AIS3

教育部先進資通安全實務人才培育計畫

112年度新型態資安實務暑期課程

NOSINT - 反情蒐瀏覽器擴充元件開發

M2 吳冠廷、陳俊誠、吳奕萱、施育凱

Outline

- Motivation
- Concept
- Architecture
- Development
- Intelligence Collecting
- Risk Index
- Demo
- References

Motivation

- 近年來詐騙與釣魚網站非常盛行，一不注意個資就被竊取洩漏，為了保護我們的個資，因此我們想要開發一個能夠檢查網站洩漏風險的擴充元件。

What is NOSINT?

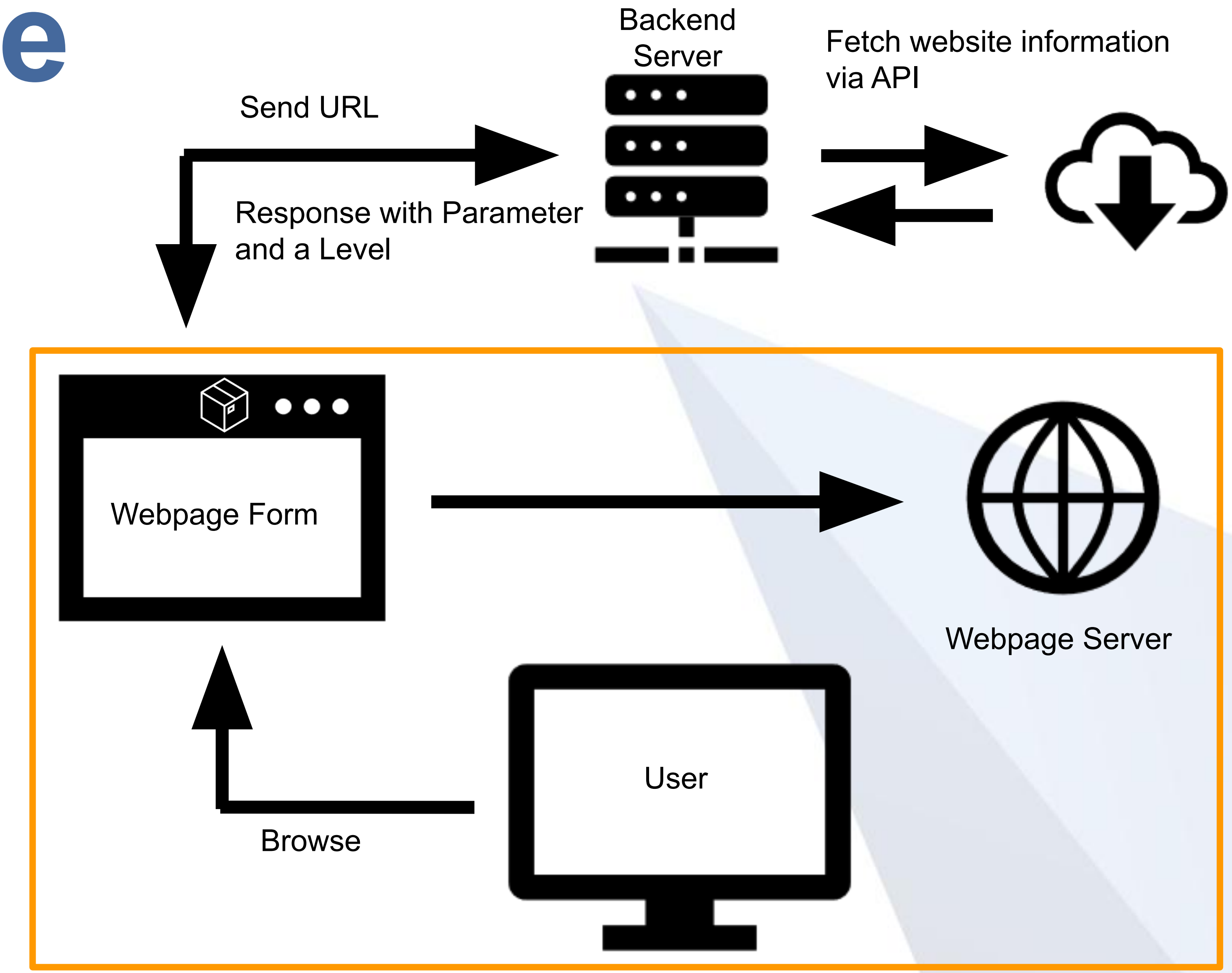
NYPD
OSINT
NOSINT

Concept

- Anti-OSINT
- 在使用者送出敏感資料之前發出警告
- 計算網站之危險程度
- 評估網站之潛在風險

Architecture

- 使用者透過瀏覽器瀏覽網頁表單
- 擴充元件與後端伺服器溝通
- 後端伺服器透過 API 查詢網站相關情資
- 擴充元件在使用者送出表單時顯示相關情資提示


Backend Server
Send URL
Response with Parameter and a Level
Fetch website information via API
Webpage Form
Webpage Server
User
Browse

Development

Front-end & Extension Develop

- 採用 Chrome Extension API
  - Manifest v3 - 因為 v2 在 2021 年 9 月後不再維護，Google 逐漸停止提供對其支援。
- 架構簡單分成三個部件
  - Popup: 用來顯示擴充元件內容，可將其視為一個網頁
  - Background Worker: 背景腳本，用來處理主要任務，可以長時間運行指令
  - Content Script: 此腳本會注入到分頁的視窗中，可以與該分頁進行互動(透過DOM或JS)
- 部件之間可以透過 API 進行溝通
  - Chrome Extensions Message passing

Development

Front-end & Extension Develop

popup

- 顯示網站相關情資
- 擴充元件功能選項

background worker

- 部件間通訊溝通
- 後端訪問與資料接收

content script

- 蒐集網頁資訊
    - URL

Development

Front-end & Extension Develop

popup

- ~~顯示網站相關情資~~
- 擴充元件功能選項

background worker

- 部件間通訊溝通
- 後端訪問與資料接收

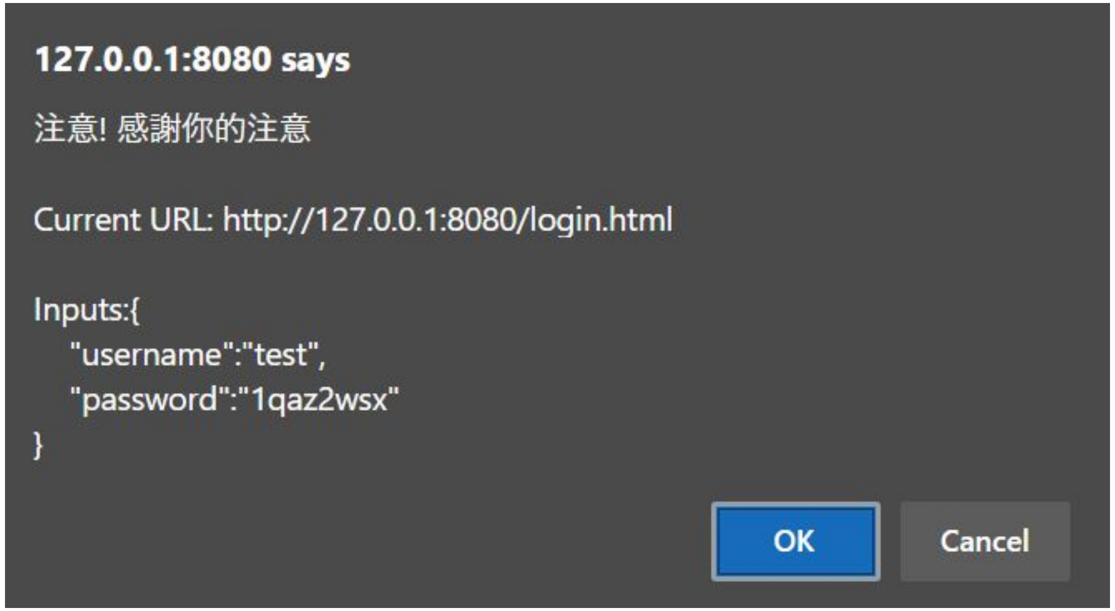
content script

- 蒐集網頁資訊
  - ○ URL

Development

Front-end & Extension Develop

- 為什麼想要 Popup 顯示網站相關情資
  - 因為最開始的版本顯示相關情資介面長這樣

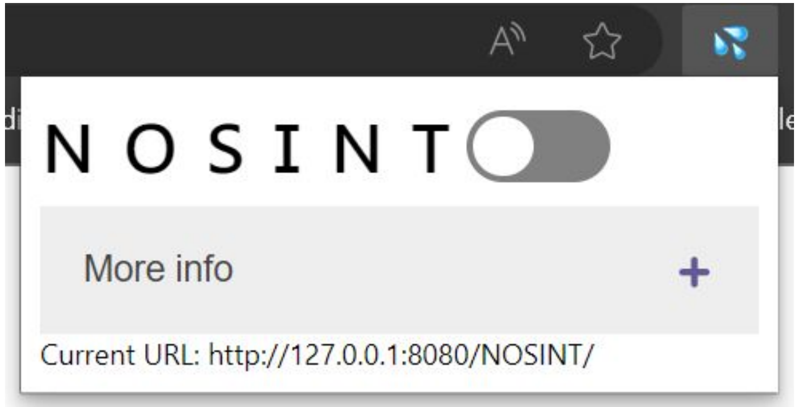


127.0.0.1:8080 says

注意! 感謝你的注意

Current URL: http://127.0.0.1:8080/login.html

```
Inputs:{
    "username":"test",
    "password":"1qaz2wsx"
}
```



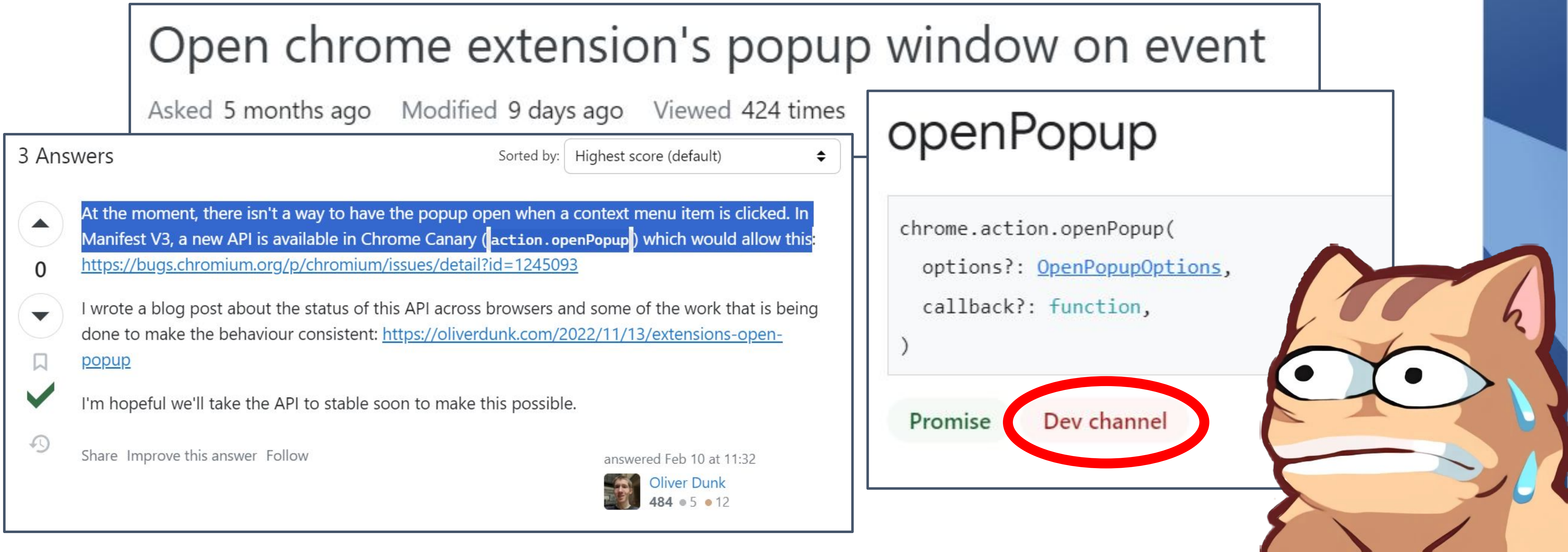
Current URL: http://127.0.0.1:8080/NOSINT/

Concept

Development

Front-end & Extension Develop

- 理想很豐滿，現實很骨感（stackoverflow.com）



Open chrome extension's popup window on event

Asked 5 months ago Modified 9 days ago Viewed 424 times

3 Answers

Sorted by: Highest score (default)

0

At the moment, there isn't a way to have the popup open when a context menu item is clicked. In Manifest V3, a new API is available in Chrome Canary (`action.openPopup`) which would allow this: https://bugs.chromium.org/p/chromium/issues/detail?id=1245093

I wrote a blog post about the status of this API across browsers and some of the work that is being done to make the behaviour consistent: https://oliverdunk.com/2022/11/13/extensions-open-popup

I'm hopeful we'll take the API to stable soon to make this possible.

answered Feb 10 at 11:32

Oliver Dunk

484 ●5 ●12

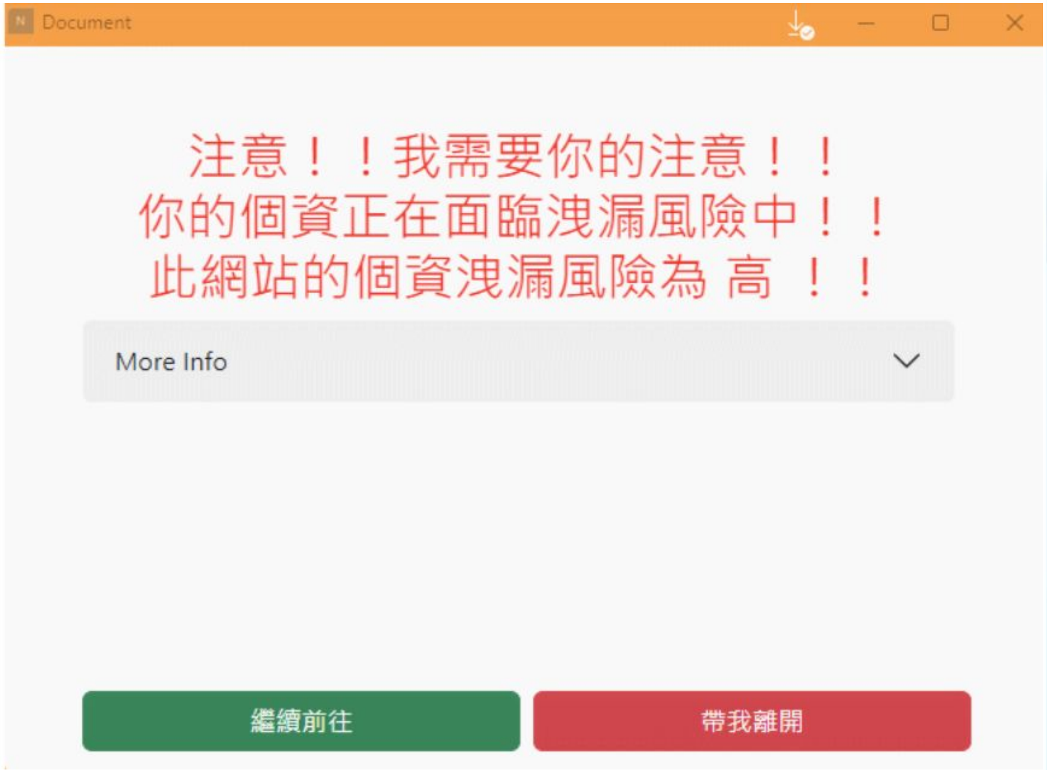
openPopup

```
chrome.action.openPopup(
  options?: OpenPopupOptions,
  callback?: function,
)
```

Development

Front-end & Extension Develop

- Plan B!
  - chrome.windows.create
    - 這樣至少能用 html 與 css 語法



注意！！我需要你的注意！！
你的個資正在面臨洩漏風險中！！
此網站的個資洩漏風險為 高 ！！

Intelligence Collecting

VirusTotal API

- last_analysis_stats
- registrar
- reputation
- last_https_certificate
- total_votes

Intelligence Collecting

Have I Been Pwned API

- PwnCount
- DataClasses

PhishTank DB

Intelligence Collecting

- Trend Micro
- DomainTools
- RedQueen威
- Myip.ms
- Scamadviser rvices
- WHOIS Searc s
- AlienVault - C
- MalwareBaza
- Censys Searc
- Interactive O
- SSLBL | Blacklist

Risk Index

Risk Index 1

$$\text{las1} = \begin{cases} (100 - |(m+s) \cdot 1.35 - h| \cdot 0.3) \cdot 0.35 \\ \text{if} \qquad\qquad (m+s) > 5, \\ (100 - |(m+s) \cdot 1.35 - h| \cdot 0.3) \cdot 0.35 \end{cases}$$

$$\text{m} = \mathit{malicious}$$
$$\text{s} = \mathit{suspicious}$$
$$\text{h} = \mathit{harmless}$$

$$rp1 = (100 - \text{reputation} \cdot 0.2) \cdot 0.1$$

$$Time_1 = \begin{cases} 0 & if \;\; expired\ days \le 0 \\ \frac{expired\ days}{365} \cdot 10 & if \;\; 0 < expired\ days \le 365 \\ 10 & if \;\; expired\ days > 365 \end{cases}$$

$$\text{vote1} = \big(1 \text{ if } [{}'total\_votes'][{}'harmless'] < [{}'total\_votes'][{}'malicious'] \text{ else } 0\big) \cdot 10$$

$$PhishTank_1 = \begin{cases} 0 & \text{if is not in PhishTank DB} \\ 5 & \text{if is in PhishTank DB} \end{cases}$$

$$pc1 = \frac{\text{PwnCount}}{10000} \cdot 0.05 \quad \text{(upperbound 10000)}$$

$$pd1 = (ID \cdot 20 + Bday \cdot 10 + TEL \cdot 15 + Email \cdot 15 + \cdot 10 + add \cdot 20 + Psw \cdot 15) \cdot 0.15$$

$$dc1 = (10 \cdot \text{dataclasses}) \cdot 0.1 \quad \text{(upperbound 10)}$$

$$\text{cal\_one} = (\text{las1} + \text{rp1} + \text{time1} + \text{vote1} + \text{ph1} + \text{pc1} + \text{pd1} + \text{dc1})$$

Risk Index 2

$$LastAnalysisStats_2 = malicious \cdot 7 \cdot 0.4 + suspicious \cdot 3 \cdot 0.2$$

$$Reputation_2 = \begin{cases} (100 - reputation) \cdot 0.05 & \text{if } reputation < 100 \\ 0 & \text{if } reputation \geq 100 \end{cases}$$

$$expired\ days = today's\ date - expiry\ date$$

$$Time_2 = \begin{cases} 0 & \text{if } expired\ days \leq 0 \\ \frac{expired\ days}{365} \cdot 10 & \text{if } 0 < expired\ days \leq 365 \\ 10 & \text{if } expired\ days > 365 \end{cases}$$

$$TotalVote_2 = \frac{malicious}{harmless + malicious} \cdot 50 \cdot 0.05$$

$$PhishTank_2 = \begin{cases} 0 & \text{if is not in PhishTank DB} \\ 5 & \text{if is in PhishTank DB} \end{cases}$$

$$PwnCount_2 = \begin{cases} \frac{PwnCount}{10000} \cdot 50 & \text{if } PwnCount \leq 10000 \\ 50 & \text{if } PwnCount > 10000 \end{cases}$$

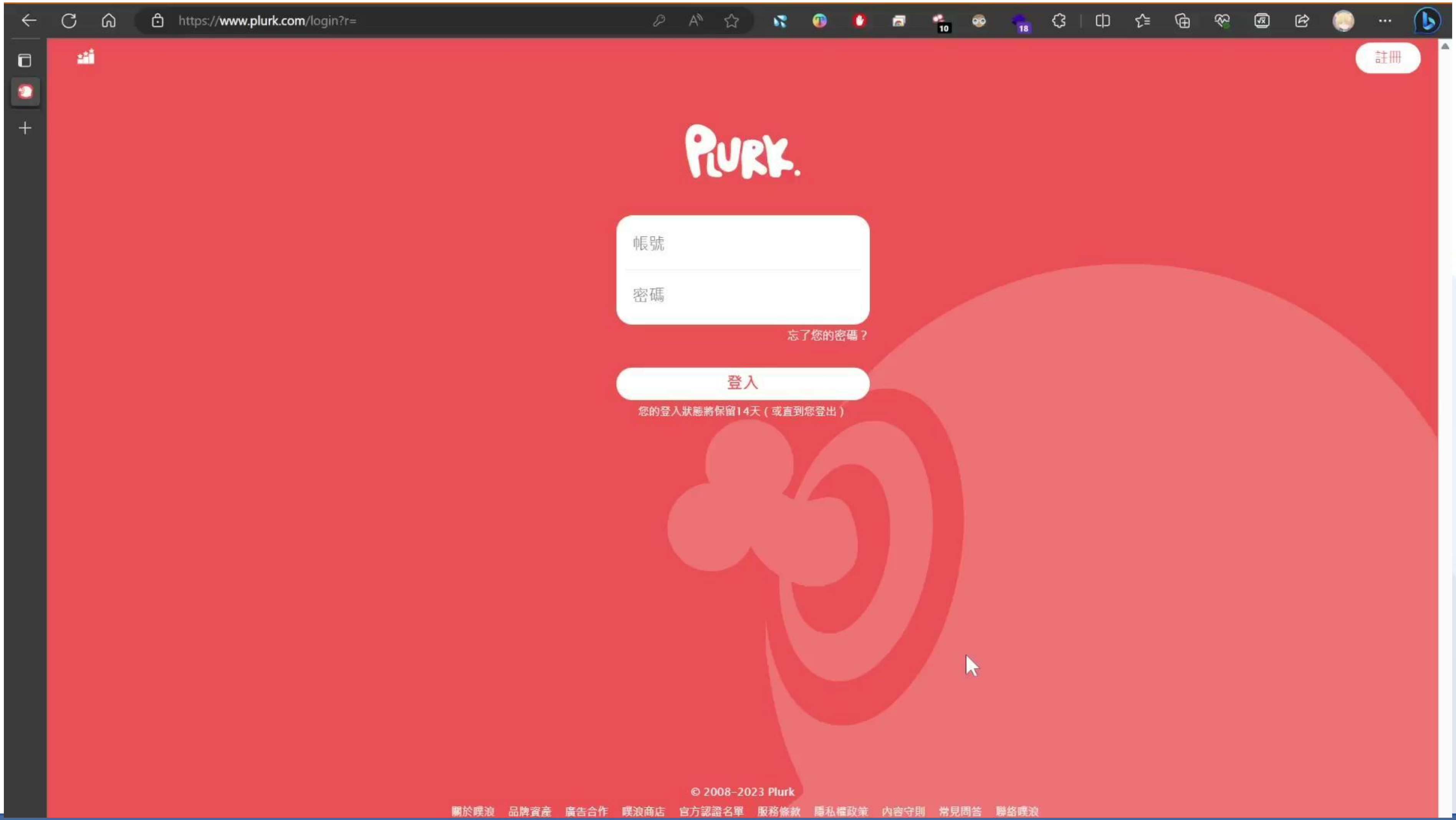
$$DataClasses_2 = \begin{cases} Data\ Classes \cdot 10 & \text{if } Data\ Classes \leq 5 \\ 50 & \text{if } Data\ Classes > 5 \end{cases}$$

$$HIBP_2 = (PwnCount_2 + DataClasses_2) \cdot 0.05$$

$$PersonalData_2 = (Name \cdot 5 + ID \cdot 30 + Birth \cdot 5 + Phone \cdot 10 + Email \cdot 10 + Address \cdot 25 + AccPwd \cdot 15)$$

$$RiskIndex_2 = LastAnalysisStats_2 + Reputation_2 + Time_2 + TotalVote_2 + PhishTank_2 + HIBP_2 + PersonalData_2$$

Demo

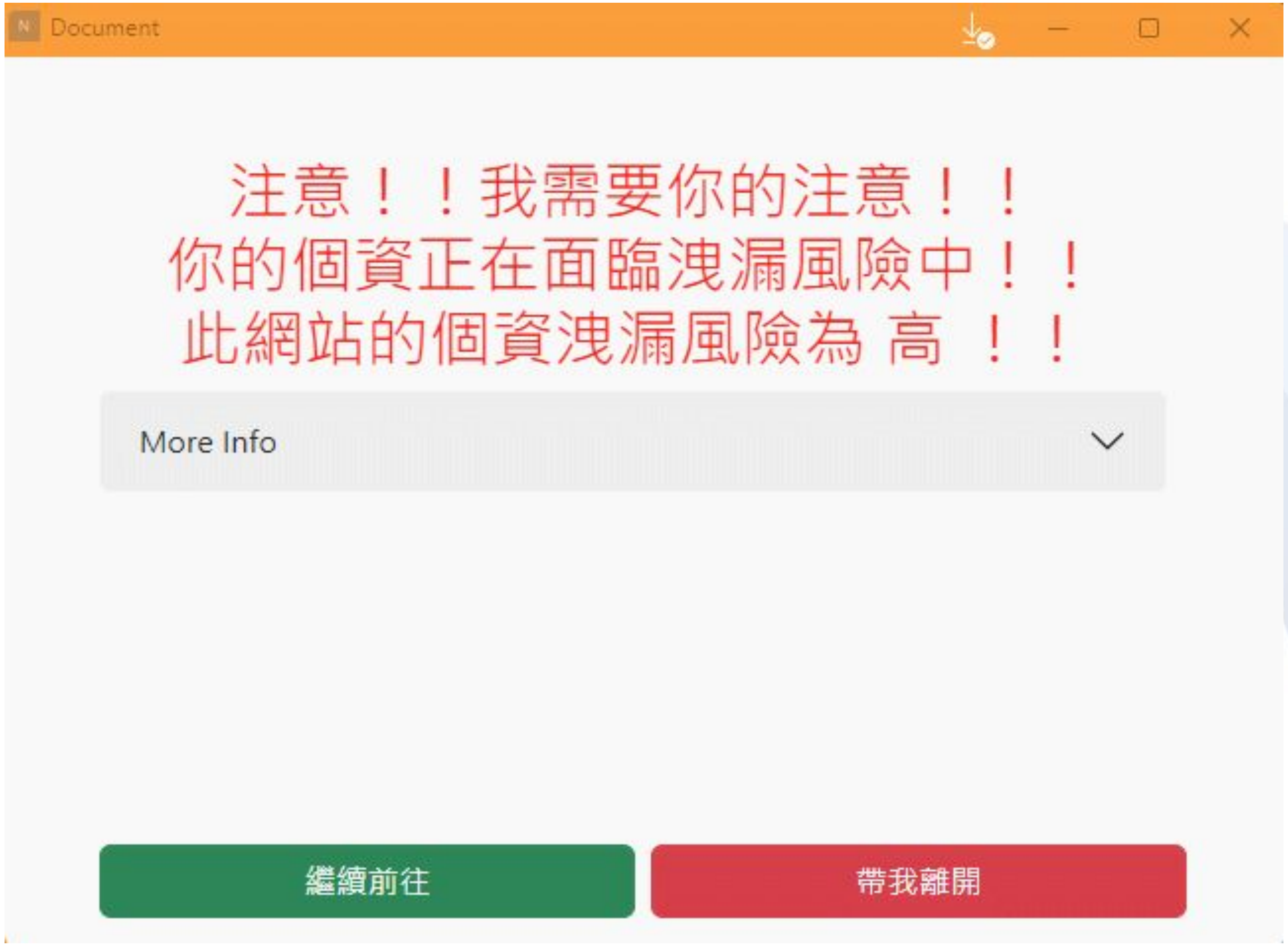

https://www.plurk.com/login?r=
註冊
PLURK.
帳號
密碼
忘了您的密碼？
登入

您的登入狀態將保留14天（或直到您登出）

© 2008–2023 Plurk

關於噗浪 品牌資產 廣告合作 噗浪商店 官方認證名單 服務條款 隱私權政策 內容守則 常見問答 聯絡噗浪

Demo



注意！！我需要你的注意！！
你的個資正在面臨洩漏風險中！！
此網站的個資洩漏風險為 高 ！！

References

Front-end & Extension Develop

- GoogleChrome/chrome-extensions-samples: Chrome Extensions Samples (github.com)
- Overview of the Chrome Extension Manifest V3 - Chrome Developers
- chrome.action - Chrome Developers
- Open chrome extension's popup window on event - Stack Overflow
- Using the Fetch API - Web APIs | MDN (mozilla.org)
- How To Create a Collapsible (w3schools.com)
- javascript - How to launch a new window in Google Chrome Extension - Stack Overflow
- John Cena "are you sure about that?" GREENSCREEN (IMPROVED VERSION) - YouTube
- chrome.windows - Chrome Developers
- Embed videos & playlists - YouTube Help (google.com)
- <iframe>: The Inline Frame element - HTML: HyperText Markup Language | MDN (mozilla.org)

References

Intelligence Resouces

- https://haveibeenpwned.com/PwnedWebsites
- https://www.virustotal.com/gui/home/url
- https://transparencyreport.google.com/safe-browsing/search
- https://github.com/OWASP/ASVS/tree/v4.0.3/4.0/en

Thanks for Listening!