

# [Full-disclosure] Firefox wyciwyg:// cache zone bypass

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2007-07/msg00153.html>

---

- *From:* Michal Zalewski <[lcamtuf@xxxxxxxxxxxxx](mailto:lcamtuf@xxxxxxxxxxxxx)>
  - *Date:* Mon, 9 Jul 2007 15:37:26 +0200 (CEST)
- 

There is an interesting vulnerability in how Mozilla Firefox handles internal wyciwyg:// pseudo-URIs. These cache-related resource identifiers are meant to be inaccessible by the user – but there are at least three routes to bypass these restrictions, one of which – HTTP 302 redirect – also improperly employs same-domain policy checks.

This combo flaw enables attackers to intercept sensitive data, perform cache poisoning, or carry out URL spoofing (including SSL certs), against sites that scriptually render documents on client side, and hence produce wyciwyg:// resources to begin with. Although not all sites are susceptible to attacks, a good chunk of "Web 2.0", a selection of popular webmails, and several major banks, very much are.

A quick demo and a more detailed discussion can be found here:

<http://lcamtuf.coredump.cx/ffcache/>

PS. The two remaining routes to bypass wyciwyg:// restrictions (XMLHttpRequest() and view-source: URIs) appear to properly implement same-domain checks (although view-source seems to be nevertheless not functioning as intended). document.write() + XMLHttpRequest to wyciwyg:// URIs can be used by rogue websites to conveniently store and retrieve persistent "markers" on visitor's machine regardless of cookie settings; that's not a disaster, but still not very nice.

PS2. Bugzilla entry here – source patch available:  
[https://bugzilla.mozilla.org/show\\_bug.cgi?id=387333](https://bugzilla.mozilla.org/show_bug.cgi?id=387333)

Cheers!  
/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/>