Information Systems Security Association
Barbados Chapter

Password Management Protocol in Mozilla Firefox

By Belnando Weekes

Firefox the popular web browser has a very useful feature where it remembers your user names and passwords for sites visited. This is an excellent tool which pops up and requests if the user wants the browser to remember both the user name and password used for any site which requires login credentials. Needless to say this is quite a handy tool because it helps users to have access to their login credentials for the several sites visited.

It is not uncommon therefore to have several user names and passwords to remember. So this password manager in Firefox is truly a great idea.

How secure is the Firefox password manager? Consider that users are storing login credentials for the bank accounts, credit cards and more; is this really a great idea? Needless to say, the really wise thing to do is "NOT USE the Firefox password manager but who can resist?

Earlier versions the web browser stored log credentials in a text file called "signons.txt". Felker (2006) stated that "On Firefox, Uniform Resource Locators (URLs), usernames, and passwords are stored in a file called *signons.txt"*. This was obviously not secure at all.

Current versions of Firefox are subject to password hacking and mining by using Cross-Site Scripting (XSS) (**Bort, 2010**) which gives hackers the ability to manipulate characters and words in text in such a manner that web sites are fooled into passing critical information via cookies to the unintended recipient. (**Vamosi 2010**)

Unfortunately web sites do not and probably cannot prevent XSS attack purely by way of encrypted connections and hence users and web designers have to be wary of this possibility in Firefox and lockdown Cross-Site Scripting.

Users can help themselves by avoiding links from site to site and instead open each site in its own tab and not via the embedded link, even though it's inconvenient. Secondly scripting can be disabled from the Firefox browser and hence block all scripts from running from various sites. From a personal perspective, I use NoScript, a small application which allows me to block or allow embedded links, scripts, video and more.

In the final analysis even though Firefox's password manager may be well intentioned and serves great purpose, users must be aware that they can take greater control over what happens on their computers. It is not enough to know that the password manager can be somewhat insecure, it's more important to take action to be safe rather than sorry.

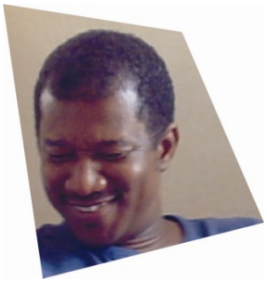
References

Felker, M. (2006) "Password Management Concerns with IE and Firefox" [INTERNET] Available from http://www.symantec.com/connect/articles/password-management-concerns-ie-and-firefox-part-one (Accessed 15th September 2010)

Bort, J (2010) "Firefox Let's Hackers Grad your Passwords" [INTERNET] Available from http://www.networkworld.com/community/blog/firefox-lets-hackers-grab-your-passwords (Accessed 15th September 2010)

Vamosi, R. (2010) "Cross-Site Scripting: An Old Problem Returns" [INTERNET] Available from https://www.networkworld.com/news/2010/061810-cross-site-scripting-an-old-problem.html (Accessed 15th September 2010)

About the Author



Belnando is the CEO of Quality Performance Systems for the past twenty years. QPS is an IT company supporting the deployment of reliable and functional technology across the Caribbean.

During the past twenty years he has amassed a wealth of experience in designing, integrating and implementing several types of networks.

In recent years he has concentrated his focus on security in networking and has conducted several workshop and seminars in the area of network/internet security, computer forensics and general networking technologies.

As a part time consultant with the Caribbean Development Bank's CTCS program he has helped several small businesses and organizations get up to speed with evolving technologies.

Contact can be made at belnando@hotmail.com or 1-246-262-3045