

[NEWS] Firefox: about:blank is Phisher's Best Friend

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-02/msg00062.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 20 Feb 2007 12:39:44 +0200
-

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>
-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.
<http://www.securiteam.com/maillinglist.html>

Firefox: about:blank is Phisher's Best Friend

SUMMARY

Firefox suffers from a design flaw that can be used to confuse casual users and evoke a false sense of authority when visiting a fraudulent website. The flaw can be also used to bypass a fix for an old UI spoofing bug that was thought to be addressed. This is a relatively minor issue, but Michal thought it's worth reporting.

DETAILS

It is possible for a script to open 'about:blank' URL in a new tab; this tab will be opened with a blank address bar (the behavior is different for new windows, where the bar will be grayed out or hidden).

The script can then interact with this document as if it were a page in the same domain, including the ability to inject of custom HTML. Some methods of adding this HTML, such as `win.document.write()`, will update `document.location` and the address bar to that of the interacting script, which seems like an intuitive choice – the user is informed about the origin of the displayed data.

[NEWS] Firefox: about:blank is Phisher's Best Friend

Since about:blank is a minimal but valid HTML document with a DOM structure, it is also possible to inject code through the use of `win.document.body.appendChild()` and friends, in which case, the URL bar remains blank, the 'reload' button is disabled, and 'page info' / 'page source' menu options will show no useful data.

Having text displayed in a window that has an empty URL bar can confuse the user as to the origin of the displayed data or security prompts, as if they were internal browser messages; an empty address bar is considerably less suspicious than a shady host name or a panic-inducing data: URL scheme.

Furthermore, there was an old UI spoofing bug – when a window was opened without URL bar and menus, the attacker could use strategically placed graphics and HTML controls (or XUL code), so that the fake URL bar read "google.com", while an IFRAME below could display "zombo.com" instead.

Similarly, he could spoof a native browser-originating modal warning or dialog to have the user do something dumb. This problem was addressed by forcibly prepending current site name to window title for all URL-bar-less windows, so that the Internet origin of such a pop-up is clear, and so that it will have a hard time mimicking a native window.

The problem is that 'about:blank' windows that have no `document.location` defined can be used to inhibit this behavior – window title can be freely controlled, except for the appended ' – Mozilla Firefox' string, and spoof browser UI elements without the user having a reason to be suspicious.

A quick if naive demonstration of the two attacks described here can be found at this URL: <http://lcamtuf.coredump.cx/ffblank/>

[Note that Michal simply used a screenshot of my UI, which is a non-standard one, and the image is not compensated for other screen resolutions etc; as such, you should be able to see that the URL bar is unusual and non-interactive; that's not a limitation of this attack, but rather, an unloved bastard child of my sheer laziness.]

ADDITIONAL INFORMATION

The information has been provided by <mailto:lcamtuf@xxxxxxxxxxxxx> Michal Zalewski.

The original article can be found at: <http://lcamtuf.coredump.cx>

=====

[NEWS] Firefox: about:blank is Phisher's Best Friend

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@xxxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxxx

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.