Google Hacking Mini-Guide

Date: May 7, 2004 By Johnny Long.

Using search engines such as Google, "search engine hackers" can easily find exploitable targets and sensitive data. This article outlines some of the techniques used by hackers and discusses how to prevent your site from becoming a victim of this form of information leakage.

The Google search engine found at http://www.google.com offers many 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 offer far more nefarious possibilities to the most malicious Internet users, including hackers, computer criminals, identity thieves, and even terrorists. This article outlines the more harmful applications of the Google search engine, techniques that have collectively been termed "Google hacking." The intent of this article is to educate web administrators and the security community in the hopes of eventually stopping this form of information leakage. This document is an excerpt of the full *Google Hacker's Guide* published by Johnny Long, and located at http://johnny.ihackstuff.com.

Basic Search Techniques

Since the Google web interface is so easy to use, I won't describe the basic functionality of the http://www.google.com web page. Instead, I'll focus on the various operators available:

- Use the plus sign (+) to force a search for an overly common word. Use the minus sign (-) to exclude a term from a search. No space follows these signs.

- To search for a phrase, supply the phrase surrounded by double quotes (" ").

- A period (.) serves as a single-character wildcard.

- An asterisk (*) represents any word—not the completion of a word, as is traditionally used.