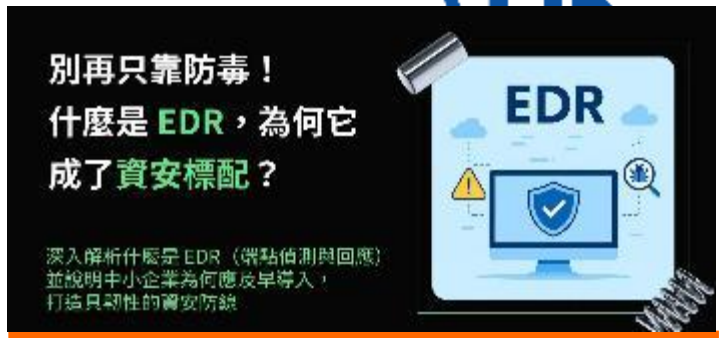
網站篡改的主因

遠端存取控制不足

- 開放VPN或遠端桌面給外判商
- 缺乏雙重驗證 (MFA)
- 資料儲存設備保護不足

防火牆及系統未修補

- 防火牆多年未更新
- 使用已停止支援的系統版本



欠缺威脅偵測機制

- 沒有主動監察系統異常
- 駭客可長期潛伏

最佳實踐:

- 使用強密碼並定期更換
- 啟用多重身分驗證
- 妥善保管賬戶資訊
- 警惕可疑電郵和連結
- 遵守公司安全政策
- 即時報告異常情況

NGO實際案例

Jan 2026

NGO實際案例1 – 登入頁面錯誤使用 Http 協定

我們以安全頁面內容為例進行視覺化，這在 .org.hk 中常見

實際例子

有些機構的登入頁面仍然使用 **HTTP 協定**，導致資料以未加密的純文字格式傳送。

影響

- **中間人攻擊 (Man-in-the-Middle Attacks)：** 攻擊者若在同一網路環境（如公共 Wi-Fi），即可攔截使用者名稱及密碼，因為它們是以純文字傳送。
- **工作階段劫持 (Session Hijacking)：** 攻擊者可劫持有效的使用者工作階段，從而獲取敏感的學生紀錄、成績或系統管理後台。
- **資料竄改 (Data Tampering)：** 由於 HTTP 流量未經加密，攻擊者可攔截並修改請求或回應（例如，竄改表單提交或更改學生成績）。

最佳實踐

- 檢查網站是否真的需要提供 **HTTP 版本**，否則應實施 **強制導向至 HTTPS** 的設定。

NGO實際案例2 – 後台開放給予公眾訪問- 目錄列表

網健通站掃描是一個快速測試的工具，能夠幫助我們在資源有限的情況下縮小範圍並集中重點。
我們進一步調查了「安全性較弱」的網站，並發現了其他有價值的問題。

實際例子

有機構的網頁允許使用者瀏覽目錄內容。
若將 **passwd** 與 **shadow** 檔案結合，可能會增加被暴力破解攻擊的風險。

影響

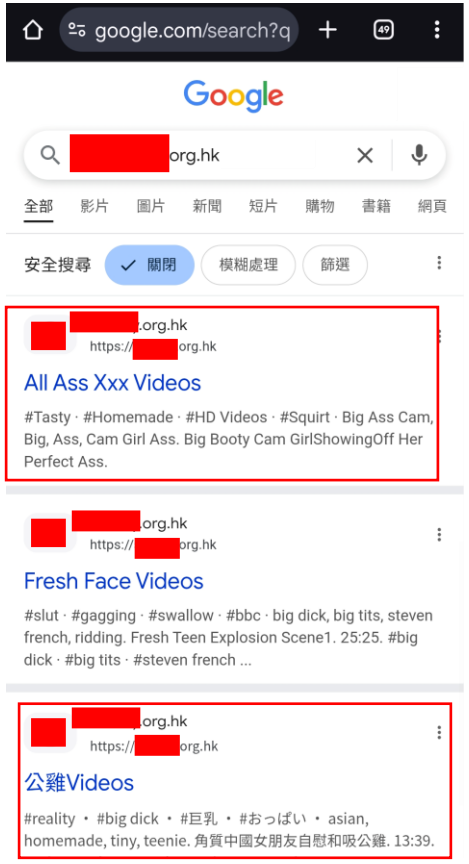
- **資料外洩 (Data Exposure)：** 目錄清單會洩露網站的結構，包括檔案名稱與目錄路徑，可能讓原本不應公開的敏感檔案被存取。攻擊面增加 **(Increased Attack Surface)：** 攻擊者可利用這些資訊識別潛在漏洞，從而更容易入侵目標的網頁應用程式。

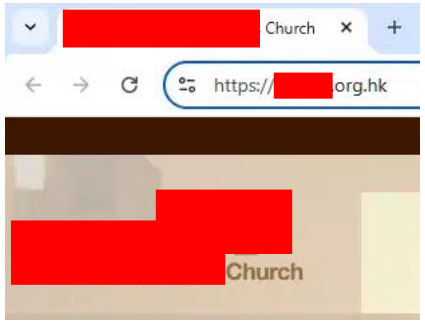
最佳實踐

- 停用目錄瀏覽 (Disable Directory Listing)

NGO實際案例3 – 開放式重定向攻擊

網健通站掃描是一個快速測試的工具，能夠幫助我們在資源有限的情況下縮小範圍並集中重點。
我們進一步調查了「安全性較弱」的網站，並發現了其他有價值的問題。





實際例子

有些機構允許將使用者重新導向至任意外部網址，這種功能常被濫用於惡意行為，例如釣魚攻擊或網站篡改。

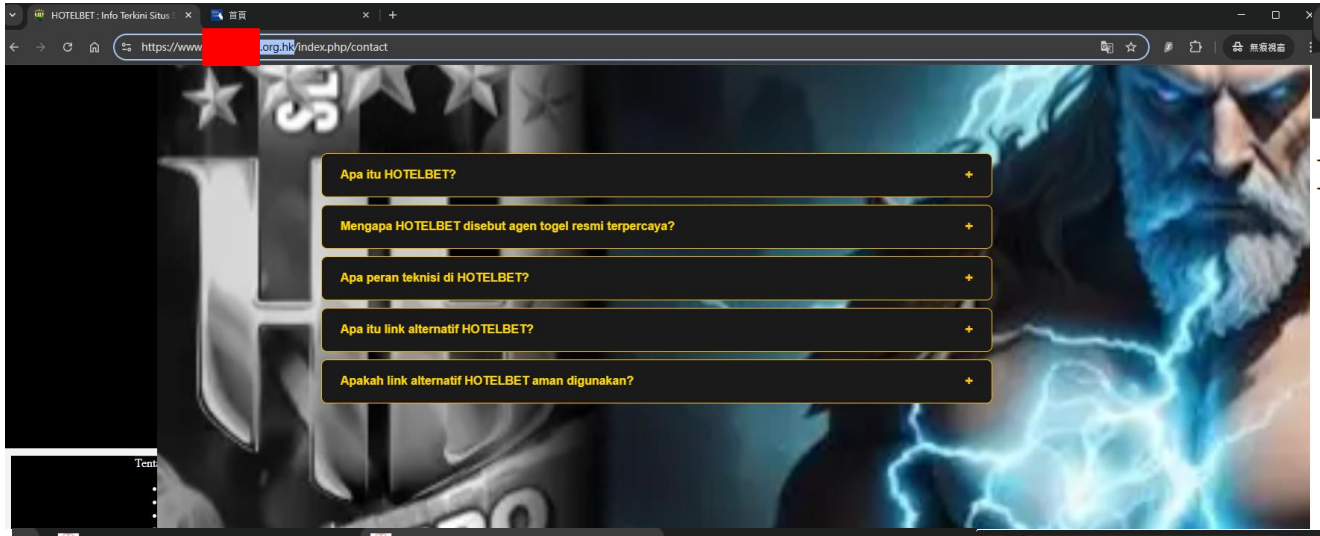
影響

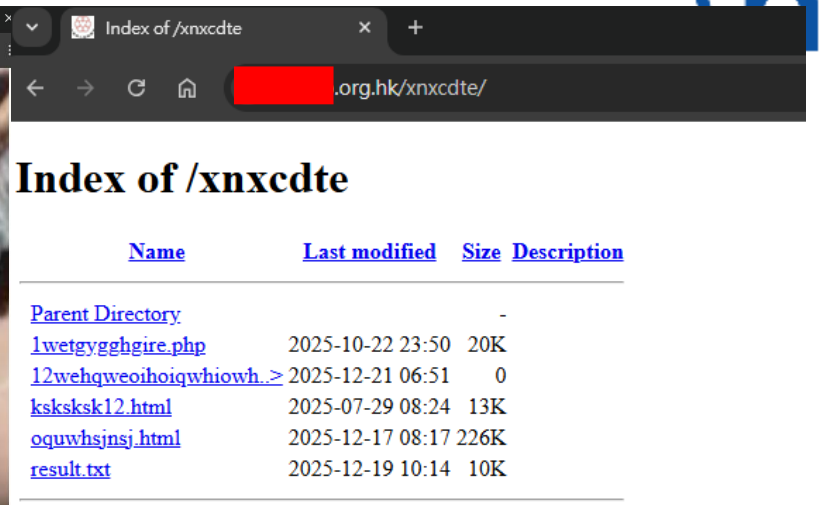
- **釣魚攻擊 (Phishing Attacks)**：攻擊者可將使用者導向至偽造的登入頁面。**信譽受損 (Reputation Damage)**：受信任的網站若將使用者導向惡意內容，會降低使用者的信任度。

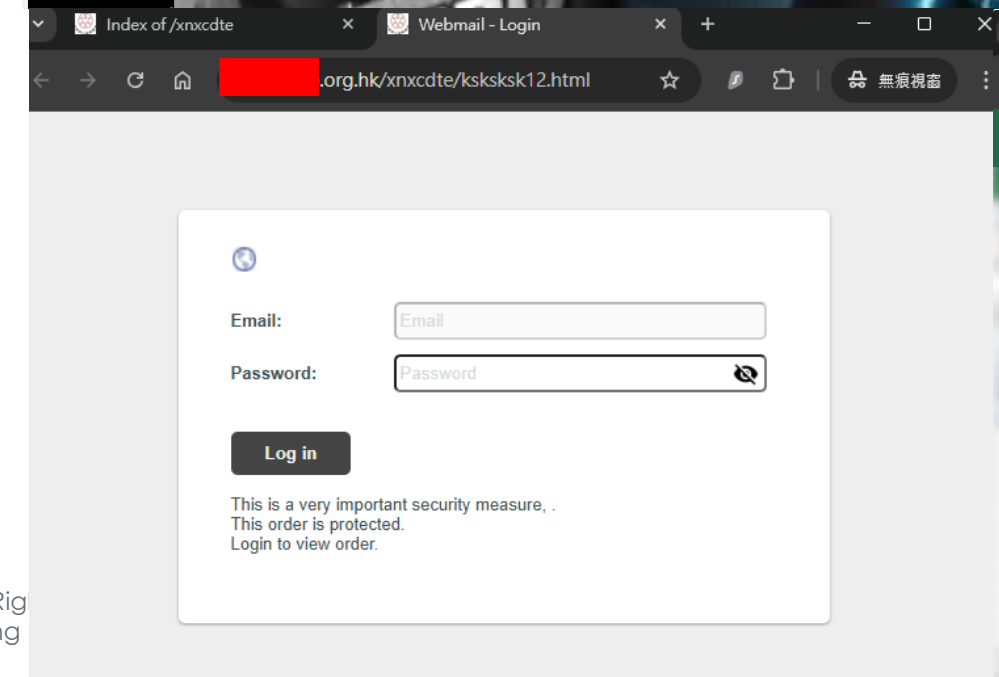
最佳實踐

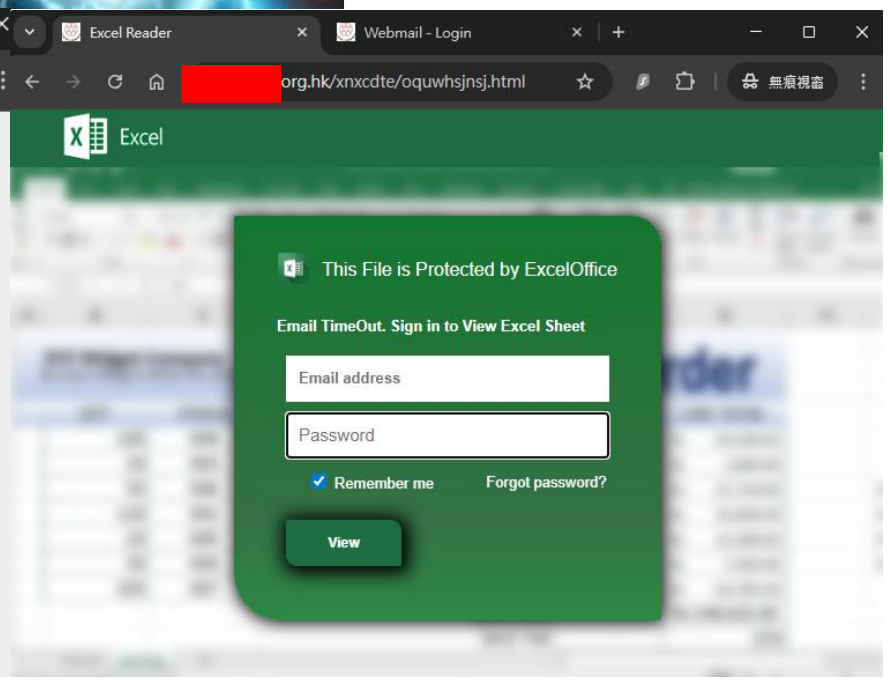
- 檢查重新導向功能是否真的必要，否則應使用 **白名單 (Whitelist)** 來限制可存取的網域。

NGO實際案例4 – org.hk 網站篡改實例









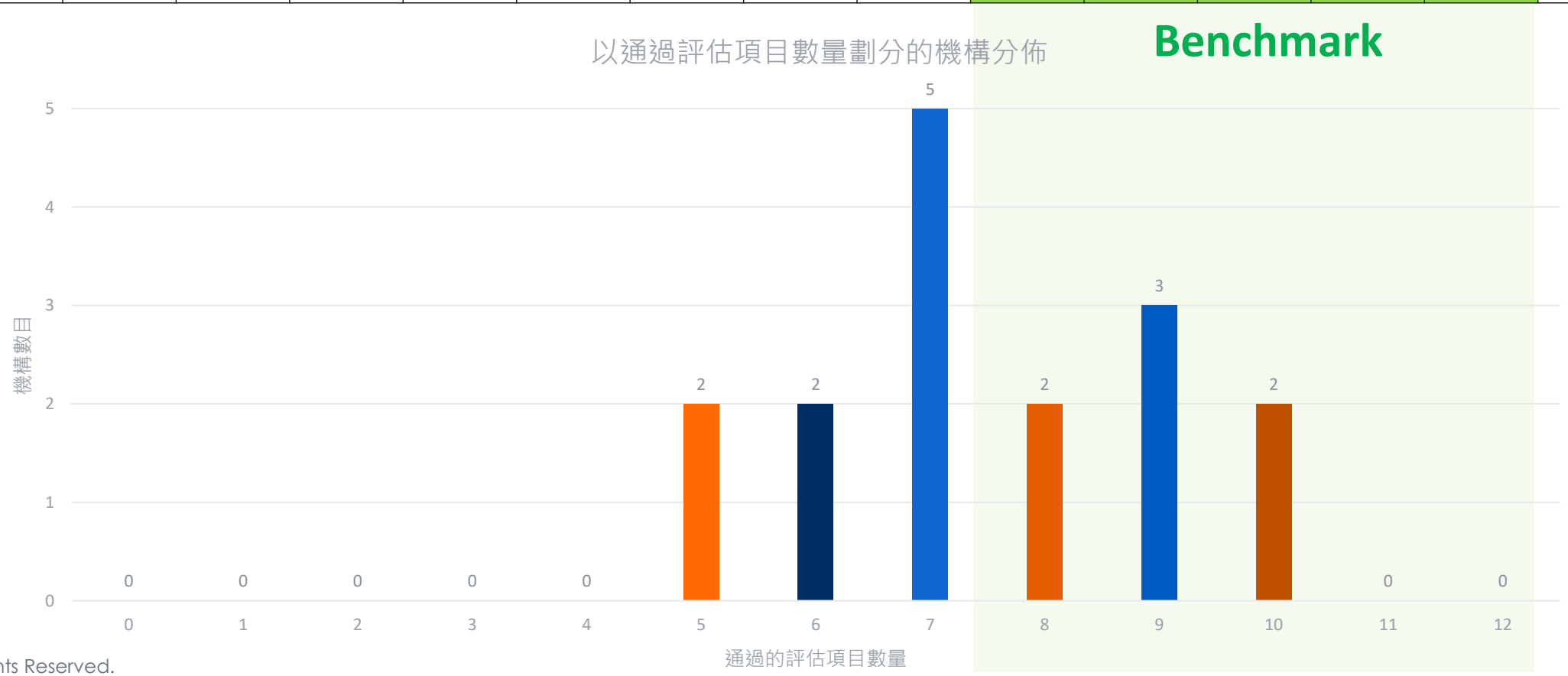
HKIRC研究 –

社福機構網站安全檢測初部結果及分析

Jan 2026

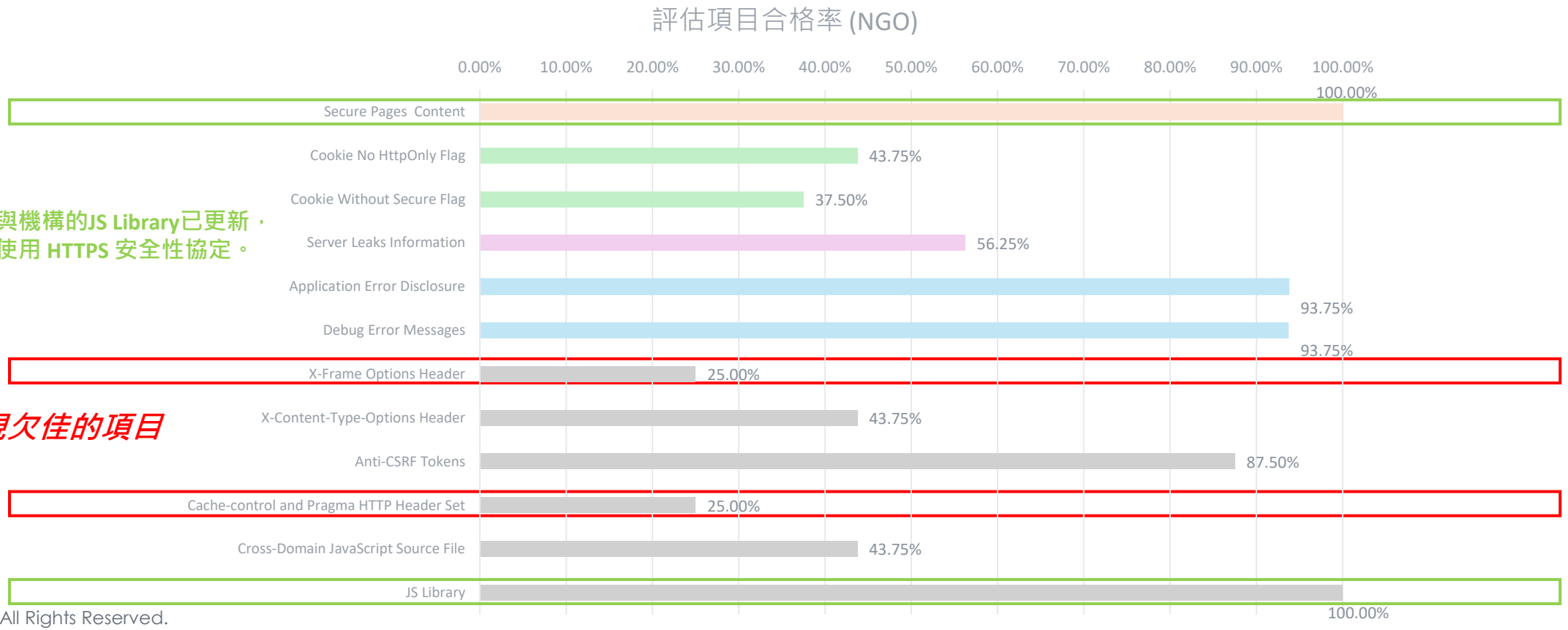
評估後的整體結果 (NGO)

通過的評估項目	0	1	2	3	4	5	6	7	8	9	10	11	12	Total
16 間機構的分佈	0.00%	0.00%	0.00%	0.00%	0.00%	12.5%	12.5%	31.25%	12.5%	18.75%	12.5%	0.00%	0.00%	100.00%



評估項目結果 (NGO)

	HTTP/HTTPS	Cookie 設定 Cookie Settings		伺服器版本 Server Version	資訊揭露 Information Disclosure		網站設定 (Website Configuration)					
	Secure Pages Content	Cookie HttpOnly Flag	Cookie Secure Flag	Server Leaks Information	Application Error	Information - Debug Error Message	X-Frame-Options Header	X-Content-Type-Options Header	Anti-CSRF Tokens	Cache-control and Pragma HTTP Header Set	Cross-Domain JavaScript Source File	JS Library
% of pass	100%	43.75%	37.5%	56.25%	93.75%	93.75%	25.0%	43.75%	87.5%	25.0%	43.75%	100.00%



所有參與機構的JS Library已更新，並且都使用 HTTPS 安全性協定。

表現欠佳的項目

表現欠佳的項目：
X-Frame-Options 標頭未設定 – 點擊劫持攻擊（Clickjacking）

- 漏洞成因： 機構的內容管理系統或內部捐款管理平台未設定 X-Frame-Options 或 Content-Security-Policy (frame-ancestors) 標頭，導致網站可以被嵌入到惡意網頁的透明框架 (iframe) 中。

例子

- **步驟 1：以「資助機會」或「免費資源」作為誘餌**
  攻擊者針對該 NGO 的通訊部門或行政人員，發送一封釣魚郵件，宣傳一個偽造的網站，標題為「**限時申請**」或「**免費下載 NGO 籌款策略白皮書**」。網頁設計精美，中間有一個醒目的「**立即申請 / 下載**」按鈕。
- **步驟 2：隱藏的後台操作 (The Hidden Iframe)**
  攻擊者知道該員工平日會保持登入機構的官方網站後台 (CMS) 或會員管理系統。
  在那個偽造的「資助申請」網頁上，攻擊者在背景載入了一個**透明的、不可見的 iframe**。這個 iframe 其實正是該 NGO 網站後台的「**新增管理員用戶**」頁面。（前提是員工已在另一個視窗登入了後台，且瀏覽器保留了登入狀態）。
- **步驟 3：欺騙性點擊與權限劫持**
  攻擊者利用 CSS 技術，將後台頁面中那個真實的「**確認新增管理員**」按鈕，**精確地對齊並覆蓋在偽造網頁的「立即申請」**按鈕正下方。
  - **員工眼中：** 我正在點擊按鈕以申請一筆資助或下載。
  - **實際操作：** 滑鼠點擊穿透了偽造圖層，直接按下了後台的「確認」鍵。
- **結果：**
  攻擊者成功在不知不覺中，將一個惡意賬號新增為該 NGO 網站的「**最高權限管理員**」。隨後，攻擊者便可利用此權限篡改網站內容（如發布詐騙募款連結）、竊取捐款人資料，或植入後門程式，而受害者完全以為自己只是點擊了一個申請按鈕。

表現欠佳的項目：
Cache-Control 與 Pragma HTTP 標頭設定

- 此警示表示網站未正確設定指示瀏覽器不要儲存（或快取）敏感資料的 HTTP 標頭，例如登入後的頁面或個人資訊頁面。
- 若瀏覽器儲存了敏感資訊（如銀行對帳單或私人儀表板頁面）：
  - 使用同一台電腦的其他人可能看到這些資訊。
  - 若裝置被竊，駭客可能從快取中取出這些資料。

例子

- **步驟 1：敏感頁面未設定適當的快取標頭**
  網頁應用程式傳送敏感內容（例如帳戶詳細資料或工作階段資訊）時，未設定安全的 HTTP 標頭。

- **步驟 2：登出後快取資料仍可存取**
  使用者登出後，擁有同一裝置存取權的人（例如共用電腦的使用者）可以按瀏覽器的「上一頁」按鈕，或直接檢查瀏覽器快取檔案，從而看到敏感資料，例如個人資訊或工作階段權杖（session token）。

- **步驟 3：身分盜用或工作階段劫持風險**
  攻擊者可從快取中取出工作階段資料，並冒充該使用者身分，導致身分盜用、未經授權的操作或資料外洩——全部原因在於瀏覽器保留了本應立即丟棄的敏感內容。

HKIRC 免費網絡安全資源 - 網絡防禦一站通(Cybersec One)

免費網絡安全資源 – 協助機構提高網絡安全

Cybersec One 整合以下免費服務:

1. **偵測與預防 -** 在事件發生前評估風險等級，並強化預防措施
   - ✓ ***網健通*** – 網站基本評估服務
   - ✓ ***風險評估*** – IT風險自我評估工具

2. **安全意識** -提升組織及員工的網路安全意識
   - ✓ ***Cybersec Training Hub*** – 線上員工網安意識培訓平台
   - ✓ ***釣魚演練*** –年度釣魚演練活動

3. **持續發展** -透過資訊分享及活動，提升對網路安全的意識及興趣
   - ✓ ***Cybersec Infohub*** –資訊分享平台
   - ✓ ***講座及研討會***–定期更新網路安全趨勢

網健通 – 網站基本掃瞄服務

網健通

模擬一般訪客存取網站，並提供無侵入性工具的檢查服務。

被動式網站掃描

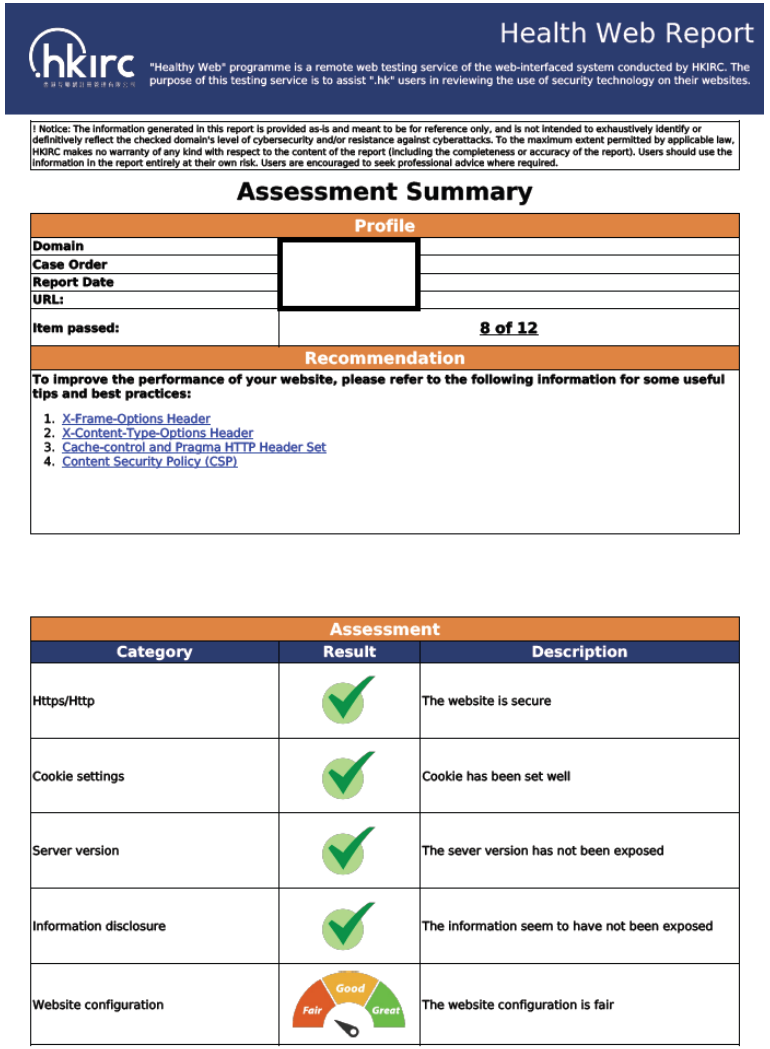
- ✓ 非侵入性掃描，僅評估公開開放資料，不影響業務運作
- ✓ 快速測試以識別潛在漏洞
- ✓ 能夠進行大規模掃描
- ✓ 參考 OWASP Top 10 中的 12 項評估

Healthy Web 掃描報告

- ✓ 適合非技術使用者輕鬆理解網站安全配置
- ✓ 提供基本資訊以支援分類分析
- ✓ 受超過 38,000 家中小企業信賴

顧問服務

- ✓ 約 30 分鐘線上諮詢
- ✓ 解釋報告內容
- ✓ 說明網站漏洞的風險及成因
- ✓ 提供可行動的修復建議及最佳實務



Health Web Report

"Healthy Web" programme is a remote web testing service of the web-interfaced system conducted by HKIRC. The purpose of this testing service is to assist ".hk" users in reviewing the use of security technology on their websites.

! Notice: The information generated in this report is provided as-is and meant to be for reference only, and is not intended to exhaustively identify or definitively reflect the checked domain's level of cybersecurity and/or resistance against cyberattacks. To the maximum extent permitted by applicable law, HKIRC makes no warranty of any kind with respect to the content of the report (including the completeness or accuracy of the report). Users should use the information in the report entirely at their own risk. Users are encouraged to seek professional advice where required.

Assessment Summary

Profile	
Domain	
Case Order	
Report Date	
URL:	
Item passed:	8 of 12

Recommendation

To improve the performance of your website, please refer to the following information for some useful tips and best practices:

1. X-Frame-Options Header
2. X-Content-Type-Options Header
3. Cache-control and Pragma HTTP Header Set
4. Content Security Policy (CSP)

Assessment		
Category	Result	Description
Https/Http	✓	The website is secure
Cookie settings	✓	Cookie has been set well
Server version	✓	The sever version has not been exposed
Information disclosure	✓	The information seem to have not been exposed
Website configuration	Fair / Good / Great	The website configuration is fair

31

Cybersec Risk Detector –自我評估工具

風險評估

為了提升組織內部的理解並評估風險等級，將針對管理層及技術人員進行評估和調查。

六項評估標準

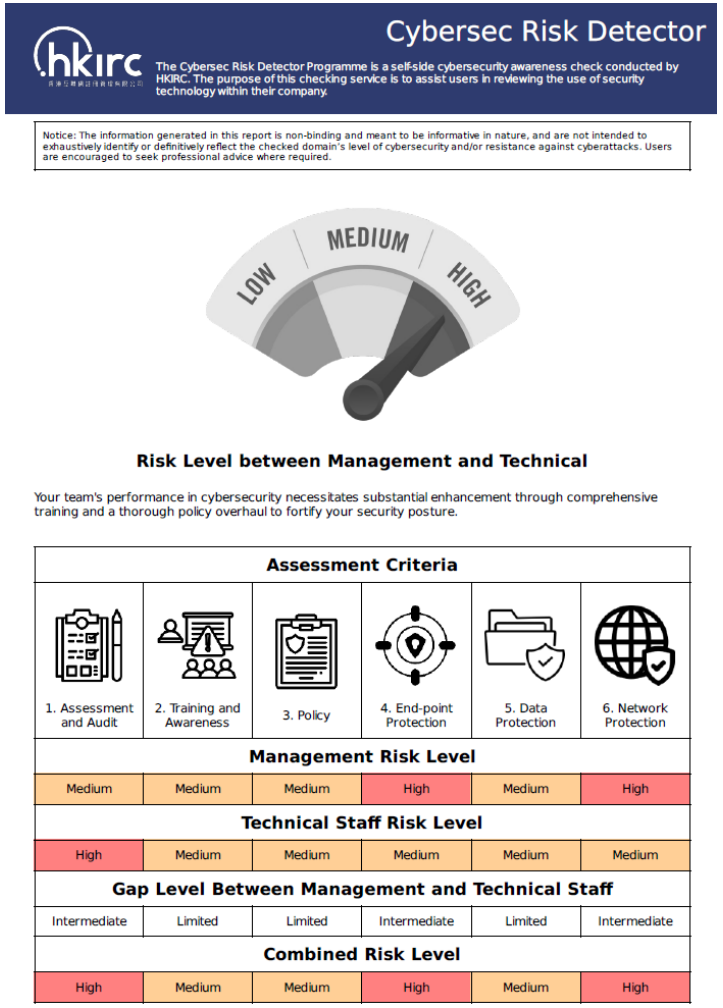
1. 評估與審計
2. 訓練與意識
3. 政策
4. 端點保護
5. 資料保護
6. 網路保護

三種評估類型

✓ 管理層評估 – 從管理層了解風險等級
✓ 技術人員評估 – 從技術人員了解風險等級
✓ 比較評估 – 了解管理層與技術人員之間的理解差距

報告與諮詢服務

✓ 提供減輕已識別風險的建議



Cybersec Risk Detector

The Cybersec Risk Detector Programme is a self-side cybersecurity awareness check conducted by HKIRC. The purpose of this checking service is to assist users in reviewing the use of security technology within their company.

Notice: The information generated in this report is non-binding and meant to be informative in nature, and are not intended to exhaustively identify or definitively reflect the checked domain's level of cybersecurity and/or resistance against cyberattacks. Users are encouraged to seek professional advice where required.

Risk Level between Management and Technical

Your team's performance in cybersecurity necessitates substantial enhancement through comprehensive training and a thorough policy overhaul to fortify your security posture.

Assessment Criteria					
1. Assessment and Audit	2. Training and Awareness	3. Policy	4. End-point Protection	5. Data Protection	6. Network Protection
Management Risk Level					
Medium	Medium	Medium	High	Medium	High
Technical Staff Risk Level					
High	Medium	Medium	Medium	Medium	Medium
Gap Level Between Management and Technical Staff					
Intermediate	Limited	Limited	Intermediate	Limited	Intermediate
Combined Risk Level					
High	Medium	Medium	High	Medium	High

基本支援

網絡安全員工意識培訓

Cybersec Training Hub

https://youtu.be/ju9How84Nvw

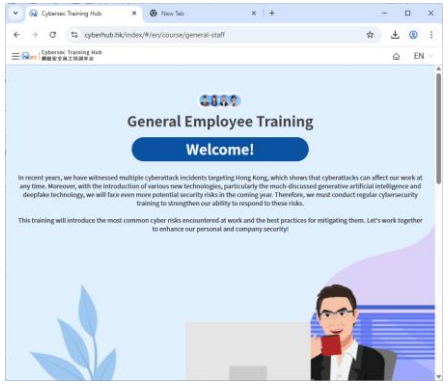
基本支援 - 網絡安全員工意識培訓

網絡安全員工意識培訓

提供免費自學平台，為機構提供網絡安全員工培訓資源

- ✓ 涵蓋基礎與進階課程
- ✓ 以員工日常可能遇到的網絡風險為出發點
- ✓ 模擬實際工作環境中的潛在網絡風險
- ✓ 提供相應的防範方法與最佳工作實踐建議

平台介面



基礎培訓

電子證書

培訓課程包括：

基 **基本培訓**

- ➢ 基本員工培訓
- ➢ 學生職前培訓

熱 **熱門話題**

- ➢ 一頁式提示的網絡安全熱話

進 **進階培訓**

- ➢ 崗位
  - ▪ 管理人員
  - ▪ 財務/會計
  - ▪ 人力資源
  - ▪ 市場營銷
  - ▪ 客戶服務
  - ▪ 資訊科技
- ➢ 行業
  - ▪ 電子商務
  - ▪ 非政府組織
  - ▪ 科技初創

基本支援 - 年度網絡釣魚演練

年度網絡釣魚演練

為提高員工防範可疑電郵的意識，香港警務處網絡安全及科技罪案調查科（網罪科）與香港互聯網註冊管理有限公司（HKIRC）將聯合舉辦「釣魚電郵演習2025」，並誠邀各機構參與。是次演習旨在教育員工辨別可疑電郵，從而提升參與機構的網絡安全水平。

簡單參與，輕鬆上手

- ✓ **設置簡易**：僅需將電郵伺服器加入白名單，對 DNS 無 任何影響。
- ✓ **專業支援**：提供配置協助及客服支援，將 IT 工作量降 至最低。
- ✓ **費用全免**：零成本即可全面提升網絡防護水平。
- ✓ **演習過程**：將於活動期間不定時發送模擬釣魚電郵，以測試員工的警覺性及應變能力。
- ✓ **專屬報告**：演習結束後，參與機構將獲得分析報告，協助管理層了解員工表現，並作規劃後續培訓依據。

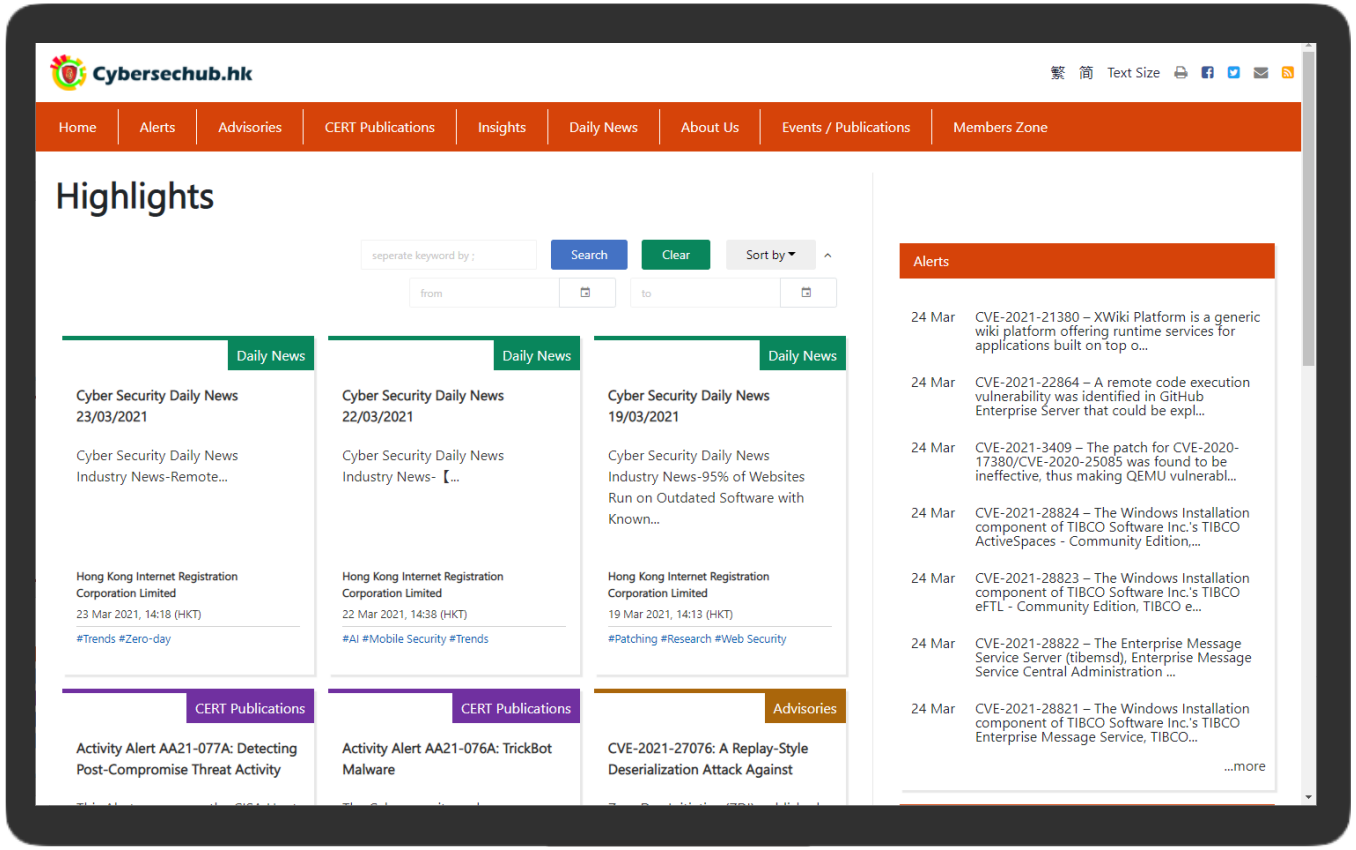
「Cybersec One」的參與機構將獲邀參與 2025 年度的網絡釣魚演練，並享有優先參加資格。

網絡安全資訊 Cybersechub.hk

網絡安全資訊 - 「網絡安全資訊共享夥伴計劃」- “Cybersec Infohub” (http://cybersechub.hk/)

提供一個跨行業的網絡安全資訊共享協作平台“Cybersechub.hk”，並舉辦業界活動，以促進業界有效地交換網絡安全威脅資訊、緩解策略、良好作業模式及知識。

- 保安警報
- 保安建議
- CERT 刊物
- 專家見解
- 每日快訊
- 網上諮詢



基本支援 - 網絡安全資訊

網絡安全資訊

「Cybersec One」的參與機構可

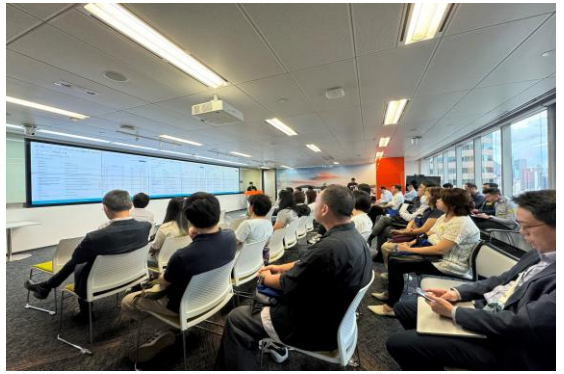
- ✓ 定期獲得最新的網絡安全資訊
- ✓ 獲邀參與 HKIRC舉辦的網絡安全活動
- ✓ 獲邀參與HKIRC合作夥伴舉辦的網絡安全活動

以掌握最新攻擊手法與行業發展趨勢。

2025國家網絡安全宣傳周香港分論壇

網絡安全技術論壇2024

定期網絡安全研討會



定期網絡安全研討會

謝謝