

Google搜索技巧与黑客入侵

白帽黑客训练营 昨天

Google提供了很多高级的搜集技巧，可以为我们日常生活提供更准确更有效的搜索结果。例如指定搜索文件类型为pdf的资源，可以加上filetype:pdf；或想搜索指定站点内的网页，可以加上site:domainname（如搜索: Nmap源码 site:blog.csdn.net）。Google的高级搜索技巧同样为黑客的信息搜集提供了巨大的便利，熟练的黑客可以google快速定位到存在漏洞的网站或暴露互联网上的文件。

谷歌入侵技巧

intitle:index-of

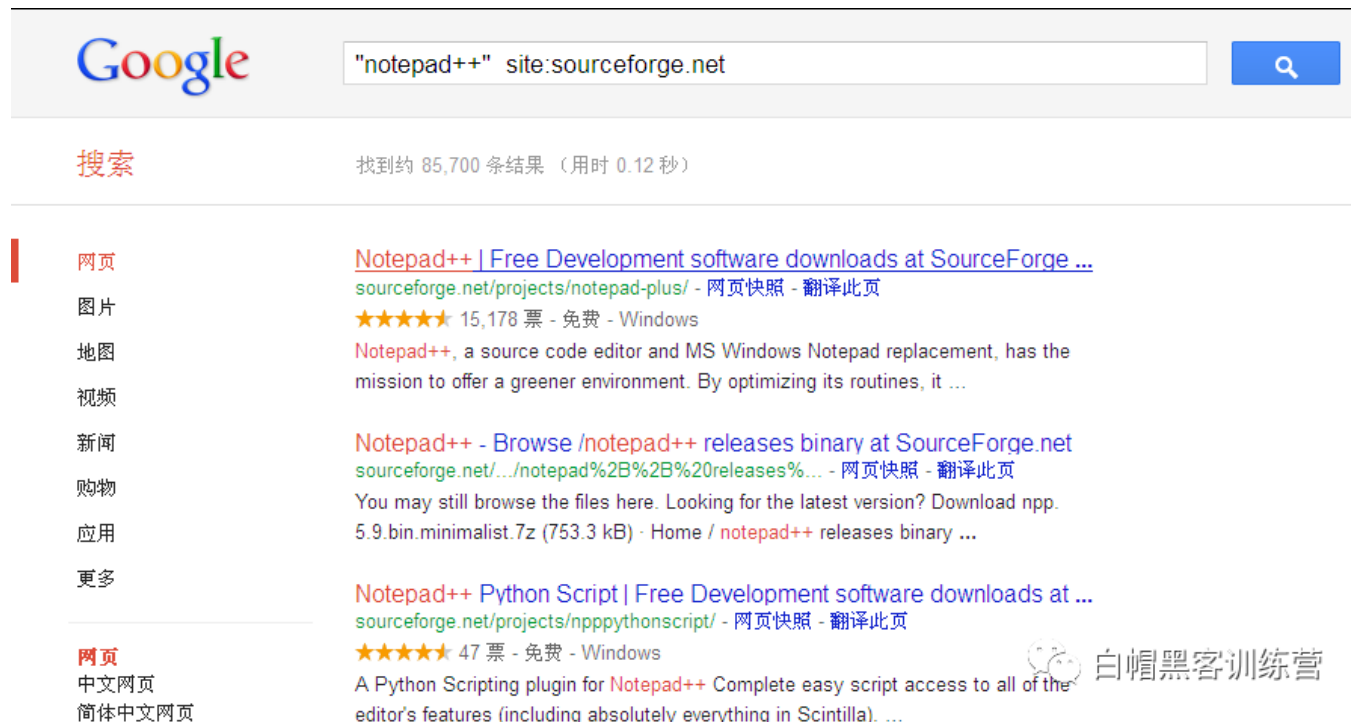
搜索某类资源的索引目录，如想搜索网站的图像、父目录等信息。可以在google搜索：intitle:index-of image和intitle:index-of “parent directory”。也可以搜索与Admin密切相关的网页：intitle:index-of “admin”。也可以尝试：intitle:index-of mp3 / intitle:index-of password等查询，具体查询内容就需要靠自己想象力了。



site: 操作符

site操作符非常有用，可以让google搜索来自指定的网站的网页。比如，想在sourceforge.net网站上搜索关于编辑器notepad++的网页，可以输入："notepad++" site:sourceforge.net。这样google就能返回来自sourceforge.net的网页。又比如，想查找csdn网站上关于端口扫描器Nmap的网页，那么可以输入："nmap" site:csdn.net。

site操作符，可用於搜索指定網站的上特殊的信息，如包含的主要資源，是否暴露出敏感文件等。



The screenshot shows a Google search interface. The search bar contains the query "notepad++" site:sourceforge.net. Below the search bar, the results are displayed. The first result is titled "Notepad++ | Free Development software downloads at SourceForge ..." and includes a link to sourceforge.net/projects/notepad-plus/. The second result is titled "Notepad++ - Browse /notepad++ releases binary at SourceForge.net" and includes a link to sourceforge.net/.../notepad%2B%2B%20releases%.../. The third result is titled "Notepad++ Python Script | Free Development software downloads at ..." and includes a link to sourceforge.net/projects/npppythonscript/. On the left side of the search results, there is a sidebar with links for "网页", "图片", "地图", "视频", "新闻", "购物", "应用", and "更多".

intile:error與intile:warning

標題中包含“error”或“warning”的網頁。用於定位網絡存在的錯誤與警告頁面，因為很多默認的提示頁可能會暴露web服務器端很多信息。

login|logon

搜索登錄頁面，很多時候令人感興趣的是登陸界面，因為如果破解登陸密碼即可獲得大量的權限與信息。最好將此搜索與site操作符結合使用，搜索某一個網站或域名內的登錄頁

面。另外可結合關鍵字admin搜索：admin login|logon



文件類型filetype:

當用戶單獨搜索某一類文件時，可使用該關鍵字。比如想搜索關於黑客技巧Hacking的PPT，可以搜索：hacking filetype:ppt。

如果想要搜索關於黑客大曝光系列圖書的PDF，可以嘗試輸入："hacking exposed" filetype:pdf，這樣就能直接搜索很多該系列圖書的PDF文檔。

同理，也可以結合site操作符，搜索指定網站內的資源，如word文件、XML文件、excel文件、PPT文檔、txt等等。



The screenshot shows a Google search interface. At the top, the Google logo is on the left, and a search bar contains the text "hacking filetype:ppt". To the right of the search bar is a blue button with a magnifying glass icon. Below the search bar, the text "搜索" (Search) is on the left, and "找到约 13,500 条结果 (用时 0.20 秒)" (Found about 13,500 results in 0.20 seconds) is on the right. On the left side, there is a vertical menu with options: 网页 (Web), 图片 (Images), 地图 (Maps), 视频 (Videos), 新闻 (News), 购物 (Shopping), 图书 (Books), 博客 (Blogs), and 更多 (More). The "网页" option is selected. The main content area displays search results. The first result is titled "Hacking Citrix - Presentation - Insomnia Security" with a URL "www.insomniasec.com/publications/Hacking_Citrix.ppt" and a "翻译此页" (Translate this page) link. Below the title, it says "文件格式: Microsoft Powerpoint - 快速查看" (File format: Microsoft Powerpoint - Quick view). The snippet describes Citrix Presentation Server 4.5 and mentions "XenApp/Server". The second result is titled "Viewing Hacking as a Process" with a URL "www.usna.edu/Users/cs/balazs/.../HackingProcess.ppt" and a "翻译此页" link. It also mentions "文件格式: Microsoft Powerpoint - 快速查看". The snippet discusses understanding hacking as a process and identifies the five phases of the hacking process. The third result is titled "Hacking Hardware" with a URL "home.ubalt.edu/abento/753/.../hackhardware.PPT" and a "翻译此页" link. In the bottom right corner of the search results area, there is a logo for "白帽黑客训练营" (White Hat Hacker Training Camp).

inurl操作符

該操作符用於在URL路徑中搜索指定的關鍵字。例如，想搜索網站上關於備份資料的信息，可以輸入：inurl:temp | inurl:tmp | inurl:backup | inurl:bak

~操作符

查找與關鍵字類似的信息，如搜索 ~mobile phone，會搜索和移動電話類似的信息“cell,” “cellular,” “wireless,” “cellphone”等等。

..時間範圍

兩點操作符用於指定一個網頁的時間範圍，比如用戶想搜索的是2011年到2012年內，出現的關於web hacking的PDF資料。

可以輸入：web hacking filetype:pdf 2011..2012



The screenshot shows a Google search interface. The search bar contains the query "web hacking filetype:pdf 2011..2012". Below the search bar, it indicates "找到约 76,500 条结果 (用时 0.55 秒)". On the left side, there is a sidebar with navigation links: 网页 (selected), 图片, 地图, 视频, 新闻, 购物, 图书, 更多. Below these links, there is a section for "网页" (Websites) with a sub-link "中文网页" (Chinese websites). The main search results are listed on the right. The first result is a PDF document titled "Web Hacking Incidents Revealed - SANS Software Security - SAN..." with a link to "software-security.sans.org/.../web-trends-stats-and-how-to-d...". It includes a "快速查看" (Quick view) link and a brief description: "Project Leader, Web Hacking Incident Database. • Project Leader, Distributed Open Proxy Honeypots. • Project Contributor, Web Application Firewall Evaluation ...". The second result is a PDF document titled "Annual ISEA Workshop 2012" with a link to "www.iitg.ernet.in/cse/news-events/isea_2012_program.pdf". It also includes a "快速查看" link and a description: "2012. Date. Speaker. Content. 17th Feb. IITG security research team ... 18th Feb-2011 Web Hacking Techniques in 2011" contest conducted every year by ...". The third result is a PDF document titled "Rep Management web page - Hacking article - 17 April 2012" with a link to "features.withersworldwide.com/.../rep_management_web_p...". It includes a "快速查看" link and a description: "Rep Management web page - Hacking article - 17 April 2012".

雙引號 ""：精確匹配

搜索完整的字符串，不對句子進行拆分。如果知道明確的搜索目標，可用雙引號將其括起來。

減號-：排除關鍵字

如果想排除已知的關鍵字，可以使用減號加關鍵字。例如，想搜索Hacking Exposed系列書籍，但排除Network Security Secrets這本書，那麼可搜索Hacking Exposed -"Network Security Secrets"

更多高級選項，請參考<http://www.googleguide.com>

學習更多黑客技巧可以關注公眾號：白帽黑客訓練營，大家也可以掃下面二維碼關注



喜歡此內容的人還喜歡

記一次理財殺豬盤滲透測試案例

瀟湘信安



滲透測試——漏洞掃描工具整理

LemonSec



24+ 常見滲透測試漏洞靶場列表

瀟湘信安

