GOOGLE - SECURITY TESTING TOOL

Georgi Staykov

Abstract: Using Google as a security testing tool, basic and advanced search techniques using advanced google search operators. Examples of obtaining control over security cameras, VoIP systems, web servers and collecting valuable information as: Credit card details, cvv codes – only using Google.

Keywords: Google – security testing tool, IJ ITA presentation.

Introduction

The Google search engine found at www.google.com offers many different features including language and document translation, web, image, newsgroups, catalog and news searches and more. These features offer obvious benefits to even the most uninitiated web surfer, but these same features allow for far more nefarious possibilities to the most malicious Internet users including hackers, computer criminals, identity thieves and even terrorists. This paper outlines the more nefarious applications of the Google search engine, techniques that have collectively been termed “Google hacking.”

Basic search techniques

The Google search engine is fantastically easy to use. Despite the simplicity, it is very important to have firm grasp of these basic techniques in order to fully comprehend the more advanced uses. The most basic Google search can involve a single word entered into the search page found at www.google.com. Once a user submit a search by clicking the “Submit Search” button or by pressing enter in the search term input box, a result page may be displayed. The search result page allows the user to explore the search results in a various ways.

The top line (found under the alternate search tabs) lists the search query, the number of hits displayed and found, and how long the search took. “Category” link takes you to the Google directory category for the search you entered. The Google directory is a highly organized directory of the web pages that Google monitors.

Main page link takes you directly to the current result web page. Description – the short description of a site. Cached link takes you to Google’s copy of this web page. This is very handy if a web page changes or goes down. “Similar pages” link takes you to similar pages on the Google category. “Sponsored links” column lists pay targeted advertising links based on your search query.

Under certain circumstances, a blank error page may be presented instead of the search result page. This page is the catchall error page, which generally means Google encountered a problem with the submitted search term. Many times this means that a search query option was not entered properly. In addition to the “blank” error page, another error may be presented. This page is much more descriptive, informing the user that a search term was missing. This message indicates that the user needs to add to the search query.

Basic Google searches, as I have already presented, consist of one or more words entered without any quotations or the use if special keywords.

Example:

peanut butter

butter peanut

‘+’ searches

When supplying a list of search terms, Google automatically tries to find every word in the list of terms, making the Boolean operator “and” redundant. Some search engines may use the plus sign as a way of signifying a Boolean “and”. Google uses the plus sign in a different fashion. When a Google receives a basic search request that contains a very common word like “the”, “how” or “where”, the word will often times be removed from the query. In order to force Google to include a common word, precede the search term with a plus (+) sign. Do not use a space between the plus sign and the search term. For example, the following searches produce slightly different results:

Where quick brown fox

+Where quick brown fox

The '+' operator can also be applied to Google advanced operators, discussed in the Advanced Google operators chapter.

'-' searches

Excluding a term from a search query is as simple as placing a minus sign (-) before the term. Do not use a space between the minus sign and the search term. For example, the following searches produce slightly different results:

quick brown fox

quick –brown fox

The '-' operator can also be applied to Google advanced operators, discussed in the Advanced operators chapter.

Phrase searches

In order to search for a phrase, supply the phrase surrounded by double-quotes. Example:

"the quick brown fox"

Mixed searches

Mixed searches can involve both phrase and individual terms. Example:

Macintosh "Microsoft office"

This search will only return results that include the phrase "Microsoft office" and the term Macintosh.

Google Advanced operators

Google allows the use of certain operators to help refine searches. The use of advanced operators is very simple as long as the attention is given to the syntax. The basic format is"

Operator :search_term

Notice that there is no space between the operator, the colon and the search term. If a space is used after a colon, Google will display an error message. If a space is used before the colon, Google will use your intended operator as a search term. Some advanced operators can be submitted to Google as a valid search query. The 'cache:www.google.com' can be submitted to Google as a valid search query. The 'site' operator, by contrast, must be used along with a search term, such as 'site:www.google.com help'.

Advanced Operator Summary

Operator	Description	Additional search
argument required?		
site:	find search term only on site specified by search_term.	YES
filetype:	search documents of type search_term	YES
link:	find sites containing search_term as a link	NO
cache:	display the cached version of page specified by search_term	NO
intitle:	find sites containing search_term in the title of a page	NO
inurl:	find sites containing search_term in the URL of the page	NO

site: find web pages on a specific web site

The advanced operator instructs Google to restrict a search to a specific web site or domain. When using this operator, an addition search is required. Example:

site:harvard.edu tuition

This query will return results from Harvard.edu that include the term tuition anywhere on the page.

filetype: search only within files of a specific type.

This operator instructs Google to search only within the next of a particular type of file. This operator requires an additional search argument. Example:

filetype:txt endometriosis

This query searches for the word 'endometriosis' within standard text documents. There should be no period (.) before the filetype and no space around the colon following the word "fletype". It is important to note that Google only claims to be able to search within certain types of file. Based on my experience, Google can easily find a word within a file of type ".txt", ".html" or ".php" since the output of these files in a typical web browser window is textual. By contrast, while a WordPerfect document may look like text when opened with the WordPerfect application, that type file is not recognizable to the standard web browser without special plugins and by extension, Google can not interpret the document properly, making a search within that document impossible. Thankfully, Google can search within specific types of special files, making a search like "filetype:doc endometriosis" a valid one. The current list of files that Google can search is listed in the filetype FAQ located at http://www.google.com/help/faq_filetypes.html. As of this writing, Google can search within the following file types:

Adobe Portable Document Format (pdf)

Adobe PostScript (ps)

Lotus 1-2-3 (wk1, wk2, wk3, wk4, wk5, wki, wks, wku)

Lotus WordPro (lwp)

MacWrite (mw)

Microsoft Excel (xls)

Microsoft PowerPoint (ppt)

Microsoft Word (doc)

Microsoft Works (wks, wps, wdb)

Microsoft Write (wri)

Rich Text Format (rtf)

Text (ans, txt)

SQL (sql)

link: search within links

The hyperlink is one of the cornerstones of the Internet. A hyperlink is a selectable connection from one web page to another. Most often, these links appear as underlined text but they can appear as images, video or any other type of multimedia content. This is advanced operator instructs Google to search within hyperlinks for a search term. This operator requires no other search arguments. Example:

link:www.news-panel.com

This query would display web pages that link to news-panel.com's main page. This special operator is somewhat limited in that the link must appear as entered in the search query. The above query would not find pages that link to www.news-panel.com/sitemap for example.

cache: display Google's cached version of a page

This operator displays the version of a web page as it appeared when Google crawled the site. This operator requires no other search arguments. Example:

cache:news-panel.com

cache:http://news-panel.com

These queries would display the cached version of news-panel web page. Note that both of these queries return the same result. I have discovered however, that sometimes queries formed like these may return different results, with one result being the dreaded "cache page not found" error. This operator also accepts whole URL lines as arguments.

Intitle: search within the title of a document

This operator instructs Google to search for a term within a title of a document. Most web browsers display the title of a document on the top title bar of the browser window. This operator requires no other search arguments. Example:

intitle:gandalf

This query would only display pages that contained the word 'gandalf' in the title. A derivative of this operator, 'allintitle' works in a similar fashion. Example:

allintitle:gandalf silmarillion

This query finds both the words 'gandalf' and 'silmarillion' in the title of a page. The 'allintitle' operator instructs Google to find ever subsequent word in the query only in the title of the page, This is equivalent to a string of individual 'intitle' searches.

Inurl: searche within the URl of a page

This operator instructs google to search only within the URL, or the web address of a document. This operator requires no other search arguments. Example:

Inurl:hair

This query would display pages with the word 'hair' inside the web address. One returned result, 'http://www.news-panel.com/en/view.category/category.374/Hair-Loss.html' contains the word 'hair' as the name of a document. The word can appear anywhere within the web address, including the name of the site or the name of a folder. A derivate of this operator, allinurl' works the similar fashion. Example:

Allinurl:hair en

This query finds both the words 'hair' and the 'en' in the URL of a page. The 'allinurl' operator instructs Google to find every subsequent word in the query only in the URL of the page. This is equivalent to a string of individual 'inurl' searches. For a complete list of the advanced operators and their usage see http://www.google.com.help/operators.html.

Example of hacking Google queries

Query	Description
"internal server error" "server at"	*Apache server could reveal admin e-mail address*
intitle: "Execution of this script not permitted"	*Cgiwrap script can reveal lots of information, including e-mail address and phone number*
intitle: index.of dead.letter	*dead.letter Unix file containing the content of unfinished e-mail.*
Filetype: reg reg +intext:"internet account manager"	*Windows registry files can reveal information such as usernames, pop3 passwords, e-mail addresses, and more.*
"Access denied for user" "using password"	*Collecting SQL usernames*
"# Dumping data for table"	*Entire SQL Database dumps (Adding 'username' or 'password' to this query makes things really interesting.)*
"ORA-00933: SQL command not properly ended"	*SQL injection hints*
filetype: inc intext:mysql_connect	*Going after SQL passwords*
filetype: sql "visa | master card"	*SQL data base dump containing credit cards information.*
Filetype: sql "cvv"	*SQL data base dump containing credit cards information.*
Intitle: VNC viewer for java"	*VNC (Virtual Network Computing) allows you to control a workstation remotely.*
Allinurl: index.htm?cus?audio	*One query, many brands of live cams!*

“active webcam page” inurl:8080	*Web cameras.*
intitle: "toshiba network camera -User Login"	*Toshiba Network Cameras*
intitle: ”speedstream Router management interface”	*speedstream Router management interface access*
inurl: vswebapp.exe	*Microsoft Virtual Server 2005 access*
inurl: ”level/15/exec/-/show’	*Open Cisco Devices*
intitle: ”ivista.main.page”	*Security Cameras*
intitle: ”everfocus edsr applet”	*My favorite security cameras – most of them using default login details – admin, admin*
filetype: ctt “msn”	*MSN Contact Lists*

Conclusion

The intent of this paper is to educate web administrators and the security community in the hopes of eventually securing this form of information leakage.

Bibliography

www.Google.com

http://johnny.ihackstuff.com, johnny@ihackstuff.com

Author’s Information

Georgi Zhechev Staykov - NBU student; Sofia, Bulgaria; e-mail: gstaykoff@gmail.com

USE OF THE MAPLE SYSTEM IN MATH TUITION AT UNIVERSITIES

Tsvetanka Kovacheva

Abstract: *The following article explores the application of educational technologies at a University level and their contribution in enhancing the educational effectiveness. It discusses the capabilities of computer algebra systems, such as Maple. It is integrated in the math tuition of the Technical University (TU) in Varna and is used by its students during laboratory exercises.*

Key words: *education, educational technology, computer algebra systems.*

Introduction.

For the purpose of improving the effectiveness of the study process it is necessary to apply a variety of educational technologies (ET). They have two *basic components*:

- *technologies/media used in the study process,* through which different educational resources are introduced such as printed materials, projector equipment, TV & video and all other related resources, computer-based resources (computer algebra systems (CAS), spreadsheets, databases, Power Point, www, email), multimedia, etc.
- *technologies of the study process*, which include planning, organization, carrying out and evaluation of the entire process. They respectively comply with the aims and purposes of education, the design of co-ordinated tuition, integrated curricula, study approaches, principles and methods of evaluation. Appropriate media needs to be selected for the purposes of the study process. This choice is influenced by main factors such as aims and time, media access, human resources, costs. In math education for the engineering speciality computer-based resources play a great role due to the capabilities those resources come with: