



# Information Disclosure Web Sweep

## Description

An Information Disclosure Sweep of the Web is designed to reveal any confidential information that may lead to a compromise of the security and integrity of a companies website or its' intellectual property. This includes vulnerabilities that do NOT typically yield immediately valuable information or control over a system but instead gives an attacker inside knowledge that may help an attacker find and exploit other vulnerabilities. Initial web sweeps are typically run against major search engines including but not limited to Google, Yahoo, AltaVista, Creative Commons, A9 Search, AskJeeves, eBay, MSN, Tucows, RU FileSearch, No Nags Freeware, IRCSpy, hack a day, Walla! Programs, SNORT Search, GeekTools WhoIs, FreeBSD, FileWatcher FTP, Crack Spider, bpdownload, and PacketStorm. Secondary web sweeps are run against blog search engines such as feedster.com.

The sweep methods usually include multiple passes through a generic web search, by adding filters to refine the search results. Generic searches are defined as those that have no modifiers, such as, company.com or company.net. Qualifiers (filters) are programmatically added to refine the search using a stepwise function to eliminate redundant responses and data tied to a generic response, such as www, etc.

## Features and Benefits

A Web sweep report provides summary and detailed information typically displayed in the following categories, others may be added or substituted based on sweep results;

1. Availability of published web site analysis data
2. Links that by-pass protected web pages without login/authentication mechanisms
3. Jobs advertised looking for specific skills with technology and tool preferences
4. Details on development tools, libraries used to build proprietary applications
5. Descriptions of usage problems with development tools and libraries, that might show release levels of current technology choices
6. Posted system or network configuration data, e.g. ports used, IP addresses, logical network maps
7. Descriptions of tools being used to manage or monitor systems
8. eMail addresses that can be used to further find details about employees and contractors or commit spoofing or masquerading attacks against the Web site
9. Descriptions of techniques in use for security and integrity detection mechanisms

## Other Services Available

nGran™ offers a complete suite of network and security services. Related security services include ***Web Site Reviews, Remote Security Monitoring, System Security Audits, Controlled Penetration Testing, Vulnerability Assessments, Site Recovery Planning***, and other consulting services, as required.

## nGran, LLC

PO Box 1555  
Westford, MA 01886  
Tel: 978-392-7867  
email: sales@ngran.com

nGran believes that the information in this document is accurate as of its publication date; such information is subject to change without notice. nGran is not responsible for any inadvertent errors. nGran™ is a trademark of nGran, LLC. All other trademarks and registered trademarks are property of their respective owners.