

Security: Referrer

By Richard Lowe

Security: Referrer

Richard Lowe
articles@internet-tips.net

Internet Tips And Secrets <http://www.internet-tips.net>

Copyright (C) Richard Lowe Jr. and Claudia Arevalo-Lowe, 1999-2001.

Permission is granted to reprint the following article as long as no changes are made and the byline, copyright information, and the resource box is included. Please let me know if you use this article by sending an email to <mailto:articles@internet-tips.net>

Article Title: Security: Referrer

Author: Richard Lowe, Jr.

Contact Author: <mailto:articles@internet-tips.net>

Publishing Guidelines: May be freely published w/bylines

Web Address: <http://www.internet-tips.net>

Autoresponder Address: <mailto:article-172@internet-tips.net>

If you are a webmaster, you will find that one of the most valuable things you can use is the referrer. On the other hand, if you are a surfer, you may want to disable this feature as it can be a security risk and a violation of your privacy.

What is this referrer thingie? Well, all web servers have the capability to create log files and virtually all web masters (at least those who know what they are doing) use these logs to determine how their web site is doing. The log files contain one line for each hit to the web site. The format and contents of the line vary from server to server (and webmasters can specify they want more or less information), but in general it has an incredible amount of information about that one hit.

Some of the information gathered for each hit to a web site includes (among other things):

- The requested file (for example, index.html)
- A status code indicating success or error (404 errors, for example)
- The browser type being used by the surfer (this is the agent name, and it can also be the name of a search engine spider or a spam harvester).
- The screen resolution of the surfer's monitor
- The date and time (locally to the server) of the hit
- The TCP/IP address of the surfer (yes, every web page that you have ever looked at has your TCP/IP recorded in a web server log file somewhere).
- The URL where the surfer came from

It's this last statistic that causes some concern. Oh, there is a minor issue in that your TCP/IP

address is stored in the server logs when you access a page, but this is not very important. You see, these logs do not tend to last very long as they get very large extremely quickly. Many (if not most) web sites purge these as soon as statistics are gathered. Conceivably, of course, this could be of concern if an investigation were performed ... and these logs are looked at by webmasters for hacking attempts.

No, the important information is the referrer field. Why? Well, first there is the privacy question. If a webmaster knew your TCP/IP address (and he would have to know your address specifically, since this is the only thing relating you to the line in the log file - there is no name or email address stored there) he could get an idea of what you looked at before you came to his site. Thus, there is a remote chance that your privacy could be compromised ... a very remote chance since this is virtually never done by any webmaster.

The second, and very critical problem is a real security risk. You see, many websites allow you to log into their sites to personalize your experience. These sites allow you to enter personal data such as credit card information, social security numbers and other items into their database. Generally cookies are used to identify you as you move from page to page through the web site. Cookies are by far the best and preferred way to do this - it's called maintaining context. However, cookies are frowned upon by many surfers for various reasons (mostly blown out of proportion fears created by a press that feels it needs dangers and bad news to stay competitive).

Thus, some clever webmasters have come up with alternate ways to allow their web sites to know that "you are you" as you move around on their site. A very sloppy method consists of adding a username and password on to the end of each URL.

For example, suppose you log into a shopping site with a username and password like so:

URL: <http://www.anyshoppingsite.com>

Username: innocent

Password: naive

If you moved to a page called "toys.htm", the URL might become:

<http://www.anyshoppingsite.com?u=innocent?p=naive>

You see the problem? Not yet? Okay, there is no problem as you move around from page to page within the shopping site. The problem results when you surf to another page outside of the shopping site.

What happens? Well, if you surfed to another site from the page above, that URL complete with the username and password would be added to the server log files. Guess what, your username and password just got recorded in plain text somewhere completely unexpected.

So what's the problem really? Well, let's say you went to your shopping site, logged in and made some purchases. To make it simple for you, your credit card numbers are stored on the site and you can retrieve them at any time after you are logged in. Everything seems safe because you need a username and password to get in.

Now, when you are finished shopping you are supposed to log out. This would remove the username and password from the referrer. However, you don't do this and instead surf to another site. You leave your username and password in that webmasters log files. If that webmaster happens to check his log files he could get your username and password, log into your account and get your credit card numbers.

Are you alarmed yet?

Okay, how do you stop this from happening? It's relatively easy, actually. You get a product called AdSubtract and install it on your computer. By default this product will remove the referrer field as you surf around. You are now protected.

Oh yes, one side effect is you cannot just surf to that shopping site, since the login information is removed by AdSubtract. Fortunately, AdSubtract allows you to configure exceptions. All you need to do is enter the "filters" section, add your shopping site and specify to not remove the referrer.

And that, my friends, is how you protect yourself from one of the internet's biggest gaping security holes. I hope this has been of use to you.

NOTE: The following information must be included if you reprint this article:

Richard Lowe Jr. is the webmaster of Internet Tips And Secrets. This website includes over 1,000 free articles to improve your internet profits, enjoyment and knowledge.

Web Site Address: <http://www.internet-tips.net>

Weekly newsletter: <http://www.internet-tips.net/joinlist.htm>

Daily Tips: <mailto:internet-tips@GetResponse.com>

Claudia Arevalo-Lowe is the webmistress of Internet Tips And Secrets and Surviving Asthma. Visit her site at <http://survivingasthma.com>

List of articles available for reprint: <mailto:article-list@internet-tips.net>

[Get-Articles.com : 1000's of reprintable business and internet marketing-related articles.](#)

[Submit your article for reprint.](#)