

# [ZH2004-18SA] Content-Type spoofing in Mozilla Firefox and Opera could allow users to bypass security restrictions

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2004-12/0133.html>

---

**From:** Giovanni Delvecchio (*badpenguin79\_at\_hotmail.com*)

**Date:** 12/14/04

Date: 13 Dec 2004 23:45:24 -0000

To: bugtraq@securityfocus.com

('binary' encoding is not supported, stored as-is)

Author: Giovanni Delvecchio

e-mail: badpenguin@zone-h.org

Original advisory: <http://www.zone-h.org/en/advisories/read/id=6502/>

Browsers tested:

- Firefox 1.0
- Mozilla 1.7.x
- Opera 7.54 (\*)
- Konqueror 3.3.1
- Epiphany
- Internet Explorer 6 with SP1
- Internet Explorer 6 with SP1 + SP2

Browsers affected:

- Firefox 1.0
- Mozilla 1.7.x
- Opera 7.51,..7.54

( maybe also previous versions)

Problem Description:

=====

A problem exists in some browsers where it is possible by a Content-Type spoofing to "force" the target user to open a page and bypass the security zone and execute javascript in local context.

Indeed, when the user "victim" visits [http://malicious\\_server/paage.html](http://malicious_server/paage.html), if malicious\_server responds with a page containing an unknown Content-Type field ( for example text/html. ,note the dot) ,the browser will show a dialog window with some options (open, save, cancel). Choosing "Open" to view this page, it will

be downloaded and opened in local ; javascript code will be executed in local context.  
Obviously, if the user chooses to save and open it after the result is equal.

I tested this with some browsers but it seems that just Mozilla Firefox and Opera(\*) are exploitable in this mode.

(\*) For Opera, this method of exploitation requires that opera must be set as Default Application in "handler for saved files" in case the user chooses "Open" in the dialog window.

#### Impact

=====

It could allow remote users to :

- obtain the content of /home/ directory ( or c:\Documents and Settings\ for windows systems ) and therefore gather a set of usernames present on the target system.

- know if a particular program is installed on the target system for a successive attack.

- Read the content of confidential files

- Read the browser's cache

In opera it is located in ~/.opera/cache4, instead in Mozilla Firefox it's in  
/.mozilla/firefox/\$RANDOM-STRING.default/Cache.

Since it is possible to enumerate the directory structure , a malicious user could easily know the path to firefox's cache