

Forum:[Hack Forums](#)

Thread: [EXPLOIT:Steal information via mozilla firefox form history](#)

Yoshistr - April 16, 2009, 7:12 pm

This is a tutorial on getting form element values from mozilla firefox's history.

Mozilla stores values entered into forms in unencrypted format in a file called 'formhistory.sqlite' under the profiles folder for example:

%AppData%\Mozilla\Firefox\Profiles\randomname.default

So you might wonder what good is that for a hacker?

The file stores values which include: passwords, credit card information, security question answers for sites, search history, etc. all in plain text format...meaning by simply accessing this file from your target computer you will have immediate access to vital information.

A keylogger is a great program but it can only log keys after being installed meaning if the information was typed in a form earlier but not again the keylogger won't acquire it.

Another great advantage of stealing this file is that your program only needs to be run once to get a lot of information for future hack attacks and therefore it is much less likely your hack attempt will ever be detected.

Here is how one such attack may proceed:

- Your target runs your executable file,
- code runs to shutdown firefox (needed to access profile files)
- formhistory.sqlite for each profile is uploaded to an ftp server owned by the hacker by the hacking exe
- exe file returns an error message that firefox was unexpectedly shutdown with a button labelled 'restart firefox'
- firefox is restarted without making the target suspicious (firefox has bugs and crashes periodically)
- exe file removes itself and all subfiles from target computer or hides in a hidden directory to be executed again at a predetermined timeframe
- hacker accesses formhistory.sqlite at leisure from ftp site and browses the file in plain text or with a script for target information

This method may also be run with a keylogger if desired

Some requirements

- exe must be run
- target must be using firefox (up to current version:3), firefox is becoming much more common among more users
- target must not delete history often (dormant exe can change firefox's settings)

This tutorial does not include the exe that will do necessary functions but you can always write your own or wait a few months until I have the time to write one.

Another great use is accessing your own form history to recover your own information if you have forgotten your password

Mr Beanz - April 16, 2009, 7:22 pm

LOL, there is already a program that is out there to do this. It also retrieves it from earlier versions of FF and IE. Also, with a CD key grabber for specific games. And yes it is free, and no I won't post the link.

DanThaBeast - April 17, 2009, 4:44 am

yea i already downloaded something like this you just click history and it bring it up...i think its easier

PaRaNo1D - April 17, 2009, 9:54 am

Thanks for the tut, broh.

KillerNay - April 17, 2009, 10:25 am

Thanks for the tut and i want to know what the program name for using read .sqlite format

now i use sqlitebrowser. Do you get a better software ?

[W4RL0CK] - April 17, 2009, 3:30 pm

yeah i use something like this with a USB hack when you "scan for viruses" ;)

Yoshistr - April 27, 2009, 11:32 pm

The idea of this exploit is not to actually get your own information but to write code to get other people's information by having them run an exe which exploits firefox's weakness here.

Sqlitebrowser or other Firefox add-ons will only show you your own information but can't be installed on a remote computer and send you their information. The idea here is to increase the functionality of a keylogger to get data or information from the user before the keylogger was ever installed, and also will supplement the logged keys in case they have software which disables keylogging.

Yoshistr - May 1, 2009, 4:16 pm

This exploit has currently been added to the latest keylogger I am writing:

<https://hackforums.net/showthread.php?tid=71771>

In addition to capturing the form history file it also gets the saved password files for firefox and sends them over as well :)

Yoshistr - May 1, 2009, 9:49 pm

This post was removed due to security reasons.