區網網站被駭處理經驗分享

中興大學| 計資中心| 研發組| 台中區網 | 張雅嵐

被駭時間軸

2016/03-04

01 第一次被駭

網頁置換

2017/06

02 第二次被駭

日文關鍵字

攻擊

被駭畫面


Google
台中區網
全部 新聞 地圖 圖片 影片 更多 設定 工具
約有 962,000 項結果 (搜尋時間：0.52 秒)
川口技研 腰壁用ホスクリーン 上下式ハイグレードタイプ ライトブロン...
www.tcrc.edu.tw/ ▾ 翻譯這個網頁
您的網頁不適合使用行動裝置瀏覽。
台中區網中心-最新消息台中區網中心台中區網中心搜尋...中心簡介年度記事概況介紹區網網路架構圖業務職掌區網中心各年度運作績效網路規範學網法規TANet相關 ...
(OS キャビネット) 大阪製罐（株）
ＯＳ デラックスキャビネットＤＸ型
最大積載 ... 台(入り数：-)JAN[-](ＯＳキ ...
余禎祥
余禎祥先生於本校資訊工程研究所畢業後，即任職本校資訊單位，以 ...
張本和
姓名：, 張本和. 出生年：. 任職單位. 台中縣教育網路中心. 學經歷 ...
蘇仕朋
一、蘇仕朋先生任職本校專任職員計17年，期間任勞任怨並善盡本分著 ...
前一個
號外！台中區網中心官方Line正式成立，趕快加入獲得最新消息吧 ...
黃永欽
黃永欽先生自任職於本校即開始協助各項行政工作的電腦化程式的 ...
tcrc.edu.tw 的其他相關資訊 »


TANet TCRC 臺中區域網路中心
Taichung Network Regional Center
最新消息
★出訪紀實
第十六次出訪記實
台中區網中心

被駭畫面


Google
台中區網
全部
新聞
地圖
圖片
影片
約有 962,000 項結果 (搜尋時間：0.52 秒)
翻譯這個網頁
頁庫存檔
類似內容
www.tcrc.edu.tw/
(OS キャビネット) 大阪製罐（株）
OS デラックスキャビネットDX型
最大積載 ... 台(入り数：-)JAN[-](OS
キ ...
張本和
姓名：, 張本和. 出生年：. 任職單位,
台中縣教育網路中心. 學經歷 ...
前一個
號外！台中區網中心官方Line正式成
立，趕快加入獲得最新消息吧 ...
tcrc.edu.tw 的其他相關資訊 »
webcache.googleusercontent.com/search?q=cache:0QIDDbW0oy8J:www.tcrc.edu.tw/+&cd=1&hl=zh-TW&ct=clnk&gl=tw
這是 Google 對 http://www.tcrc.edu.tw/ 的快取。這是該網頁於 2017年5月2日 02:35:16 GMT 顯示時的快照。
在此期間，目前網頁可能已經變更。
完整版
純文字版
檢視原始碼
提示：如要在這個網頁上快速尋找您所搜尋的字詞，請按下 Ctrl+F 鍵或 ⌘-F 鍵 (Mac)，然後使用尋找列進行搜尋。
川口技研 腰壁用ホスクリーン　上下式ハイグレードタイプ　ライトブロンズ 1セット（2本組）
物干しスタンド 物干しタオル 物干 物干し台
日用品雑貨・文房具・手芸→DIY・工具
商品名：川口技研 腰壁用ホスクリーン　上下式ハイグレードタイプ　ライトブロンズ 1セット（2本組）ライトブロンズ （LP-55-LB）物干しスタンド 物干しタオル 物干 物干し台
川口技研
GOOD DESIGN
ライトブロンズ
※イメージ画像
腰壁用ホスクリーン　上下式ハイグレードタイプ　ライトブロンズ　(LP-55-LB)
d&gtools
図：
品番：bHjPk14614
14000.0000円　8680.0000円
割引: 38%OFF
メーカー：

移除網址

查看 Google 搜尋結果中的頁庫存檔

頁庫存檔連結會顯示 Google 最近一次檢索網頁時儲存的網頁版本。

關於頁庫存檔連結

Google 會為每個網頁擷取快照備份，如果網頁之後無法顯示，備份就能派上用場。這些網頁隨即會納入 Google 的「頁庫存檔」，您只需點選 [頁庫存檔] 連結，畫面上就會顯示 Google 儲存的網站版本。

如果您要造訪的網站載入速度緩慢或是沒有回應，也可以改為查看頁庫存檔。

如何前往頁庫存檔連結

1. 在電腦上使用 Google 搜尋所需網頁。
2. 按一下該網站網址右邊的綠色向下箭頭。
3. 按一下 [頁庫存檔]。
4. 開啟頁庫存檔後，只要按一下目前網頁的連結，即可返回實際的線上網頁。

提示：如果想將某個頁庫存檔從 Google 搜尋結果中移除，請參閱要求 Google 移除已過時或已刪除的資訊 一

移除網址工具

「移除網址」工具可讓您暫時封鎖 Search Console 資源中的網頁，不讓這些網頁出現在 Google 搜尋結果中。如需封鎖其他類型的網頁，請參閱這裡的說明。

- 要求獲准後，封鎖效期大約只能維持 90 天的時間。90 天後，您所封鎖的資訊便會再次出現在 Google 搜尋結果中 (請參閱「永久移除內容」一節)。
- 您必須是 Search Console 中的資源擁有者，才能使用這個工具移除該資源對應的網址。如果您不是資源擁有者，請參閱這篇文章。

如何讓 Google 搜尋暫時停止顯示特定的 Search Console 資源網頁：

1. 開啟移除網址網頁。
2. 按一下 [暫時隱藏]。
3. 輸入要移除的圖片、網頁或目錄所在的**相對路徑**，然後按一下 [繼續]。這個路徑是 Search Console 資源根目錄的相對路徑，且開頭必須是 / 符號。
4. 在表單中選擇下列其中一項操作：

移除網址：

→把錯誤的頁面、快取和失效的網址..等，請 Google於搜尋引擎中下架移除

Search console

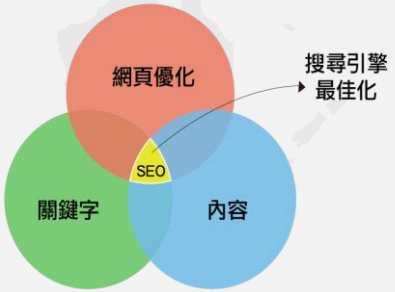
Google Search Console：

google提供給網站管理者提升**SEO**的工具

SEO，search engine optimization

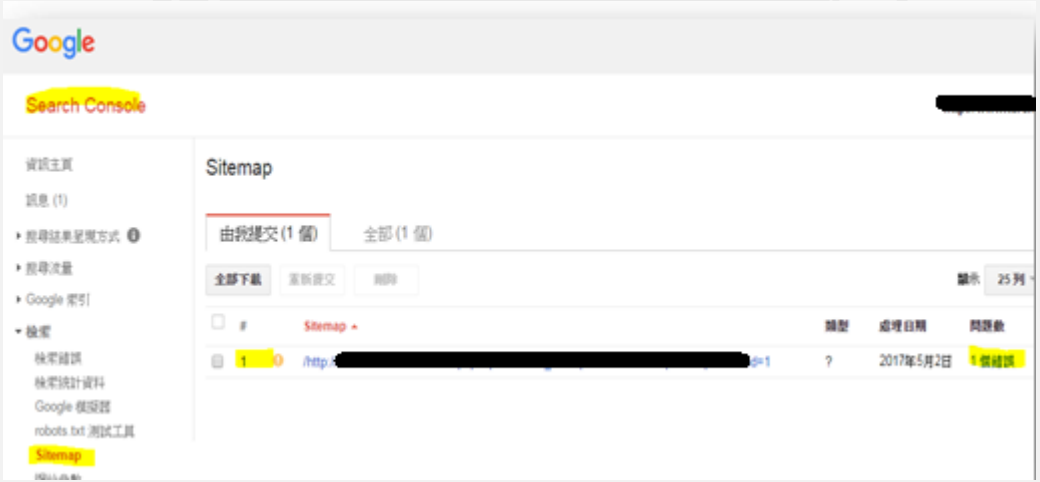
(搜尋引擎最佳化)

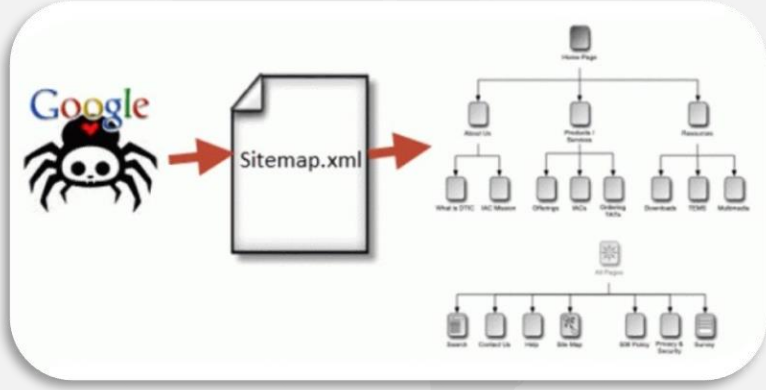
- 是一種搜尋引擎的演算法規則
- 目的：提升網站的排名



更新sitemap

Sitemap：幫助搜尋引擎爬取網站上的資料內容



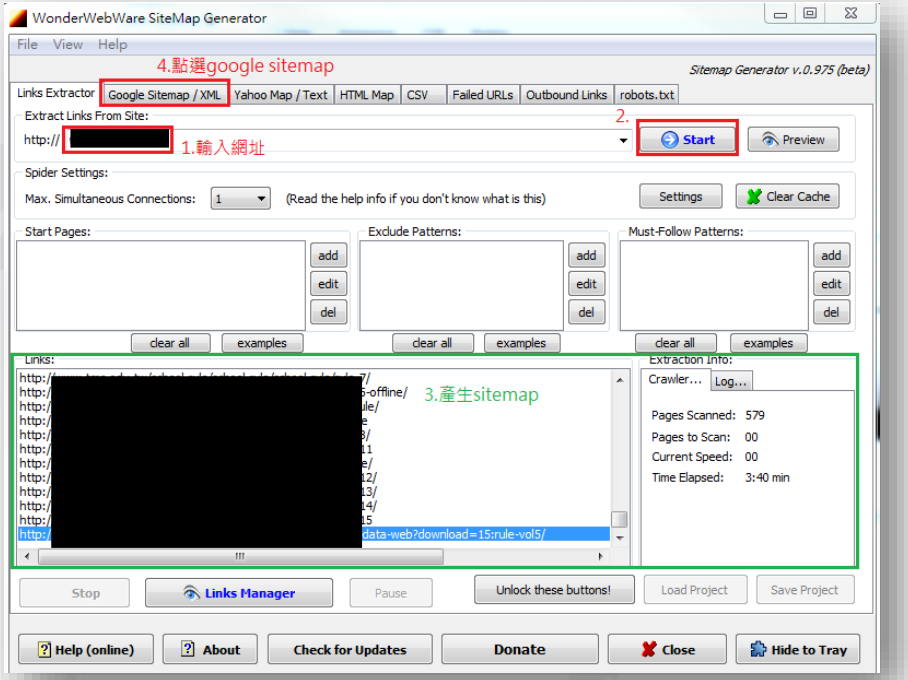


Sitemap產生器

Wonder WebWare Sitemap

推薦理由：

- 免費
- 沒有限制網頁數量
- 速度快
- 支援google 格式(XML)
- 支援yahoo格式(TXT)
- 爬到的資訊完整



10 Best Free Sitemap Generator you should know
https://www.lauyou.com/10-best-free-sitemap-generator/

Google論壇詢問

谷歌网站管理员帮助论坛 公開

動作

請幫我刪除頁庫存檔 http:[redacted]cd=1&hl=zh-TW&ct=clnk&gl=tw

新增回覆

作者 [redacted]

輸入台中區網，標題卻顯示日文字，點日文字，出現原本的網頁內容，但是頁庫存檔 http://[redacted]c
edu.tw/+&cd=1&hl=zh-TW&ct=clnk&gl=tw ，也是出現日文相關內容，不知道能不能麻煩您幫我把這個快取刪掉?

2 則留言 瀏覽次數：13 次 1 則專家回覆

社群內容可能並未經過驗證或不符合現況。

回覆

17/5/3

fan77說：

您好，刪除搜索結果中的信息请参考以下文档进行操作：
https://support.google.com/websearch/troubleshooter/3111061?hl=zh-Hans

+1

从Google搜索结果中移除信息

您可以要求 Google 从 Google 搜索结果中移除敏感的个人信息，例如，您的银行帐号或手写签名的图片。

Google 会移除哪些信息

请参阅我们的移除政策，了解 Google 会移除哪些信息。

如果您想从 Google 搜索结果中移除照片、个人资料链接或网页，则通常需要网站所有者（即网站站长）移除相应信息。

为何需要与网站站长联系？

即使 Google 从搜索结果中删除了网站或图片，相应的网页也仍然存在，而且用户可通过该网站的网址、社交媒体分享功能或其他搜索引擎找到该网页。因此，最佳做法就是与可彻底移除该网页的网站站长联系。

如果照片或信息显示在 Google 搜索结果中，这只是表示互联网上能找到该照片或信息，并不意味着 Google 会为这些信息提供任何担保。

您想执行哪些操作？

- ○ 移除您在 Google 搜索中看到的信息
- ○ 阻止信息显示在 Google 搜索中

搜尋索引狀況

Site: 指令

檢查 Google搜尋引擎建立網站索引狀況，也就是檢查網站是否有健康的被收錄於搜尋引擎之中。

Google Hacking：

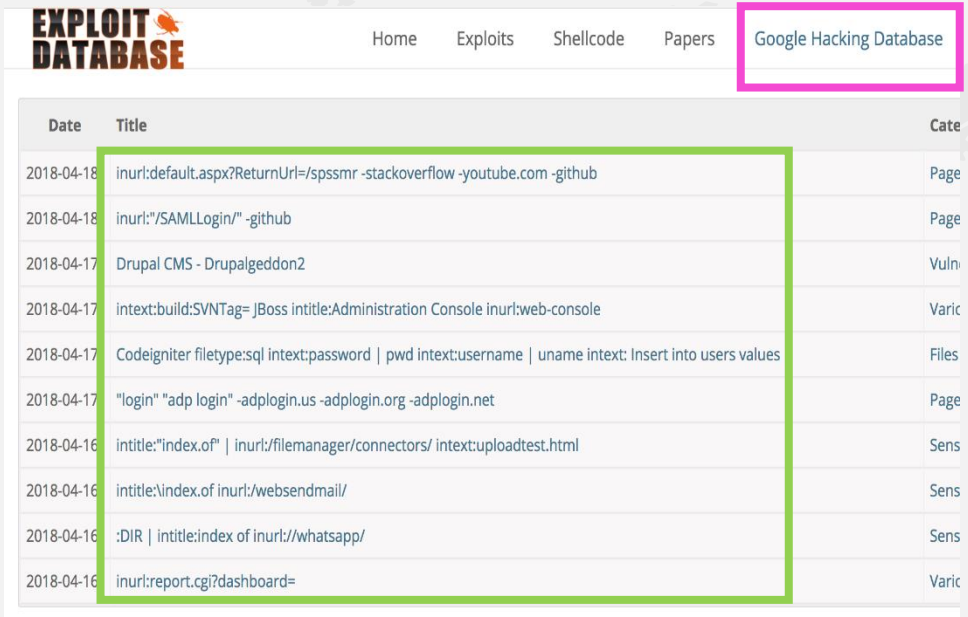
利用google搜尋引擎尋找安全漏洞的駭客技術，也是一種駭客攻擊前的偵查。

operator	說明
site	指定一個特定的網域做搜尋
inurl	找出於url有該字串的網頁
intitle	找出於網頁標題有該字串的網頁
intext	找出於網頁內文有該字串的網頁
filetype	明確找出指定的檔案類型

"Index Of"
網站的目錄曝光在公眾之下

Google Hacking https://goo.gl/XTM6zz
白帽駭客新兵訓練營(電子書) https://goo.gl/sPXp7g
Google Hacking for Penetration Testers https://goo.gl/ebuhrF

GHDB



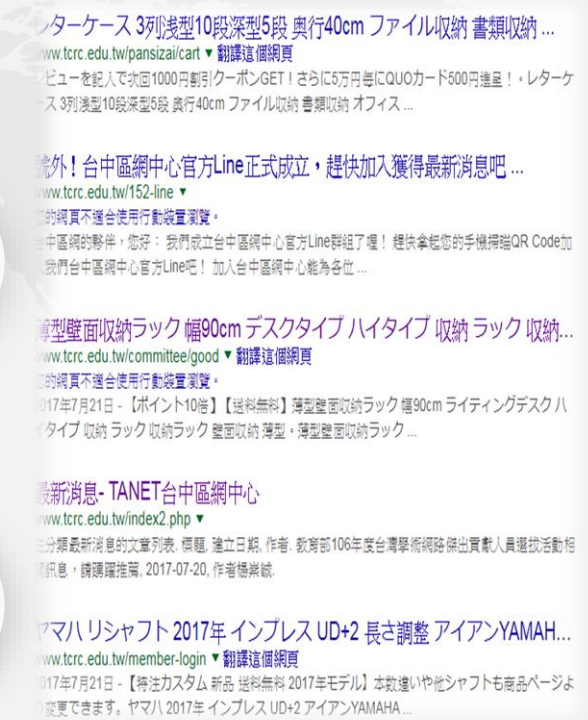
Exploit DB
https://www.exploit-db.com/

- 駭客提交漏洞的平台，又稱漏洞資料庫，除了提供漏洞外，也一併提供程式碼與工具。
- GHDB
  - 存放許多利用GOOGLE進階搜尋指令搭配相關關鍵字的方法，搜尋網頁的漏洞或機密資料。

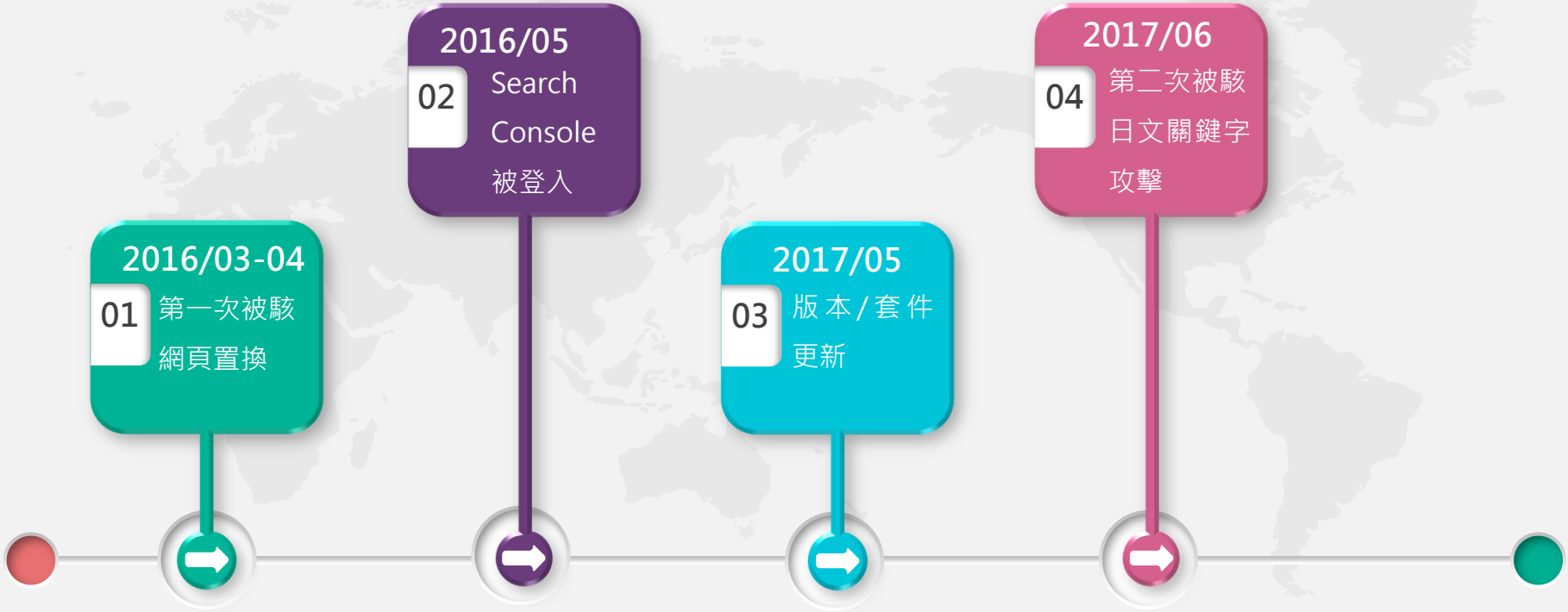
漏洞或機密資料：企業內伺服器、檔案、密碼記錄檔、公開的目錄、網頁介面的設備管理畫面、遠端桌面的用戶協定以及管理介面、或是路由器、交換器的管理者介面存在的弱點

日文關鍵字攻擊

1. 在目標網站上以隨機產生的目錄名稱建立含有日文的新網頁。
2. 網頁會超連結到特定的販售仿冒品牌商品的網站藉以牟利。
3. 利用SEO的方式，提高關鍵字搜尋的引擎排名並顯示搜尋結果。
4. 駭客的帳戶會加入 Search Console 成為網站擁有者。



被駭時間軸


2016/03-04
01
第一次被駭
網頁置換
2016/05
02
Search
Console
被登入
2017/05
03
版本/套件
更新
2017/06
04
第二次被駭
日文關鍵字
攻擊

處理步驟

- 更新sitemap
- 完整備份網站/網站下線
- 免費網站掃毒軟體
- 論壇詢問
- 檔案權限管理
- 搜尋惡意程式碼
- 移除網址
- 更新密碼

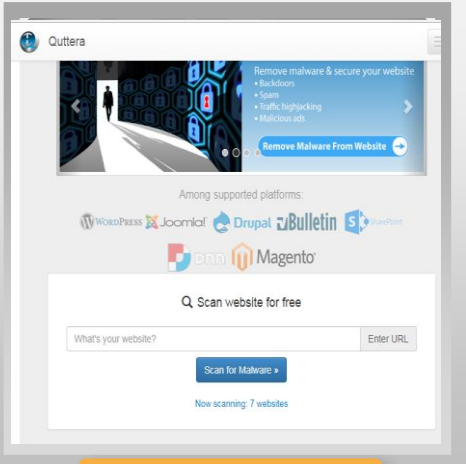
線上免費掃毒軟體

virustotal

Google子公司
一次使用數十種防毒
軟體來掃描
https://www.virustotal.com/zh-tw/

Sucuri

美國網站安全公司
與另外10權威
網站安全資料庫比對
https://sitecheck.sucuri.net



Quttera

Quttera 提供了黑名單功能，
主要市場WordPress
https://www.quttera.com/home

Top 11 Free Online Tools for Testing Your Website’ s Security https://goo.gl/qjnfBp

尋找遭到入侵的檔案

- 網站被攻擊之后，駭客通常會留後門(webshell)，並使用**混淆技術**來躲避檢測。
- 較常用的混淆技術(php涵式)
  - base64() :使用base64對數據進行編碼
  - eval() :使一段字符串如同PHP代碼一樣執行
  - gzinflate() :對數據進行解壓縮
  - str_rot13() :對字元串執行 ROT13 轉換
- 舉例:
- eval(gzinflate(base64_decode('5b19@#@.....^&*Z9P8C')));

執行　解壓縮　進行解碼　使用base64 編碼的數據

php後門木馬常用命令分析與防範 http://www.wenwenti.info/article/50563

關鍵字搜尋惡意程式

指令：

列出目前目錄底下所有的 PHP 檔案

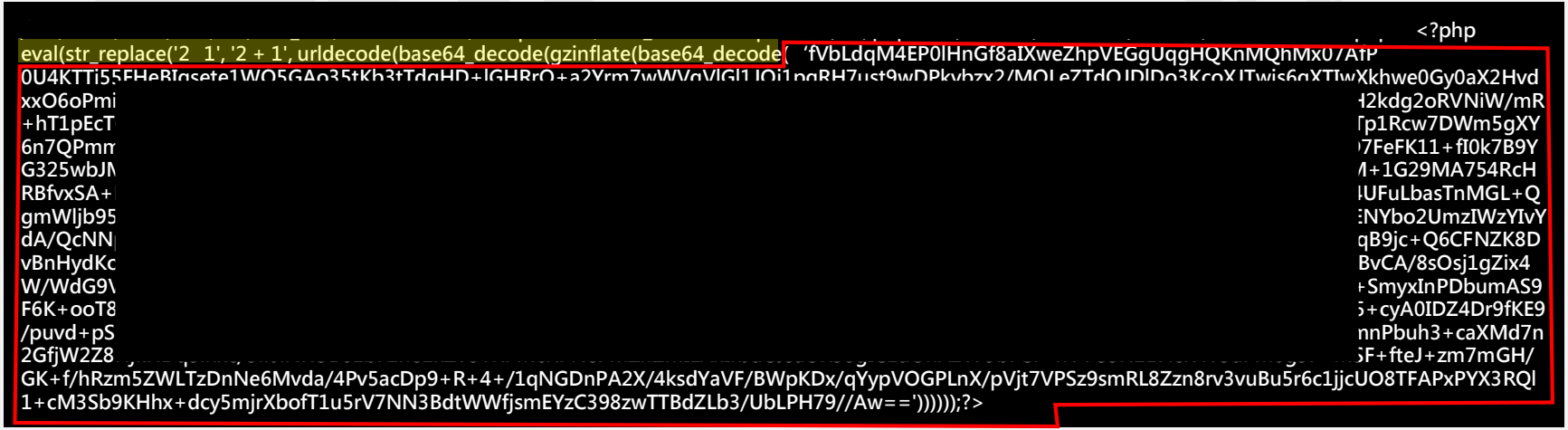
關鍵字：
base64、eval...

> find 搜尋的路徑 -type f -name “*.php” |xargs grep "eval"

查詢檔案

指定檔案類型搜尋
- d：目錄。
- f：一般的檔案。
- l：連結檔

進一步的搜尋檔案中的內容



關鍵字搜尋惡意程式

WEBDIR+

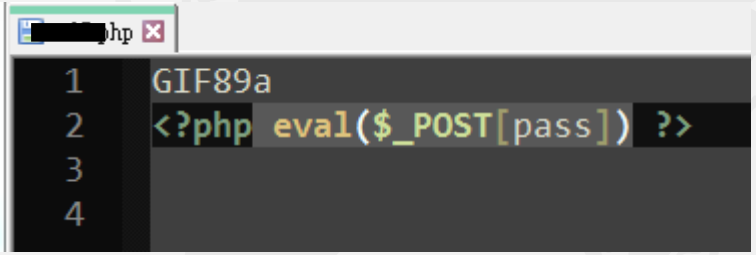
百度安全團隊開發的一套線上webshell掃描服務。

https://scanner.baidu.com/#

關鍵字搜尋惡意程式

一句話木馬：

- 僅需要短短的一串執行指令，就可以讓駭客入侵網站。
- 沒有完整的網站控制功能之腳本，透過遠端工具連接，獲得完整的控制功能。

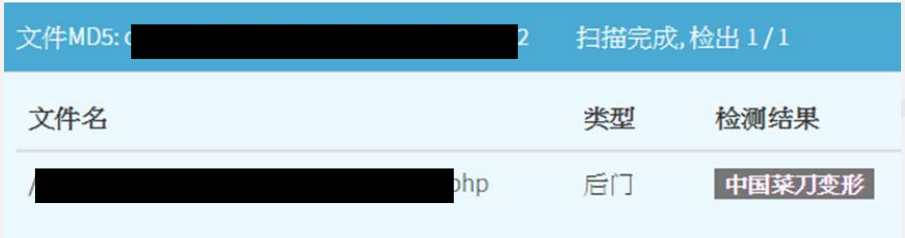


$_POST[ ] 函式：server取得clinet傳送的資料

常用的一句話木馬

- eval($_POST[pass]); 可以抓到使用者提交的密碼
- eval($_POST[cmd]); 可以執行使用者提交的任何cmd命令

https://goo.gl/wbUVbs



中國菜刀

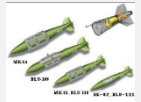
一款專業的網站管理工具，大小只有300多KB，為駭客常用的webshell工具，功能非常強大。

http://www.jb51.net/hack/164013.html

China Chopper

- 澳洲國防分包商遭中國網路犯罪者慣用的遠端存取木馬「中國菜刀」攻擊，並安裝了許多webshell以供遠端存取，藏匿時間長達5個月。
- 被駭的資訊：
  - F-35匿蹤戰鬥機
  - P-8反潛巡邏機
  - C-130運輸機
  - 聯合直接攻擊導引炸彈（JDAM）



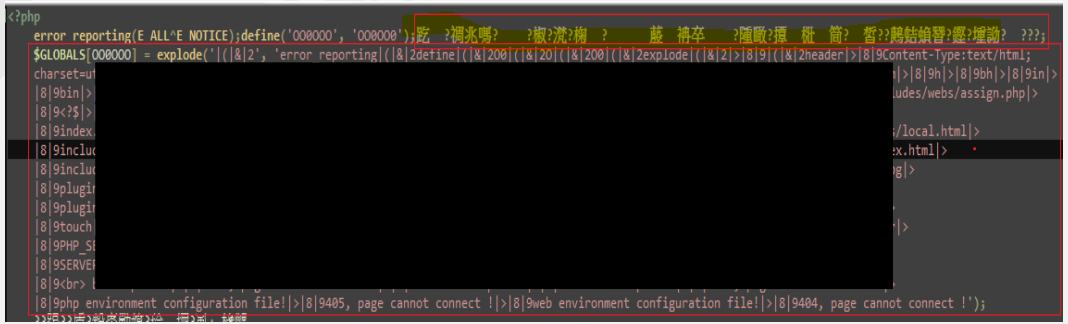
https://goo.gl/Jfwypy
https://goo.gl/3Feobp

關鍵字搜尋惡意程式

其他隱藏方式：

- 利用$GLOBALS變數來預防被掃描軟體偵測到
- 使用explode函式來干擾代碼被檢測

$globals[] = explode(‘分格符號’, ‘需要分解的字串');



Google重審

Search Console

資訊主頁

訊息 (2)

搜尋結果呈現方式

搜尋流量

Google 索引

檢索

安全性問題

Web Tools

← 刪除

☆ 「[redacted]」的重審要求遭到拒絕

收件者：「[redacted]」網站管理員

Google 收到您的重審要求後，已再次審查您的網站。依據這次的審查結果，Google 依然認為您的網站違反了Google《網站管理員指南》的規定。如要撤銷所有人工介入處理行動，請再次檢查您的網站並修正所有必要項目，然後再次提出重審要求。

審查者附註：

我们目前无法查看您的网站因为我们无法打开您的网页。请在确定您的网站可以被正常访问之后，再申请重新审核给我们查看。

如何修正這個問題：

1 檢查您網站上是否有任何違規事項

使用「人為介入處理檢視器」瞭解 Google 在您的網站中施行了哪些人工介入處理行動。

人為介入處理檢視器

2 修正所列問題

利用「人為介入處理檢視器」提供的詳細資訊，修正尚未處理的問題。如果您的網站遭到入侵，請參考「安全性問題」瞭解更多詳細資訊。

3 提交重審要求

建議提供相關的詳細資料或說明文件，協助我們瞭解您在網站上修正了哪些內容。

重審要求

需要其他協助嗎？

- 進一步瞭解網站中出現人工介入處理項目的原因。
- 如要瞭解如何清除遭入侵的內容，請參閱遭入侵網站指南。
- 如有其他問題，歡迎前往我們的論壇提問，並請記得註明郵件類型[WNC-646702]。

網站遭入侵時的疑難排解工具

駭客一旦入侵網站，通常會設法隱藏植入的內容，避免讓人輕易查覺。如果您難以找出網站上遭入侵的內容，或是想要再次查看是否已將遭入侵的內容完全從網站上清除，請遵循這個疑難排解工具中的步驟執行。文中將完整說明如何在 Google 中使用 site: 搜尋運算子，以及如何在網站管理員工具 中使用 Google 模擬器 找出垃圾內容。

是否曾使用 site: 搜尋運算子檢查網站遭入侵的內容？

- ● 是
- ○ 否

對網站使用 site: 搜尋運算子進行搜尋時，是否看見任何可疑結果？

- ○ 是
- ● 否

在網站的根或首頁上使用 Google 模擬器 。

駭客入侵網站時，除了在網頁上植入內容外，通常還會在網站的根或首頁也植入內容。植入的內容通常讓您無法輕易查覺，但卻可讓 Google 看見。因此，有必要在網站的根或首頁使用 Google 模擬器 工具，查看是否存有遭入侵的內容。務必徹底查看 Google 模擬器 的輸出內容，檢查是否已有可疑的文字或連結加到您的網站中。

報告者：張雅嵐