

[Full-disclosure] MSIE7 entrapment again (+ FF tidbit)

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2007-07/msg00290.html>

- *From:* Michal Zalewski <lcamtuf@xxxxxxxxxxxxx>
 - *Date:* Sat, 14 Jul 2007 00:20:54 +0200 (CEST)
-

Hello again,

Microsoft Internet Explorer seems to have a soft spot for browser entrapment vulnerabilities. Just to recap, in these attacks, the user is made believe he had left a webpage (and the URL bar or SSL state data reinforce him in this belief) – but in reality, is prevented from doing so, and his browser continues to display assorted content originating from the attacker.

This is a close, but somewhat more sinister relative of vanilla URL bar spoofing. I reported a few of each kind in the recent months.

Well, here's another one, this time based on `document.open()` calls. In essence, repeatedly calling this function after a new URL is entered by the user, before `onBeforeUnload` is invoked, inhibits page transition – but target URL bar state is retained. This is remarkably silly.

A live demo is available here:
<http://lcamtuf.coredump.cx/ietrap3/>

That is all.

...

PS. The promised tidbit – since I'm leaving for a while and won't have time to research this – in Firefox, `javascript: windows` can set 'domainless' cookies by specifying `'domain=.'` – for example:

```
open("javascript:document.cookie='foo=bar;domain=.',"_blank");
```

Fortunately/unfortunately, these cookies do not get sent to all sites – no session fixation – though can be retrieved by other null-domain `javascript: / data: pages`. Specifying other domains won't work. Multiple periods will be trimmed. Path can be set arbitrarily, with certain exceptions. Null-domain cookies load properly when stored in `cookies.txt`.

Q: can this be used in a manner more sinister than merely facilitating exchange of "markers" between various user-tracking sites?

[Full-disclosure] MSIE7 entrapment again (+ FF tidbit)

/mz

Full-Disclosure – We believe in it.

Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>

Hosted and sponsored by Secunia – <http://secunia.com/>