

September 27, 2006

How a Google Search Can Become a Security Threat

By DAVID STROM

WHEN [Ralph Nader](#) wrote “Unsafe at Any Speed” in 1965, he exposed how certain design decisions had made some automobiles inherently unsafe. Much the same can be said for Web sites these days.

Many sites contain inherent design flaws that leave them ripe for exploitation. Unlike lack of seat belts in cars, these flaws are not immediately obvious and the fixes are not simple.

One widespread vulnerability can be exploited through a practice that has come to be known as [Google](#) hacking. The term refers to the use of an Internet search site — [Yahoo](#), Ask, Google or any other — to uncover useful and compromising information that has been inadvertently left on a Web site.

“Some Web site owners may simply not understand that their sites aren’t as secure as they think,” said Jeff Williams, chief executive of a Columbia, Md., consulting company, Aspect Security. Mr. Williams is also the chairman of the Open Web Application Security Project, a Web site that describes many of the vulnerabilities and provides tips on how to prevent or fix them.

Examples of the material that can be uncovered include the locations of Web security cameras, administrator passwords for applications like payroll or other personnel matters, private phone numbers for company executives and even the contents of Internet commerce transactions.

In most cases, intruders can enter sites and extract data without leaving a trace because the information is already indexed and stored on the servers of various Internet search sites.

These hacks require no special tools and little skill.

All that is needed is a Web-connected PC and a few keywords to look for, like “filetype:sql password” or “index.of.pass word.”

“There is a lot of privileged information that wasn’t supposed to be played out in the public that is available with these sorts of attacks,” said Jeff Pettorino, a senior consultant in the Global Security Consulting department of [VeriSign](#) and a former police officer in Colorado.

Much of the data indexed by the search sites can be used for nefarious means, and site owners may not realize that sensitive or confidential information is so readily available as part of a search index.

“If you are dealing with sensitive data or data that you care about, you have to think about these exploits,” said Michael Howard, a senior security program manager at [Microsoft](#) in Redmond, Wash.

As more businesses put up Web sites, the chances increase that more of this information is available.

“A business owner has risks even if they aren’t doing e-commerce and if they just have a Web site,” said Shena Crowe, an agent in the [F.B.I.](#)’s San Francisco field office who has helped prosecute cybercriminals who used Google hacks and other techniques. “Once you are plugged into the Web, your backyard can become

open, and it is easy to have your information taken from you.”

While it isn't the only way Web sites are exposed, it is one of the easiest and most common methods to gain unauthorized information.

“At any given time, you can find thousands of sites that are subject to Google hacks,” says Howard Schmidt, a former White House cybersecurity adviser and now a private security consultant in Issaquah, Wash.

Johnny Long, a security researcher with the [Computer Sciences Corporation](#) in El Segundo, Calif., said he had found vulnerabilities “in every Web site and application I have audited.”

Mr. Long, who maintains a Web site cataloging Web security vulnerabilities, johnny.ihackstuff.com, added, “Some Google hacking style vulnerabilities are more revealing than others, but it is a pervasive threat.”

Google acknowledges that its index can be misused. “Search engines reflect what is on the Web,” said Barry Schnitt, a Google spokesman. “We still work to try to prevent and stop exploits and encourage Webmasters to employ best practices and effective security for their Web sites.” On Google's site you can find tips on how to remove sensitive data from its index, for example.

Law enforcement is just stepping up to the challenges presented by search-based Web site intrusions.

“This is very underreported,” says Kevin Patten, network services manager with the Florida Department of Law Enforcement in Tallahassee. “There are far more site breaches that take place than are actually reported. It is an embarrassing incident, and to report it could be monetarily devastating for a company.”

Google hacks are an issue for both large and small businesses, but for different reasons.

Smaller companies generally have simpler sites but may be less sophisticated when it comes to auditing their software. And smaller businesses often rely on independent Web contractors that may not have the ability to build secure applications.

Larger companies usually have better security practices, but they use hundreds or even thousands of Web applications, which must be maintained by more people — some of whom may try to get at sensitive information they shouldn't see.

“Google hacking can find application vulnerabilities in many applications at once, so it works better as a shotgun than a rifle,” Mr. Williams of Aspect Security said. “These vulnerabilities can be found and exploited with a minimum of effort by relatively unskilled attackers.”

One way for businesses to protect themselves is to try the Google hacking methods themselves, using tips at johnny.ihackstuff.com and on the Owasp.org sites.

There are also free scanning tools that are available from numerous sites, including SPIdynamics.com, Qualys.com and ScanAlert.com. The tools check for open ports that allow outside communication with particular software programs or points of entry that could be used to compromise a Web site.

But using scanners is just the first step.

Business owners need to specifically address the security audits and testing services when they hire outside programmers to build their sites.

“What you have to get across,” said Mr. Schmidt the security consultant, “is that ‘I am not buying a service, I am buying a secure service.’” The Owasp site, he said, offers boilerplate contract language that can be used in dealing with programmers.

And the vigilance must be continuous. “It is always an arms race between security professionals and cybercriminals,” said Scott Larson, a former F.B.I. computer intrusion manager who now works at Stroz Friedberg, a technical services firm in New York.

Even after “Unsafe at Any Speed” shook up the automobile industry, it took a while for Detroit to make safety a priority in designing cars. “And it’s going to take years for the software industry to start building applications that adequately address security,” said Mr. Williams of Aspect Security.

For wary business owners, it’s time to buckle up.

[Copyright 2006 The New York Times Company](#)

[Privacy Policy](#) | [Search](#) | [Corrections](#) | [RSS](#) | [First Look](#) | [Help](#) | [Contact Us](#) | [Work for Us](#) | [Site Map](#)