HK 網站安全體檢｜黑箱、只讀

# 網站安全體檢報告

域名：**loldraftpick.com**
授權人：**本人（自用資產）**
授權日期：**2026-11-17**
產生時間：**2026-11-17 01:26**
授權書／參考：**self-owned**
檢查項數：**30**｜請求數：**37**

**D**
51／100

**結論：**多個高危缺口同時存在，屬「隨時會被掃到」的狀態。

未通過 5 項（高 1／ 中 3／ 低 1） ｜通過 19｜需留意 0｜不適用 6

## 高風險項目（優先處理）

### HTTP 自動轉 HTTPS 風險 高 未通過

HTTP 明文可直達（200）

修復方向：在 80 端口做 301 去 443，不要只在應用層做

建議方案：急救包 HK$8,000–15,000（3–5 個工作日）

## 中／低風險項目

### HSTS 標頭與有效期 風險 中 未通過

回應沒有 Strict-Transport-Security

修復方向：加 HSTS，max-age 至少 15552000（180 日）

建議方案：標準硬化 HK$20,000–40,000（4 週）

### Content-Security-Policy 存在 風險 中 未通過

沒有 Content-Security-Policy

修復方向：由 Report-Only 開始收窄 script-src／object-src

建議方案：標準硬化 HK$20,000–40,000（4 週）

### 防點擊劫持（XFO／frame-ancestors） 風險 中 未通過

沒有 X-Frame-Options，亦沒有 CSP frame-ancestors

修復方向：加 X-Frame-Options: SAMEORIGIN 或 CSP frame-ancestors

建議方案：標準硬化 HK$20,000–40,000（4 週）

### Referrer-Policy 存在 風險 低 未通過

沒有 Referrer-Policy

修復方向：設 strict-origin-when-cross-origin

建議方案：標準硬化 HK$20,000–40,000（4 週）

## 分類統計

| 類別 | 項數 | 未通過 | 通過 | 留意／不適用 |
|---|---|---|---|---|
| 傳輸與憑證 | 5 | 2 | 3 | 0 |
| 伺服器指紋 | 4 | 0 | 3 | 1 |
| 敏感檔案 | 8 | 0 | 8 | 0 |
| 資訊洩漏 | 2 | 0 | 2 | 0 |
| 防護標頭 | 4 | 3 | 1 | 0 |
| Cookie 與跨域 | 4 | 0 | 2 | 2 |
| 表單與輸入 | 3 | 0 | 0 | 3 |

## 傳輸層

| | |
|---|---|
| 最終連線 | https://loldraftpick.com/（HTTP 200） |
| 伺服器標頭 | cloudflare |
| TLS | TLSv1.3／TLS_AES_256_GCM_SHA384／到期 Feb 13 18:56:34 2027 GMT |

## 附錄：30 項檢查結果

| # | 項目 | 風險 | 結果 | 證據摘要 |
|---|---|---|---|---|
| 1 | TLS 憑證有效且未過期 | 高 | 通過 | TLSv1.3 TLS_AES_256_GCM_SHA384｜到期 Feb 13 18:56:34 2027 GMT（89 日） |
| 2 | 停用 TLS 1.0／1.1 | 中 | 通過 | TLS 1.0／1.1 握手失敗（伺服器已停用，或本機客戶端已封鎖） |
| 3 | HSTS 標頭與有效期 | 中 | 未通過 | 回應沒有 Strict-Transport-Security |
| 4 | HTTP 自動轉 HTTPS | 高 | 未通過 | HTTP 明文可直達（200） |
| 5 | TRACE 方法已關閉 | 低 | 通過 | TRACE → 405 |
| 6 | 不洩漏 X-Powered-By | 低 | 通過 | 沒有 X-Powered-By |
| 7 | Server 標頭不含版本號 | 低 | 通過 | cloudflare |
| 8 | PHP 版本仍在安全支援期 | 高 | 不適用 | 外部看不到 PHP 版本 |
| 9 | CMS 版本不過舊 | 中 | 通過 | 沒有對外指紋（或非 CMS 站） |
| 10 | 環境變數檔不可下載（/.env） | 高 | 通過 | /.env → 404 |
| 11 | 版本庫不可下載（/.git/） | 高 | 通過 | /.git/config → 404 |
| 12 | 備份／暫存檔不可下載 | 高 | 通過 | 探測 10 條備份路徑，全部非 200 |
| 13 | phpinfo／測試檔已移除 | 高 | 通過 | 5 條常見 phpinfo 路徑全部無效 |
| 14 | server-status／server-info 已關閉 | 中 | 通過 | server-status／server-info 未開放 |
| 15 | 目錄列舉已關閉 | 中 | 通過 | 6 條常見目錄都冇列舉 |
| 16 | 管理後台不對公網開放 | 中 | 通過 | 5 條常見後台路徑都唔存在 |
| 17 | xmlrpc.php 已停用 | 低 | 通過 | /xmlrpc.php → 404 |
| 18 | 錯誤頁不洩露伺服器路徑 | 中 | 通過 | 404 頁冇路徑或堆疊洩露（404） |
| 19 | robots.txt 不洩露敏感路徑 | 低 | 通過 | robots.txt 沒有敏感路徑 |
| 20 | Content-Security-Policy 存在 | 中 | 未通過 | 沒有 Content-Security-Policy |
| 21 | X-Content-Type-Options: nosniff | 低 | 通過 | nosniff |
| 22 | 防點擊劫持（XFO／frame-ancestors） | 中 | 未通過 | 沒有 X-Frame-Options，亦沒有 CSP frame-ancestors |
| 23 | Referrer-Policy 存在 | 低 | 未通過 | 沒有 Referrer-Policy |

| # | 項目 | 風險 | 結果 | 證據摘要 |
|---|---|---|---|---|
| 24 | Cookie 有 Secure／HttpOnly／SameSite | 中 | 不適用 | 首頁沒有 Set-Cookie |
| 25 | CORS 不開放萬用字元 | 高 | 通過 | 沒有 CORS 標頭 |
| 26 | HTTPS 頁不混用 HTTP 資源 | 中 | 通過 | 首頁資源全部 HTTPS 或相對路徑 |
| 27 | 外部 script 有 SRI | 低 | 不適用 | 首頁沒有跨域 script |
| 28 | 表單提交不走明文或外部域 | 中 | 不適用 | 首頁沒有表單 |
| 29 | 上傳表單有 CSRF 保護 | 低 | 不適用 | 首頁沒有上傳表單 |
| 30 | SQL 錯誤訊息不外洩 | 高 | 不適用 | 需要 --active 授權才做主動測試 |

## 方法、範圍與限制

本報告由 `audit.py v0.2.0` 產生：對外黑箱、只發 GET／HEAD／TRACE， 預設請求間隔 0.5 秒、單次不超過 120 個請求；未做主動測試（無 --active）。

不包括：登入後台內部檢查、原始碼審計、伺服器主機層（OS／資料庫設定）、第三方 SaaS、 0-day 漏洞、壓力測試與入侵行為。報告只列風險、影響與修復方向，不提供逐步攻擊指令。

---

本報告只供委託人內部使用，未經書面同意不得轉交第三方或公開發佈。 風險評分＝100 −（高危 18／中危 9／低危 4 分），下限 0；等級 A ≥90、B ≥80、C ≥65、D ≥50、其餘 F。

報告按 30 項清單完成檢查，不構成「零漏洞」保證；修復後可安排一次覆檢（7 個工作日內）。