Demystifying Google Hacks

by
Debasis Mohanty (Orissa, India)
www.hackingspirits.com

Introduction

Google is world's most popular and powerful search engine which has the ability to accept pre-defined commands as input and produce unbelievable results. This enables malicious users like hackers, crackers, and script kiddies etc to use Google search engine extensively to gather confidential or sensitive information which is not visible through common searches.

In this paper I shall cover the below given points that an administrators or security professionals must take into account to prevent such information disclosures:

- Google's Advance Search Query Syntaxes
- Querying for vulnerable sites or servers using Google's advance syntaxes
- Securing servers or sites from Google's invasion

Google's Advance Search Query Syntaxes

Below discussed are various Google's special commands and I shall be explaining each command in brief and will show how it can be used for critical information digging.

[intitle:]

The "**intitle:**" syntax helps Google restrict the search results to pages containing that word in the title. For example, **"intitle:** *login password***"** (without quotes) will return links to those pages that has the word "*login*" in their title, and the word "*password*" anywhere in the page.

Similarly, if one has to query for more than one word in the page title then in that case "**allintitle:"** can be used instead of "**intitle**" to get the list of pages containing all those words in its title. For example using "**intitle:** *login* **intitle:** *password*" is same as querying "**allintitle:** *login password*".

[inurl:]

The "**inurl:**" syntax restricts the search results to those URLs containing the search keyword. For example: "**inurl:** *passwd"* (without quotes) will return only links to those pages that have "*passwd*" in the URL.

Similarly, if one has to query for more than one word in an URL then in that case "**allinurl:**" can be used instead of "**inurl**" to get the list of URLs containing all those search keywords in it. For example: "**allinurl:** *etc/passwd*" will look for the URLs containing "*etc*" and "*passwd*". The slash ("/") between the words will be ignored by Google.

[site:]

The "**site:**" syntax restricts Google to query for certain keywords in a particular site or domain. For example: "*exploits* **site:***hackingspirits.com*" (without quotes) will look for the keyword "*exploits*" in those pages present in all the links of the domain "*hackingspirits.com"*. There should not be any space between **"site:"** and the **"domain name".**

[filetype:]

This "**filetype:**" syntax restricts Google search for files on internet with particular extensions (i.e. doc, pdf or ppt etc). For example: "**filetype:***doc* **site:***gov confidential*" (without quotes) will look for files with ".doc" extension in all government domains with "*.gov" extension* and containing the word "confidential" either in the pages or in the ".doc" file. i.e. the result will contain the links to all confidential word document files on the government sites.

[link:]

"link:" syntax will list down webpages that have links to the specified webpage. For Example: "**link:***www.securityfocus.com*" will list webpages that have links pointing to the SecurityFocus homepage. Note there can be no space between the "link:" and the web page url.

[**related:**]

The “related:” will list web pages that are "similar" to a specified web page. For Example: “related:www.securityfocus.com” will list web pages that are similar to the Securityfocus homepage. Note there can be no space between the "related:" and the web page url.

[**cache:**]

The query “**cache:**” will show the version of the web page that Google has in its cache. For Example: “**cache:***www.hackingspirits.com*” will show Google's cache of the Google homepage. Note there can be no space between the "cache:" and the web page url.

If you include other words in the query, Google will highlight those words within the cached document. For Example: “**cache:***www.hackingspirits.com guest*” will show the cached content with the word "*guest*" highlighted.

[**intext:**]

The “**intext:**” syntax searches for words in a particular website. It ignores links or URLs and page titles. For example: “**intext:***exploits”* (without quotes) will return only links to those web pages that has the search keyword "*exploits*" in its webpage.

[**phonebook:**]

“**phonebook**” searches for U.S. street address and phone number information. For Example: “**phonebook:***Lisa+CA*” will list down all names of person having “*Lisa*” in their names and located in “*California (CA)*”. This can be used as a great tool for hackers incase someone want to do dig personal information for social engineering.

Querying for vulnerable sites or servers using Google's advance syntaxes

Well, the Google's query syntaxes discussed above can really help people to precise their search and get what they are exactly looking for.

Now Google being so intelligent search engine, malicious users don't mind exploiting its ability to dig confidential and secret information from internet which has got restricted access. Now I shall discuss those techniques in details how malicious user dig information from internet using Google as a tool.

Using "Index of " syntax to find sites enabled with Index browsing

A webserver with Index browsing enabled means anyone can browse the webserver directories like ordinary local directories. Here I shall discuss how one can use "index of" syntax to get a list links to webserver which has got directory browsing enabled. This becomes an easy source for information gathering for a hacker. Imagine if the get hold of password files or others sensitive files which are not normally visible to the internet. Below given are few examples using which one can get access to many sensitive information much easily.

```
Index of /admin
Index of /passwd
Index of /password
Index of /mail

"Index of /" +passwd
"Index of /" +password.txt
"Index of /" +.htaccess

"Index of /secret"
"Index of /confidential"
"Index of /root"
"Index of /cgi-bin"
"Index of /credit-card"
"Index of /logs"
"Index of /config"
```

Looking for vulnerable sites or servers using “inurl:” or “allinurl:”

a. Using **“allinurl:**winnt/system32/” (without quotes) will list down all the links to the server which gives access to restricted directories like “system32” through web. If you are lucky enough then you might get access to the cmd.exe in the “system32” directory. Once you have the access to “cmd.exe” and are able to execute it then you can go ahead in further escalating your privileges over the server and compromise it.

b. Using **“allinurl:**wwwboard/passwd.txt”(without quotes) in the Google search will list down all the links to the server which are vulnerable to “WWWBoard Password vulnerability”. To know more about this vulnerability you can have a look at the following link:
http://www.securiteam.com/exploits/2BUQ4S0SAW.html

c. Using **“inurl:**.bash_history” (without quotes) will list down all the links to the server which gives access to “.bash_history” file through web. This is a command history file. This file includes the list of command executed by the administrator, and sometimes includes sensitive information such as password typed in by the administrator. If this file is compromised and if contains the encrypted unix (or *nix) password then it can be easily cracked using “John The Ripper”.

d. Using **“inurl:**config.txt” (without quotes) will list down all the links to the servers which gives access to “config.txt” file through web. This file contains sensitive information, including the hash value of the administrative password and database authentication credentials. For Example: Ingenium Learning Management System is a Web-based application for Windows based systems developed by Click2learn, Inc. Ingenium Learning Management System versions 5.1 and 6.1 stores sensitive information insecurely in the config.txt file. For more information refer the following links:
http://www.securiteam.com/securitynews/6M00H2K5PG.html

Other similar search using “inurl:” or “allinurl:” combined with other syntaxs

```
inurl:admin filetype:txt
inurl:admin filetype:db
inurl:admin filetype:cfg
inurl:mysql filetype:cfg
inurl:passwd filetype:txt
inurl:iisadmin
inurl:auth_user_file.txt
inurl:orders.txt
inurl:"wwwroot/*."
inurl:adpassword.txt
inurl:webeditor.php
inurl:file_upload.php

inurl:gov filetype:xls "restricted"
index of ftp +.mdb allinurl:/cgi-bin/ +mailto
```

Looking for vulnerable sites or servers using “intitle:” or “allintitle:”

a. Using [**allintitle:** "index of /root”] (without brackets) will list down the links to the web server which gives access to restricted directories like “root” through web. This directory sometimes contains sensitive information which can be easily retrieved through simple web requests.

b. Using [**allintitle:** "index of /admin”] (without brackets) will list down the links to the websites which has got index browsing enabled for restricted directories like “admin” through web. Most of the web application sometimes uses names like “admin” to store admin credentials in it. This directory sometimes contains sensitive information which can be easily retrieved through simple web requests.

Other similar search using “intitle:” or “allintitle:” combined with other syntaxs

```
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:"index of" htpasswd
intitle:"index of" members OR accounts
intitle:"index of" user_carts OR user_cart

allintitle: sensitive filetype:doc
allintitle: restricted filetype :mail
allintitle: restricted filetype:doc site:gov
```

Other interesting Search Queries

- **To search for sites vulnerable to Cross-Sites Scripting (XSS) attacks:**

```
allinurl:/scripts/cart32.exe
allinurl:/CuteNews/show_archives.php
allinurl:/phpinfo.php
```

- **To search for sites vulnerable to SQL Injection attacks:**

```
allinurl:/privmsg.php
allinurl:/privmsg.php
```

Securing servers or sites from Google's invasion

Below given are the security measures which system administrators and security professionals must take into account to secure critical information available online, falling into wrong hands:

- Install latest security patches available till date for the applications and as well as the operating system running on the servers.

- Don't put critical and sensitive information on servers without any proper authentication system which can be directly accessible to anyone on internet.

- Disable directory browsing on the webserver. Directory browsing should be enabled for those web-folders for which you want to give access to anyone on internet.

- If you find any links to your restricted server or sites in Google search result then it should be removed. Visit the following link for more details: http://www.google.com/remove.html

- Disable anonymous access in the webserver through internet to restricted systems directory.

- Install filtering tools like URLScan for servers running IIS as webserver.

Conclusion

Sometimes increase in sophistication in the systems creates new problems. Google being so sophisticated can be used by any Tom, Dick & Harry on internet to dig sensitive information which is normally neither visible nor reachable to anyone.

The only options left for the security professionals and systems administrators are to secure and harden their systems from such un-authorized invasion.

About Me

To know more about me visit www.hackingspirits.com

Debasis Mohanty
www.hackingspirits.com
Email: debasis_mty@yahoo.com

I can also be found at:
http://groups.yahoo.com/group/Ring-of-Fire

Comments and suggestion are invited in debasis_mty@yahoo.com.