

# [REVS] Hacking with the Google Search Engine

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-01/msg00097.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxxxx)>
  - *Date:* 30 Jan 2006 11:08:01 +0200
- 

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

-----

Hacking with the Google Search Engine

---

## SUMMARY

Hackers and security experts use various custom and open source tools to complete their tasks. In fact, one of the tools they use you probably use every time you browse the web, the Google Search Engine.

Paul remembers the first time he used the Google Search Engine years ago. Paul was amazed at how quickly it fulfilled my search request. Google's huge index of systems / information and it's ability to perform complex searches have evolved over the years. When we performed security assessments and penetration test, we regularly use Google to locate information that organizations typically want to keep private and confidential.

## DETAILS

The reason for me writing this article is to give you several examples of basic and complex Google search terms and queries. As a disclaimer, it is not my intention that you use this information to invade the privacy of someone else or access data and files on systems that do not belong to you. It is strictly educational information and a way to make people more aware of what kind of information they may be exposing to the rest of the

world.

Using Google To Locate Password Files:

One of the most common remote web authoring tools is Microsoft's Front Page. Front page extensions and WebDav, the services on the web server that allow you to remotely connect and author web pages, can be configured with a certain degree of security. However, in certain configurations, the userID and password are stored in local files on the server. Using a Google query, you can easily locate thousands of these files and dump the contents.

The query form is quite simple: "inurl:(filename).pwd", where (filename) is the name of the .pwd file. This query can be expanded to be very specific and target a specific site by using a command to search for a specific site or domain. The results of a specific search like this would list hundreds if not thousands of these files that would contain something like "# -FrontPage- dmiller:11KEaH1TZqxew". Basically dumping the userID and password.

This type of basic query can be used to find all kinds of interesting information such as using the "intitle:"index of" (name of directory you want to locate)" which not only reveals many web directory structures of "index of/", it also reveals how many web servers on the Internet do not have even the most basic forms of permissions and directory security. You will find that once you access a particular directory, that you can then move up the directory tree and you never know what you may find.

The rest of the article can be found at:

<http://castlecops.com/article-6466-nested-0-0.html>  
<http://castlecops.com/article-6466-nested-0-0.html>

ADDITIONAL INFORMATION

The information has been provided by <mailto:zx@xxxxxxxxxxxxxxxx> Paul Laudanski.

The original article can be found at:

<http://castlecops.com/article-6466-nested-0-0.html>  
<http://castlecops.com/article-6466-nested-0-0.html>

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

[list-unsubscribe@xxxxxxxxxxxxxxxx](mailto:list-unsubscribe@xxxxxxxxxxxxxxxx)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@xxxxxxxxxxxxxxxx](mailto:list-subscribe@xxxxxxxxxxxxxxxx)

=====  
=====  
  
DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.

---

- Prev by Date: [\*\[NT\] Cerberus FTP Server DoS \(CVH, Exploit\)\*](#)
- Next by Date: [\*\[UNIX\] Eterm Local Buffer Overflow\*](#)
- Previous by thread: [\*\[NT\] Cerberus FTP Server DoS \(CVH, Exploit\)\*](#)
- Next by thread: [\*\[UNIX\] Eterm Local Buffer Overflow\*](#)
- Index(es):
  - ◆ [\*Date\*](#)
  - ◆ [\*Thread\*](#)