# Exploiting IE8 UTF-7 XSS Vulnerability using Local Redirection

**Exploiting IE8 UTF-7 XSS Vulnerability using Local Redirection** - Author not stated, securethoughts.com.

- Published: date not stated
- Original: <http://securethoughts.com/2009/05/exploiting-ie8-utf-7-xss-vulnerability-using-local-redirection/>
- Current location: <https://securethoughts.com/2009/05/exploiting-ie8-utf-7-xss-vulnerability-using-local-redirection/>
- Preserved from: https://securethoughts.com/2009/05/exploiting-ie8-utf-7-xss-vulnerability-using-local-redirection/ (live) on 2026-08-09
- 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.

Exploiting IE8 UTF-7 XSS Vulnerability using Local Redirection | SecureThoughts.com

---

## Exploiting IE8 UTF-7 XSS Vulnerability using Local Redirection

**Conventions:** Attacker Domain – Securethoughts.com Target Domain – 50webs.com

If you don't remember, there was an important XSS vulnerability reported in all major browsers a while ago – IE7, Firefox and Opera. More Information is available in the Secunia advisories here. The vulnerability was that if you don't specify a charset in your application page, then it is susceptible to inherit the charset in the parent page via iframes. So, if you accidently land on an evil site, an attacker might be able to steal your application session since your usual XSS prevention stuff [<,>,",',etc] will not filter the utf-7 encoded chars and XSS will execute in your vulnerable domain. Proof of Concept that works in IE7 but not in IE8 - http://www.securethoughts.com/security/ie8utf7/ie7utf-7.html

This vulnerability was patched in Firefox 2.0.0.2, Opera 9.20 and recently in Internet Explorer 8. Ideally, we should not be vulnerable to this attack anymore. However, I have found a way to attack the fix that was done in Internet Explorer 8. I have tested it working with IE8 RC1 and final release version IE8.0.6001.18702. I call this a **"Local Redirection Attack"**.

The attack works as follows:

1. You are authenticated to vulnerable domain e.g. 50webs.com.

1. You land onto the evil site via link –

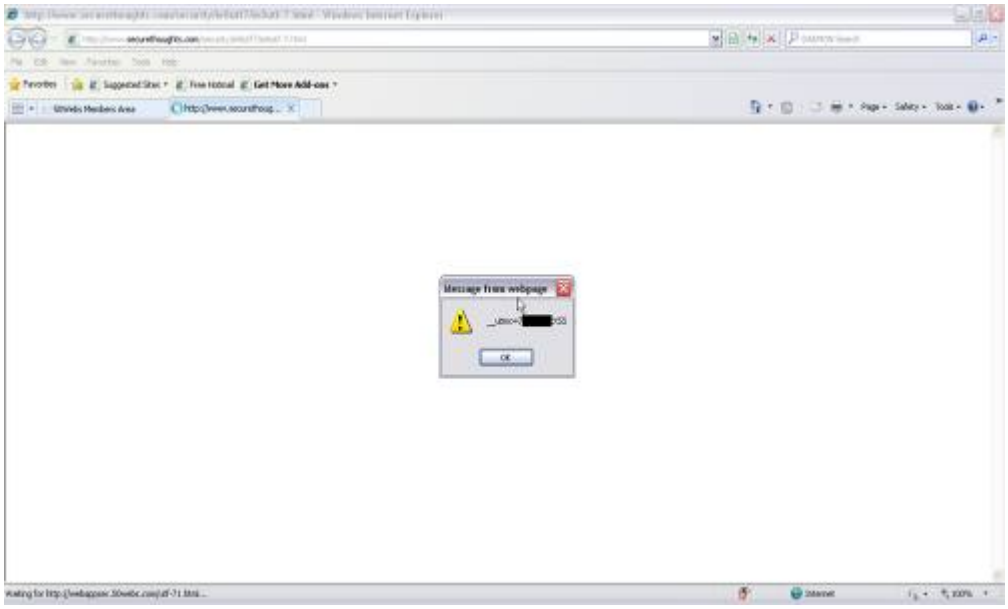
http://www.securethoughts.com/security/ie8utf7/ie8utf-7.html.

1. The page loads into your IE8 browser.

**4. IE8 thinks that it is loading a child page - [http://www.securethoughts.com/security/ie8utf7/utf-71.html] from the same domain and hence removes the restriction on charset inheritance.**

1. This is where Local Redirection Attack comes into play. The attacker sets a temporary redirect on the child page to vulnerable site [http://webappsec.50webs.com/utf-71.html]. Make sure that the link to vulnerable site is a page with your UTF-7 injected characters [Persistent/Reflected XSS]. In this case, my utf-71.html page on 50webs.com has a persistent XSS with UTF-7 characters.

1. The XSS executes in the context of vulnerable site. E.g. if you see below, you can see my 50webs.com member cookie appended with 'XSS' in an alert box.



I have been in touch with Jack from Microsoft Security Response Center (MSRC) team for the last 2 months. I would like to thank the Microsoft Security Team for their timely responses and letting me discuss these issues with the security community. They are actively working to resolve this issue and a fix for this vulnerability is expected to arrive in the next version of Internet Explorer, IE9.

---