物聯網應用資訊安全與風險管理

API 請求實作作業

組員：劉定睿、曾彥輔、羅勻瑄、黃世君

日期：2025-10-01

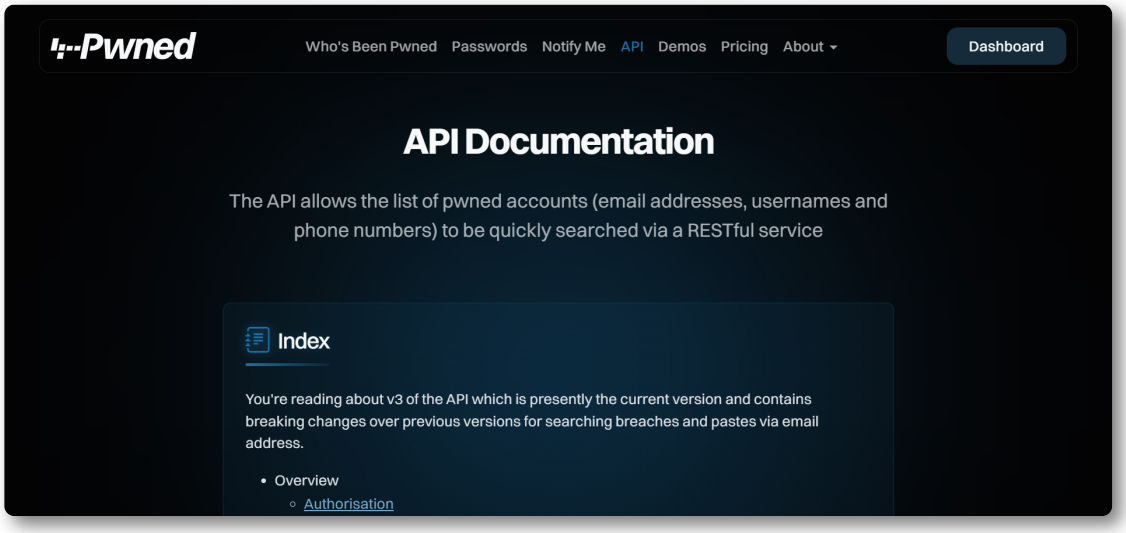
目錄

一、Haveibeenpwned API 實作

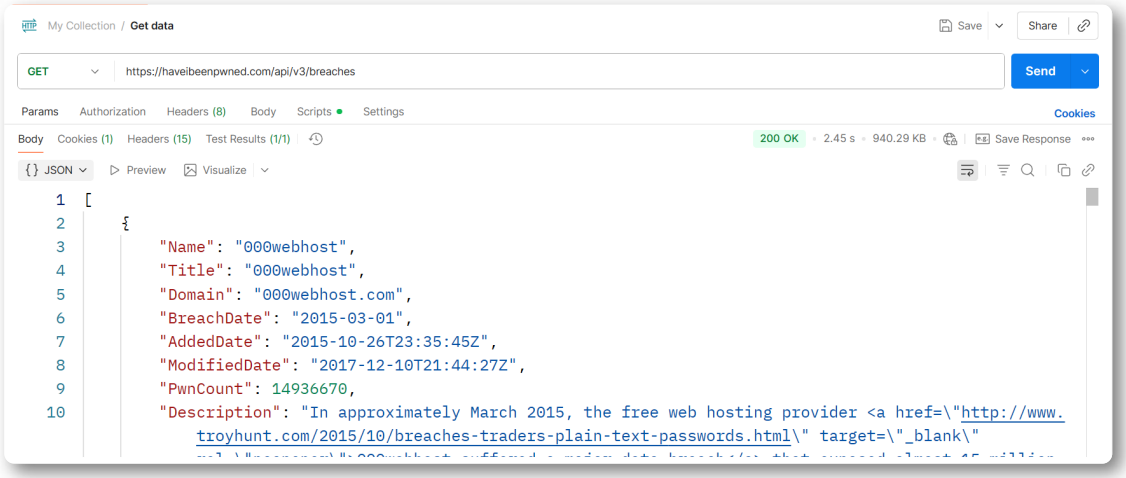
- 問題背景：我使用的是 Haveibeenpwned 的 API ，Haveibeenpwned 本身就是一個外洩資訊資料庫，可以針對Email, Domain ...等資訊查詢外洩資訊。本次實作是利用多個免費開放的 API 端點進行查詢實作，透過以postman 進行封包傳送與回應，了解 API 實作流程。

- 執行方法與步驟

  1. 查詢 https://haveibeenpwned.com/API/v3 免費之 API 端點

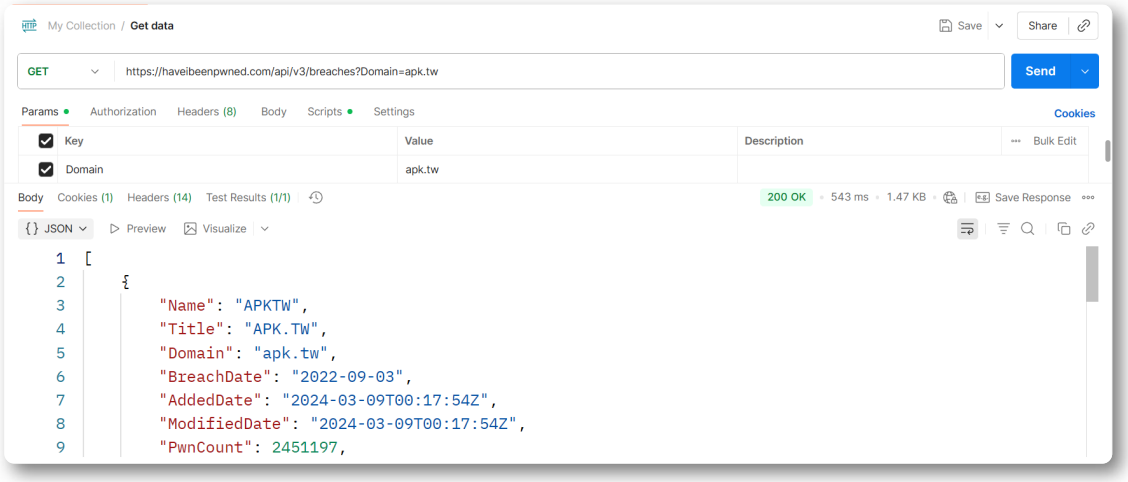


  2. 實作請求一：以 `GET` 傳送請求 https://haveibeenpwned.com/api/v3/breaches 查詢 **所有** 被入侵資訊

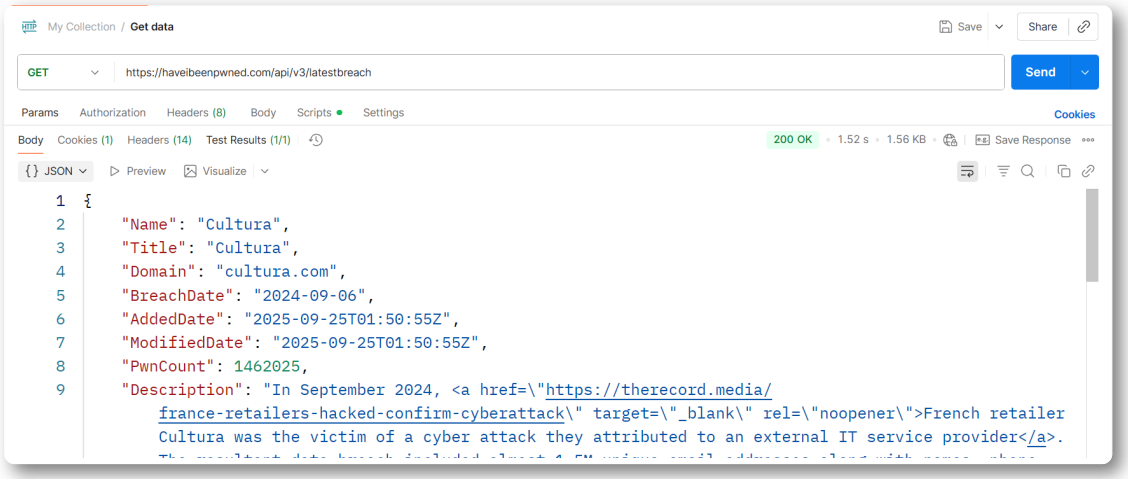


  2.1 以 `GET` 傳送請求，並帶有 `GET` 參數 `Domain` 以指定查詢該網域外洩資訊

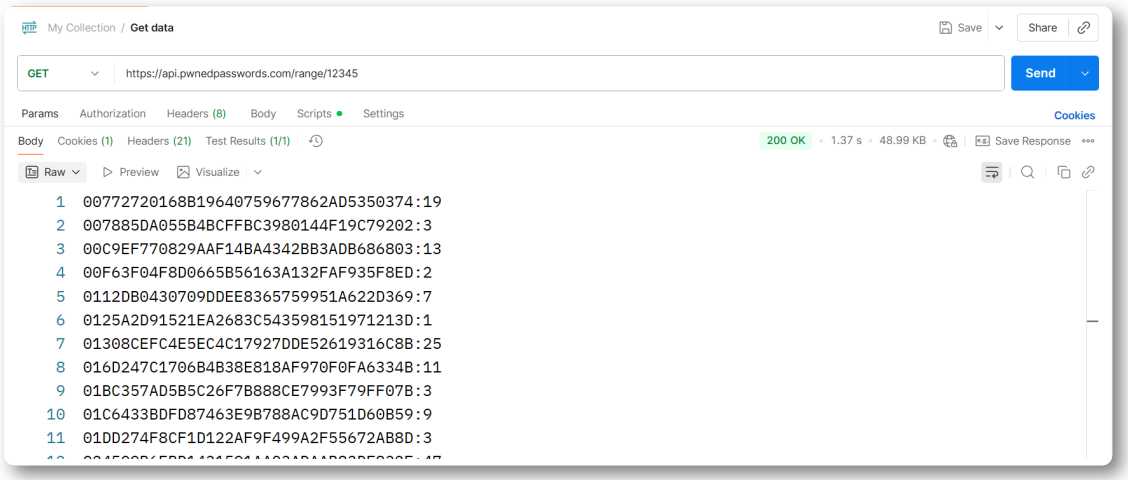
https://haveibeenpwned.com/api/v3/breaches?Domain=apk.tw



3. 實作請求二：以 `GET` 傳送請求 https://haveibeenpwned.com/api/v3/latestbreach 查詢最新外洩資訊



4. 實作請求三：以 `GET` 傳送請求 https://api.pwnedpasswords.com/range/{密碼 hash 前綴5個字元}，此查詢以 `12345` 當作前綴。



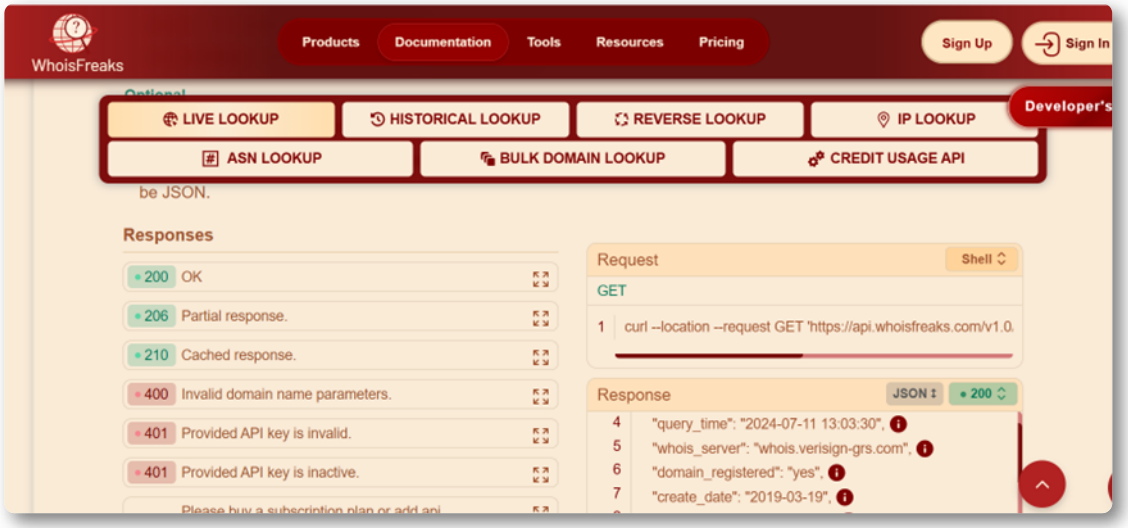
- 結論：
  本次實驗的 API 雖並不需要以 POST 方法實作封包架構，操作 POSTMAN 過程中可以理解到 GET 與 POST 在封包架構上的差異，若之後需要以 POST 送出封包，也能快速理解並上手。

此外，本次實作 API 之回應為 JSON 格式，經過此次實驗了解回應格式之內容架構，也能了解為何資料必須以特定通用格式傳送，不管是 XML 或 JSON 都代表直觀明瞭的資料格式，方便繼續解析或串接其他功能。

二、whoisfreaks API 實作

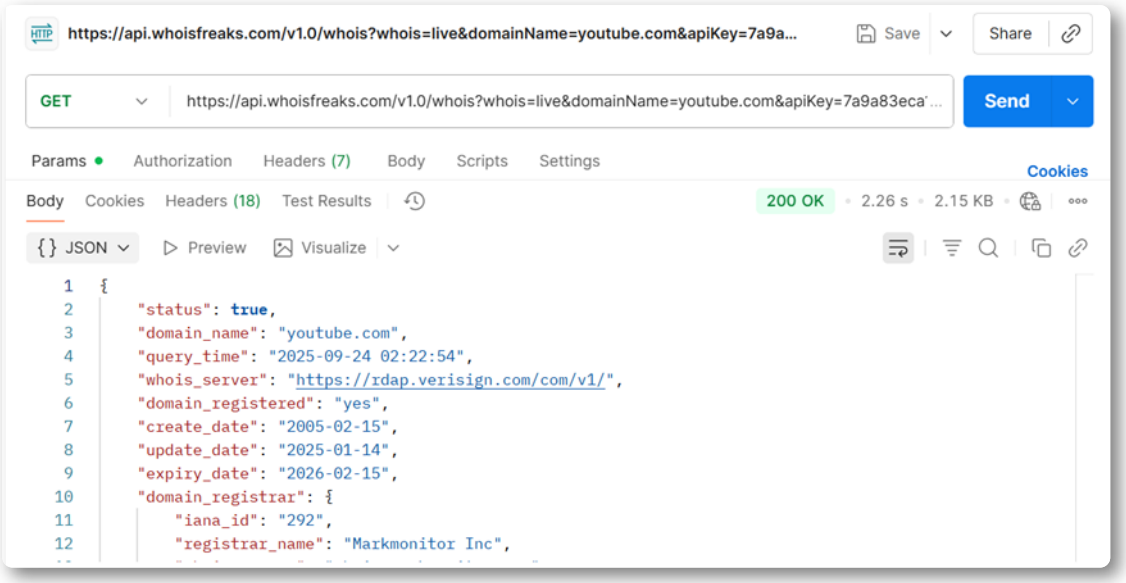
- 問題背景
  我選用的是whoisfreaks的api
  whoisfreaks 的核心功能：
  - 可以根據domain name去查詢他的一些歷史紀錄，包含創建日期（create date）、更新日期（update date）、到期日（expiry date）、註冊商（registrar）、註冊者（registrant contact）、管理與技術聯絡人、DNS 名稱伺服器等資訊
  - 另外也可透過域名擁有者名字 (owner)、公司名稱 (company)、email等關鍵字去反向查詢domain name
  - 也可以同時查詢多個domain name的資料，上傳域名的列表，並透過他們的系統做批次處理，但須注意一次送出的api請求，避免超出限制

- 執行方法與步驟
  1. 進到https://whoisfreaks.com/ 註冊帳號

  2. 到Documents頁面查看api相關服務與常見問題
     

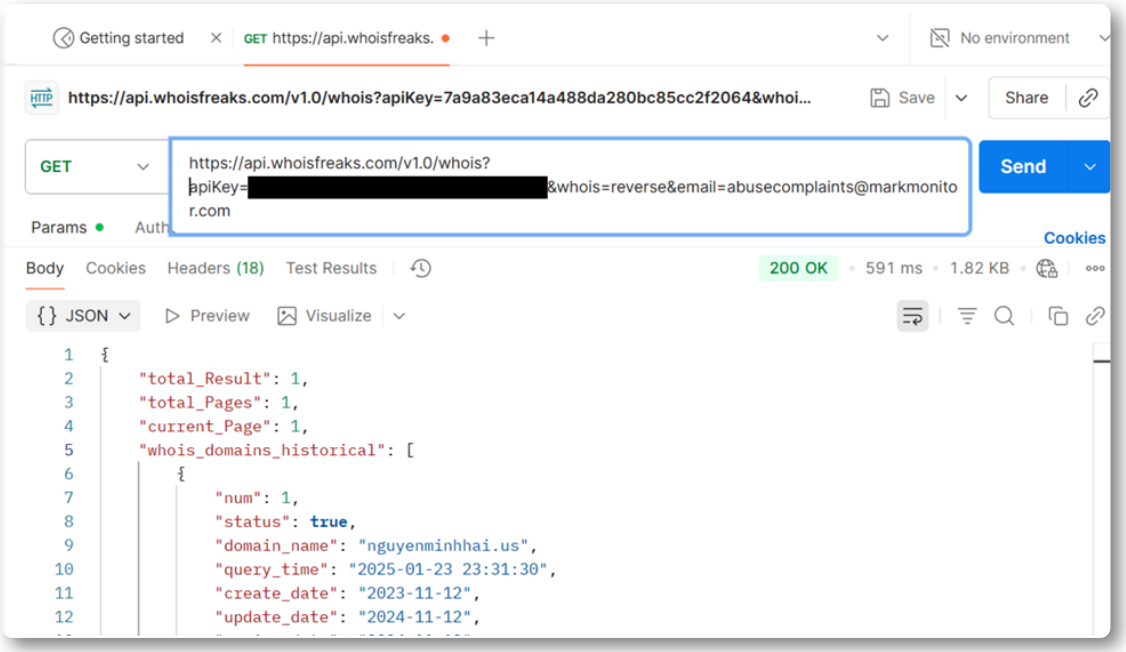
  3. 進到https://www.postman.com/ 做測試

  4. GET測試
     貼上https://api.whoisfreaks.com/v1.0/whois?whois=live&domainName=whoisfreaks.com&apiKey=API_KEY
     將domain name換成自己要測試的網域，API_KEY要放自己的Key

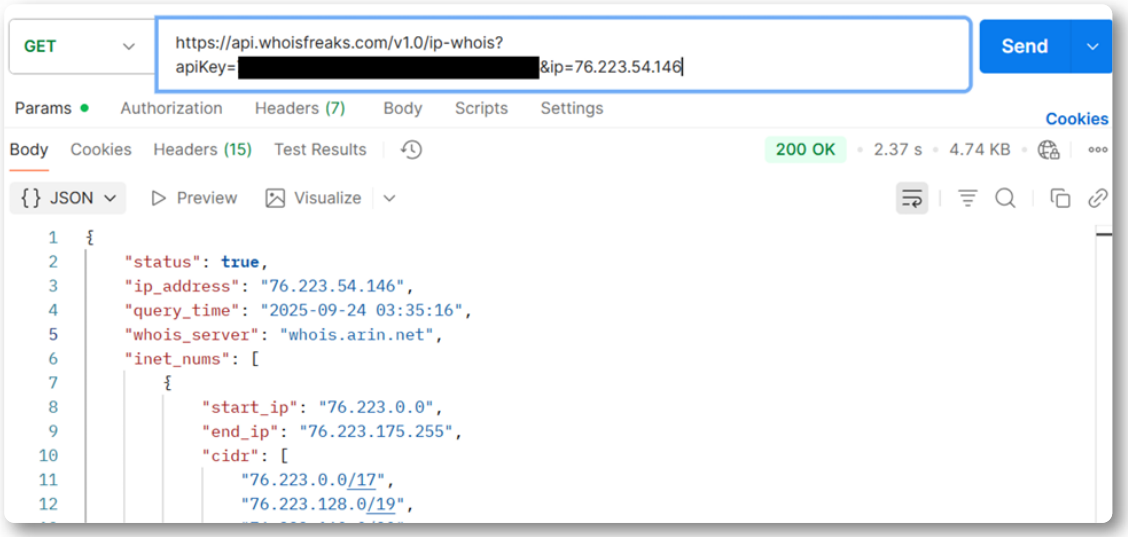


這邊我測試的是 youtube.com

5. Reverse測試



6. 透過IP位址查詢資料



- 結論

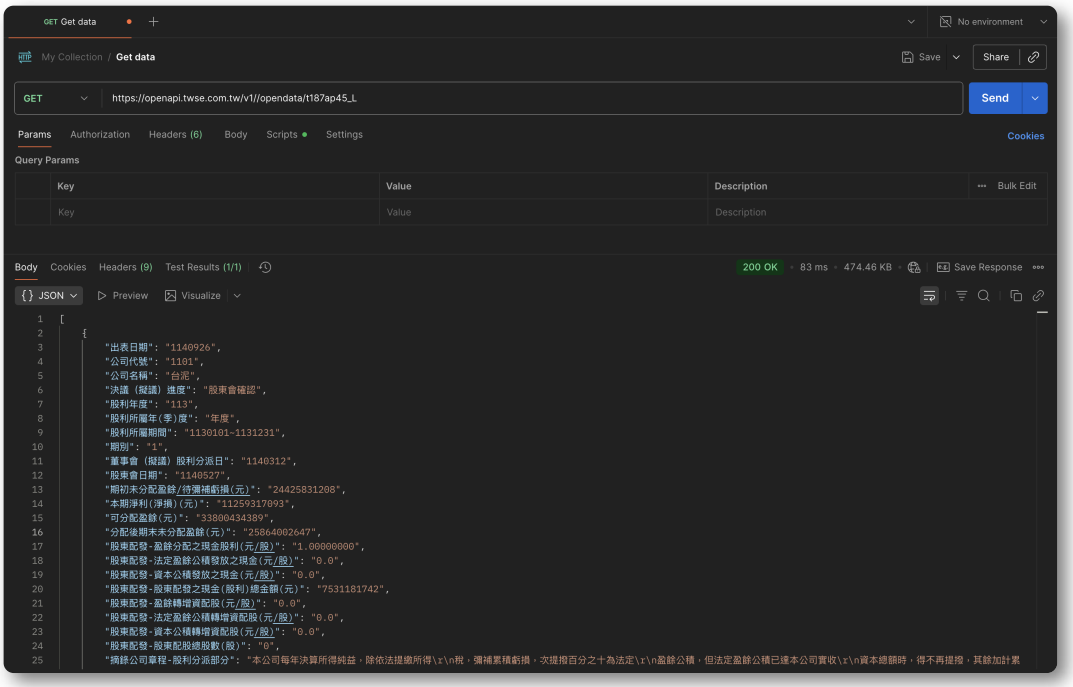
  除了上述的測試，whoisfreaks還有多個功能可以做測試。

  這次我透過 Postman 測試了 WhoisFreaks API，不同功能的表現各有特色。使用 Live Lookup 時，可以即時取得域名當前的註冊資訊，包含註冊商、到期日與名稱伺服器，對於快速確認域名狀態很實用。而透過 Historical Lookup，能夠看到域名過去的所有權與變更紀錄，對安全調查與品牌保護特別有幫助。Reverse WHOIS 則讓我能根據 email 或公司名稱反查相關域名，適合做威脅情報分析。整體來說，在 Postman 上操作很直覺，只要帶上 API key 與參數就能清楚看到 JSON 格式的結果，對測試與整合系統都相當方便。

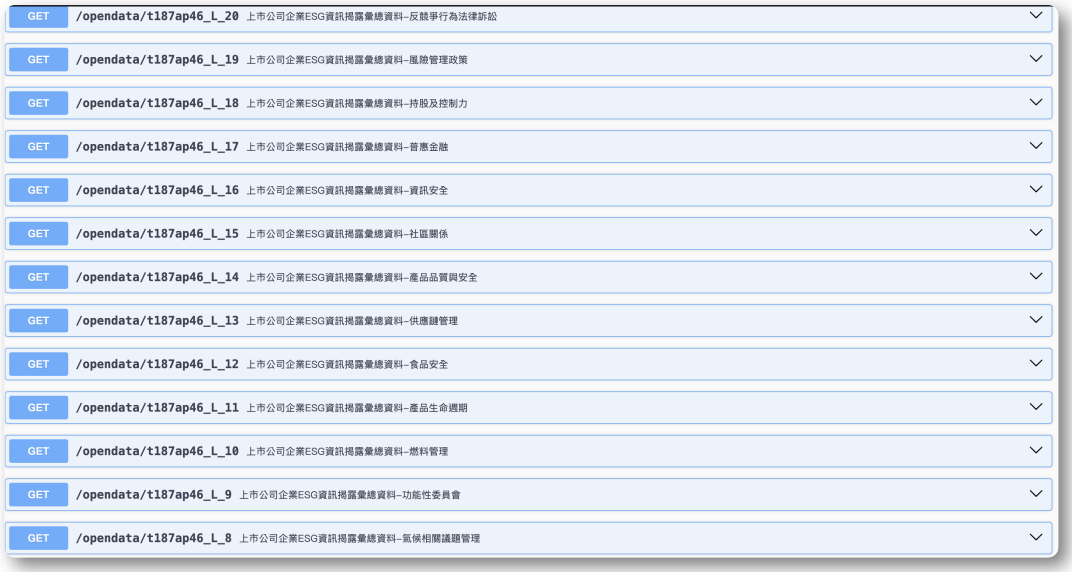
三、臺灣證券交易所 OpenAPI 實作

- 問題背景
  - 台灣證券交易所（TWSE）是在政府推動建立健全資本市場的背景下，於 1961 年成立的民營公司組織。
  - 負責經營台灣唯一的證券集中交易市場，為企業籌資和民眾投資提供平台。
  - 此 API 提供給客戶進行程式交易和金融數據串接，讓使用者可自行開發交易程式或串接程式，以取得原始的即時量價數據，達成自動化交易的目的。

- 執行方法與步驟
  - 公司治理
    - 可了解上市公司的營運與管理狀況
    - 可利用 `GET https://openapi.twse.com.tw/v1//opendata/t187ap45_L` 來查詢上市公司股利分派情形



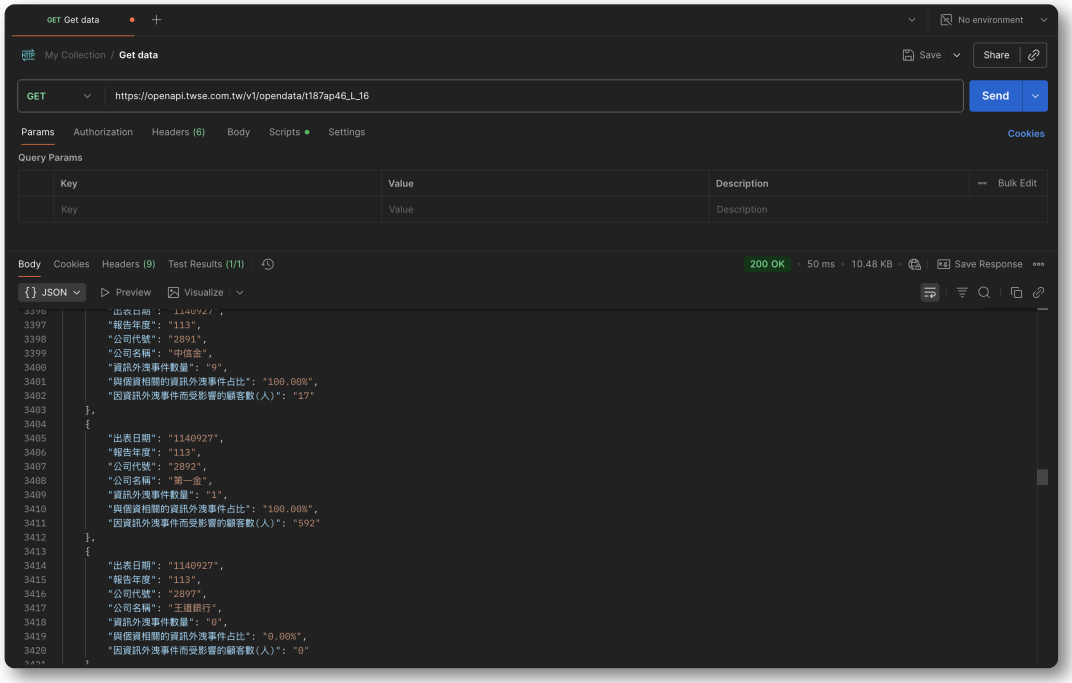
該網頁也有將各家上市公司企業的EAG資訊揭露彙整分門別類，如下圖所示：



以資訊安全為例，可利用

`GET https://openapi.twse.com.tw/v1/opendata/t187ap46_L_16`

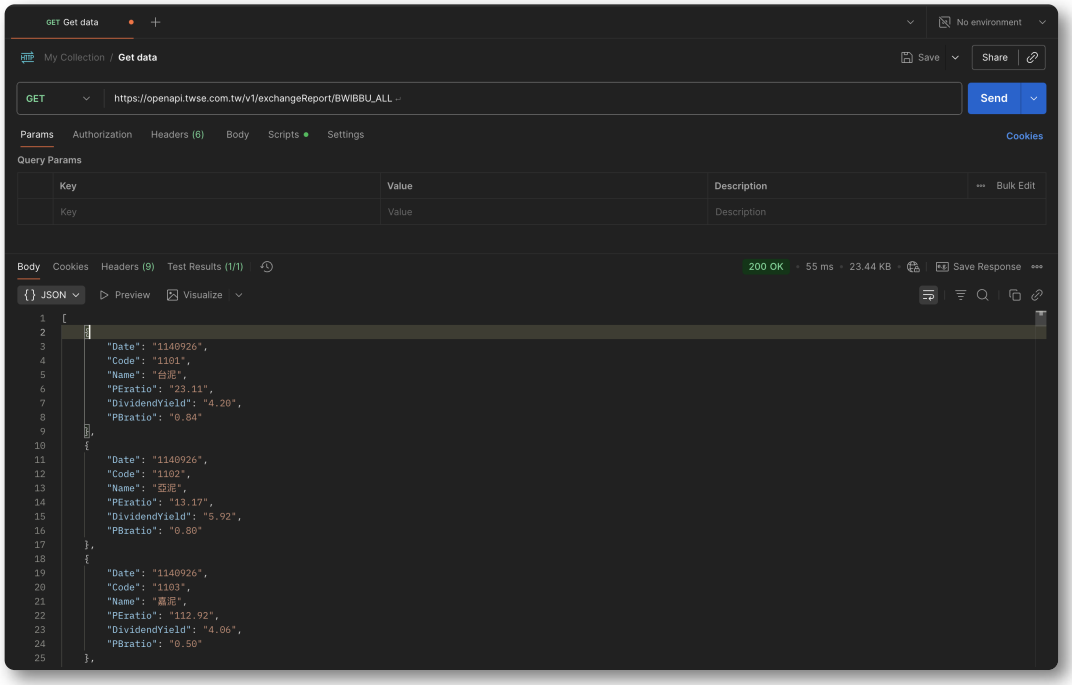
來查詢上司公司的資訊外洩事件數量、因外洩事件影響人數等



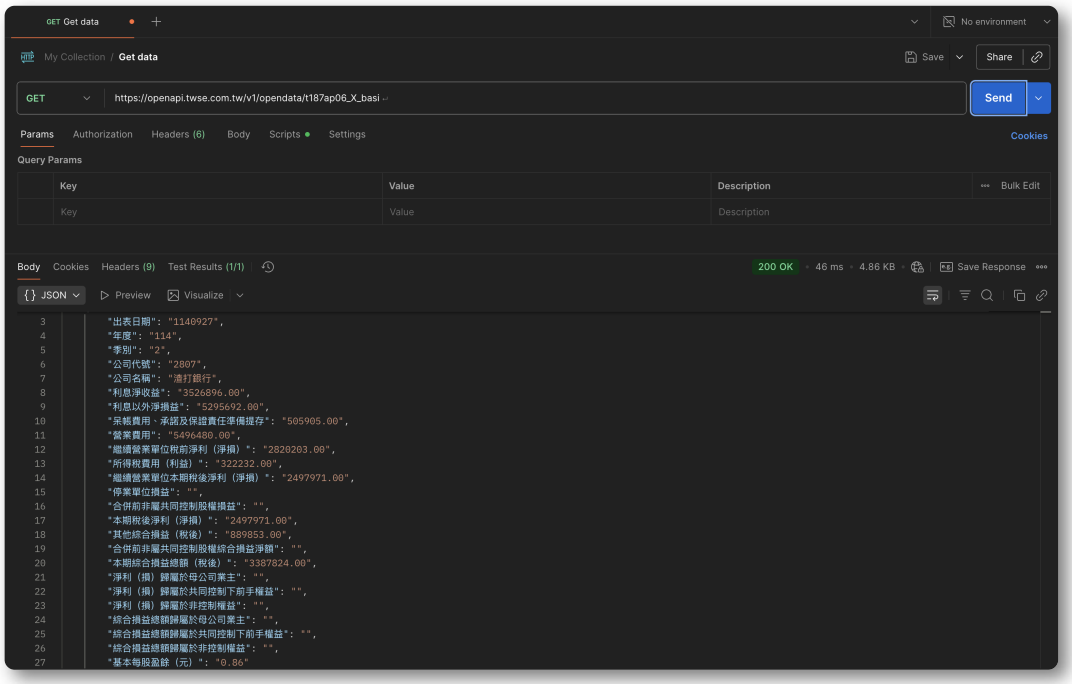
- 證卷交易
  - 可查詢公司在交易市場上的資訊做近一步利用
  - 可利用 `GET https://openapi.twse.com.tw/v1/exchangeReport/BWIBBU_ALL` 來查詢上市公司上市個股日本益比、殖利率及股價淨值比（依代碼查詢）

    response 欄位解釋：
  - PEratio： 本益比
  - DividendYield: 殖利率

- PBratio: 股價淨值比

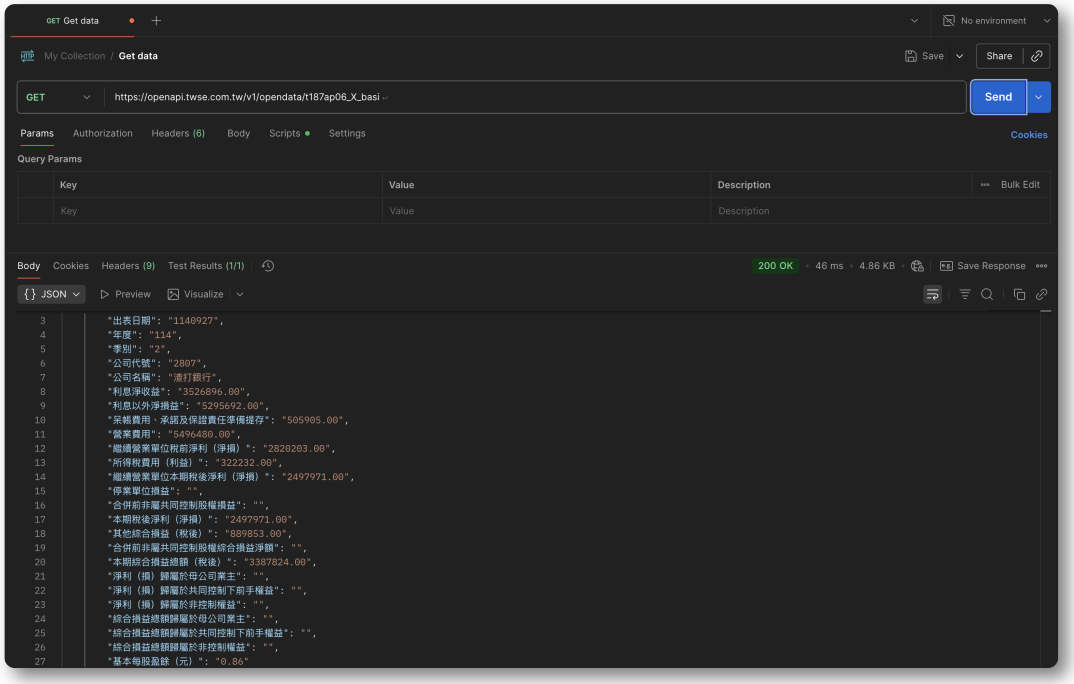


- 財務報表
  - 可查詢公發公司或上市公司的資產負債表/綜合損益表
  - 可利用 `GET https://openapi.twse.com.tw/v1/opendata/t187ap06_X_basi`



- 指數
  - 每日上市上櫃市場成交資訊，幫助投資人可快速了解當日市場整體表現。
  - response 欄位解釋：
    - FormosaIndex：發行量加權股價指數
    - Change：漲跌點數

- 可利用 `GET https://openapi.twse.com.tw/v1/opendata/t187ap06_X_basi`



- 結論

1. 學到的內容

- 理解 API 結構：透過 Postman 測試，學會如何設定請求、查看回應格式（JSON），並理解欄位意義。
- 資料解析能力：學到如何解讀像 PEratio、DividendYield、FormosaIndex 等數據，將原始回應轉換成有意義的資訊。
- 工具使用經驗：熟悉 Postman 介面，可以快速驗證 API 是否能正確回應並觀察資料內容。

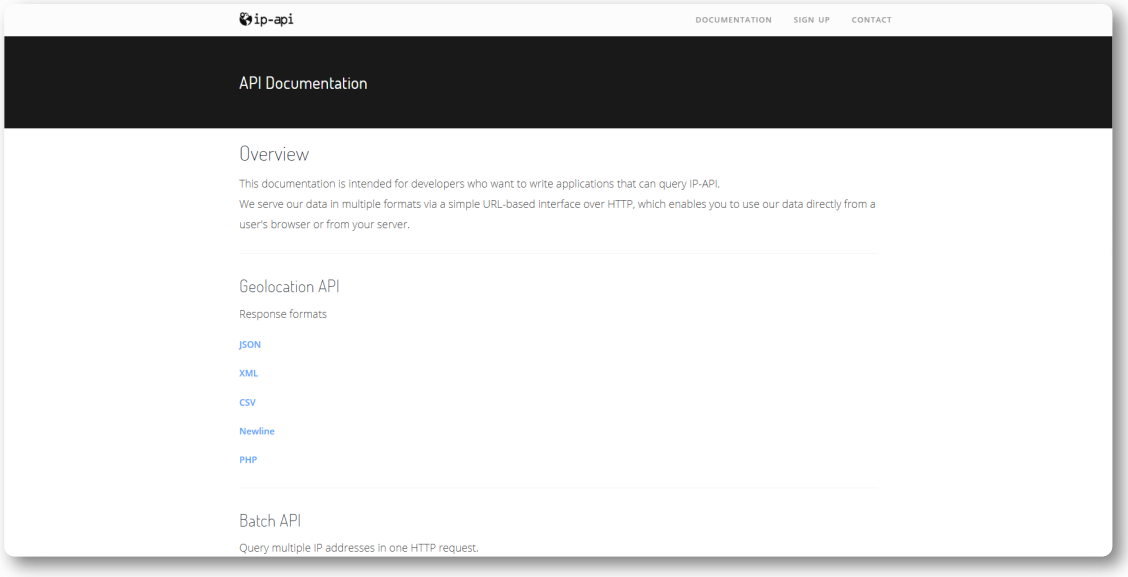
2. 可以應用的地方

- 投資決策：將 API 回傳的數據（本益比、殖利率、大盤指數）作為投資分析的依據。
- 自動化數據收集：未來可以把這些 API 整合進程式或報表，定期自動更新股市資訊。
- 學術/專案應用：在課堂作業、研究或專案中，利用這些公開資料做數據分析、視覺化，增進專業報告的價值。
- 延伸開發：作為金融應用（例如投資儀表板、風險評估工具）的資料來源。

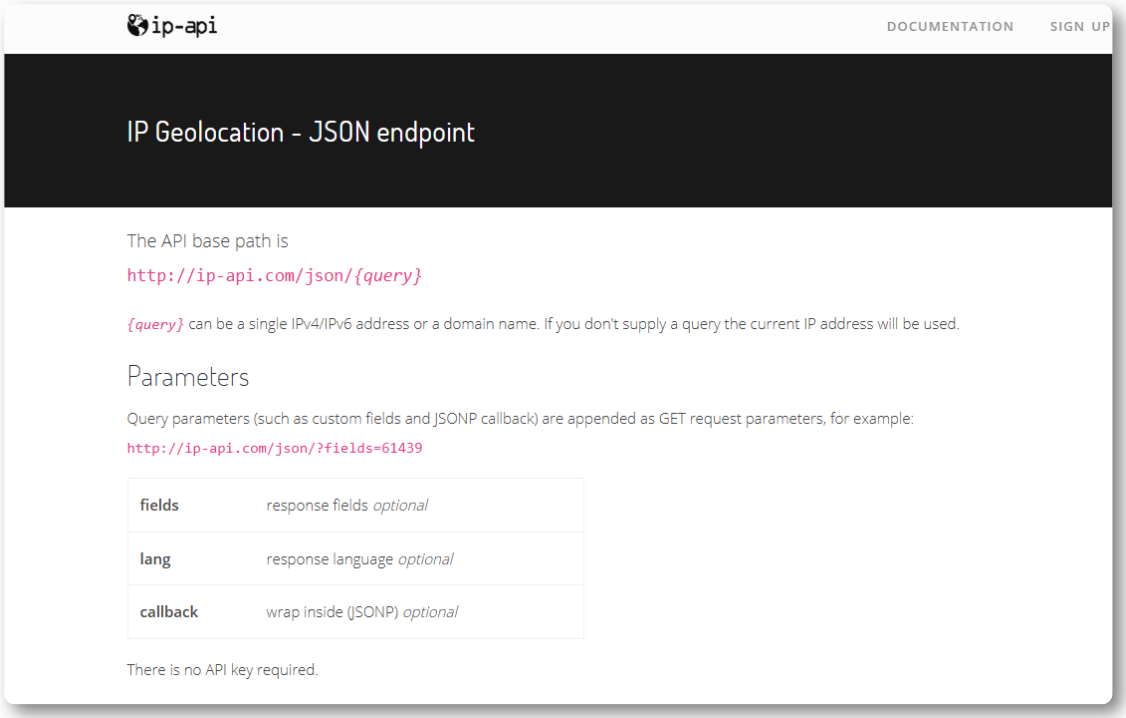
四、IP 威脅情報及地理定位 (Geolocation) API 實作

- 問題背景
  - 在資安分析中，追蹤惡意 IP 位址的來源或確認可疑連線的地理位置是常見的第一步。
  - IP Geolocation 屬於 OSINT (開源情報) 的基礎應用，可快速判斷連線的國家、網路服務提供商 (ISP) 或是否被標記為惡意節點。
  - 本次實作將使用公開且免費的 Geolocation API 查詢 IP 的地理位置資訊，作為資安調查的起點。

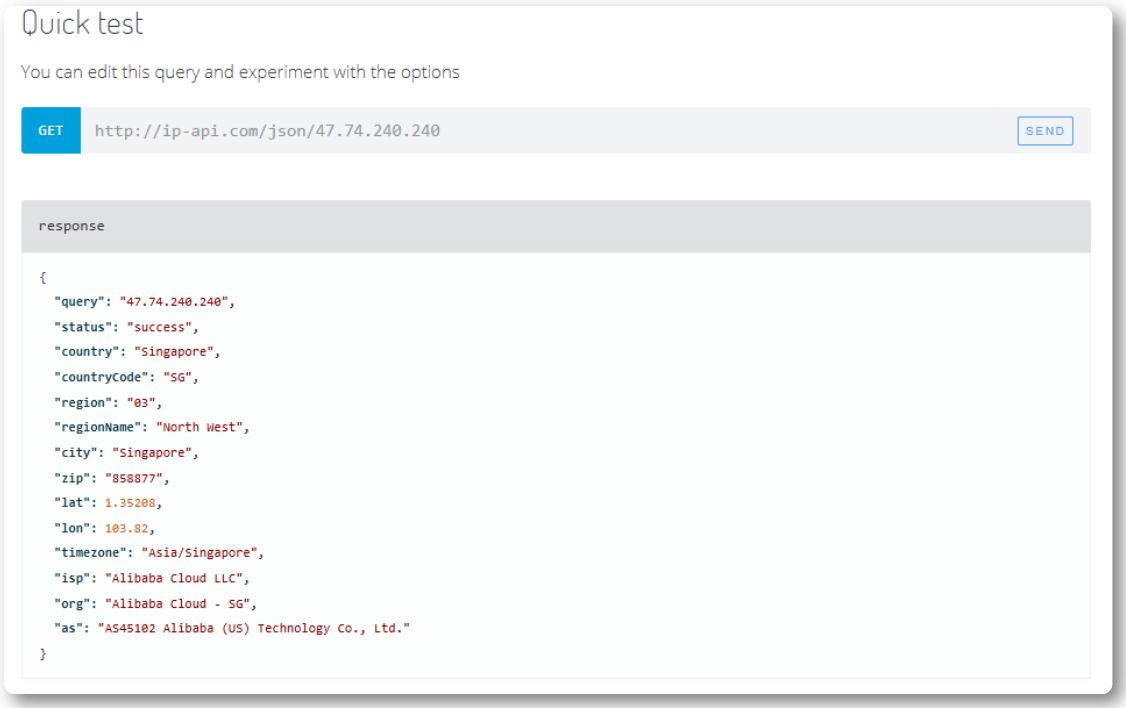
- 執行方法與步驟
  1. 鎖定 API： 選擇一個知名的開放 IP Geolocation API，例如 ip-api.com，它通常無需 API Key 即可進行基本查詢。



2. 確定 API 端點： 使用查詢單一 IP 位址的固定 API 端點。

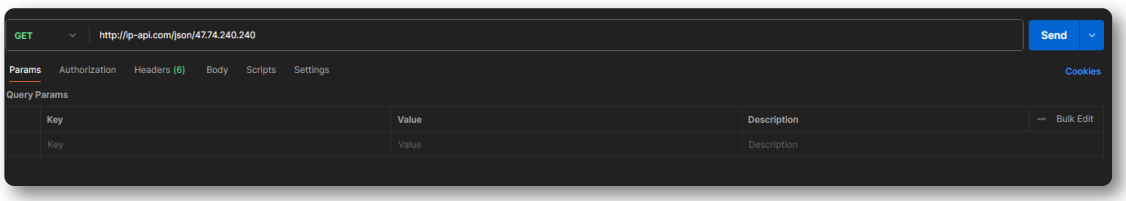


- 實作請求： 以 GET 傳送請求至指定的 JSON 端點，查詢一個國際雲端服務的 IP：http://ip-api.com/json/47.74.240.240 (此為阿里巴巴雲的 IP 位址)

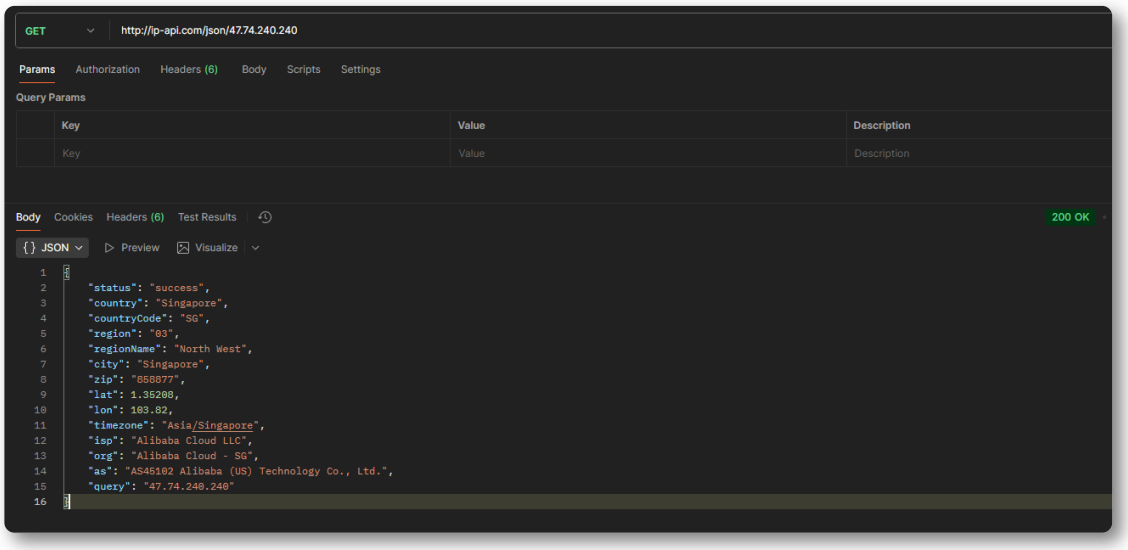


3. Postman 實際測試：

- 操作： 在 Postman 中選擇 GET 方法，貼上上方 URL 後點擊 Send。



- 結果與截圖： 確認回應狀態碼為 200 OK，並截圖整個 Postman 畫面 (包含請求 URL、狀態碼及 JSON 回應本文)。



- 簡要說明： 根據 Postman 實際傳送 GET 請求後，確認回應狀態為 success (成功)。JSON資料顯示，查詢的 IP 位址 47.74.240.240 來自新加坡 (Singapore)，其網路服務提供商 (ISP) 和組織 (Org) 皆為 Alibaba Cloud LLC (阿里巴巴雲)。這代表該 IP 是一個雲端服務器的節點。在資安分析中，如果看到攻擊或可疑連線來自知名雲服務商的 IP，則通常需要進一步追查該雲主機上的具體租戶和活動，這證明了該 API 能夠有效進行跨國基礎設施的資安情資收集。

4. 解析回應內容 (結構確認)： 針對 API 回傳的 JSON 結構，理解各欄位意義：

- status：回應狀態 (success/fail)
- country：IP 所屬國家
- city：IP 所屬城市
- isp：網路服務提供商 (ISP)
- query：查詢的 IP 位址

- 結論
  - 學到的內容
    - 資安情資收集： 了解如何使用基礎的 OSINT (開源情報) 工具，透過 IP 查詢來定位潛在威脅的地理位置。
    - 無 Key 存取： 成功串接不需要 API Key 的公開服務，熟悉基礎 API 存取流程。
    - 資訊欄位判讀： 學會判讀 country、city、isp 等欄位，並將這些資訊用於情境分析。
  - 可以應用的地方
    - 防火牆規則強化： 程式化地查詢 IP 來源，並根據國家或 ISP 封鎖特定惡意連線。

- 日誌分析輔助： 將伺服器日誌中的 IP 位址與 Geolocation API 串接，快速識別異常登入或攻擊的地理來源。
- 專案實作： 作為網路監控或資安儀表板的基礎數據來源，豐富專案的實用性。