Security Advisory

Cross Site Scripting (XSS)

Amish Shah
Chief Technology Officer
mailto:amish@net-square.com
net-square solutions pvt. ltd.
http://www.net-square.com
23rd July 2007

Advisory ID: NS-072307-XSS

URL: http://reserach.microsoft.com/search/search.aspx
OS: Windows XP SP2
Browsers: Internet Explorer 6.0, Firefox 2.0
Severity: High

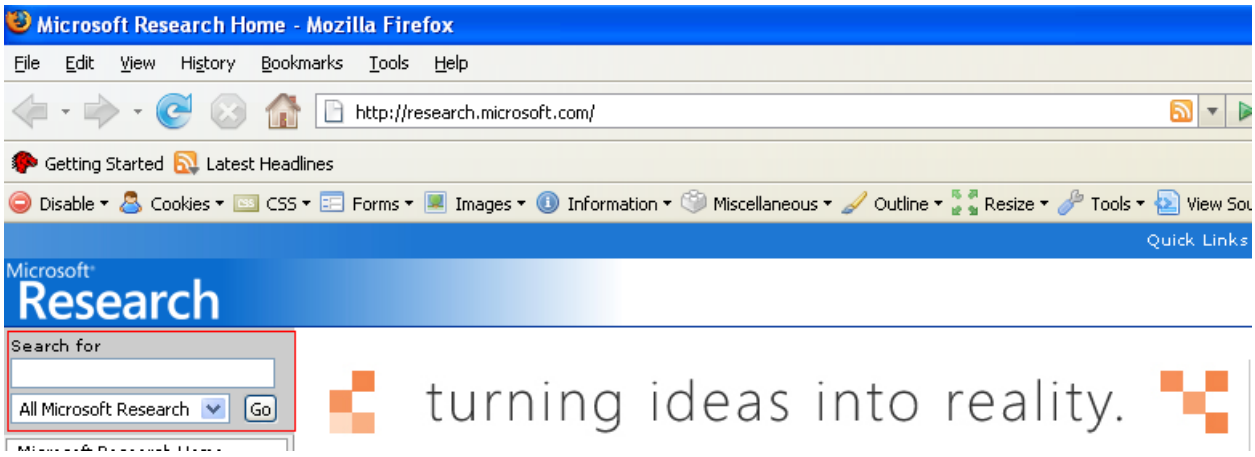
Vendor Response

Microsoft Security Response Center (MSRC) identified this bug immediately and rectified also. The acknowledge reference found at,

http://www.microsoft.com/technet/security/acknowledge/default.mspx

Proof of concept:

Microsoft research website home page



Microsoft research home page contains an html form to search various data into different Microsoft research locations. The form is shown in the above image with red border. The search form details are as follows,

http://research.microsoft.com/

1 form

Form

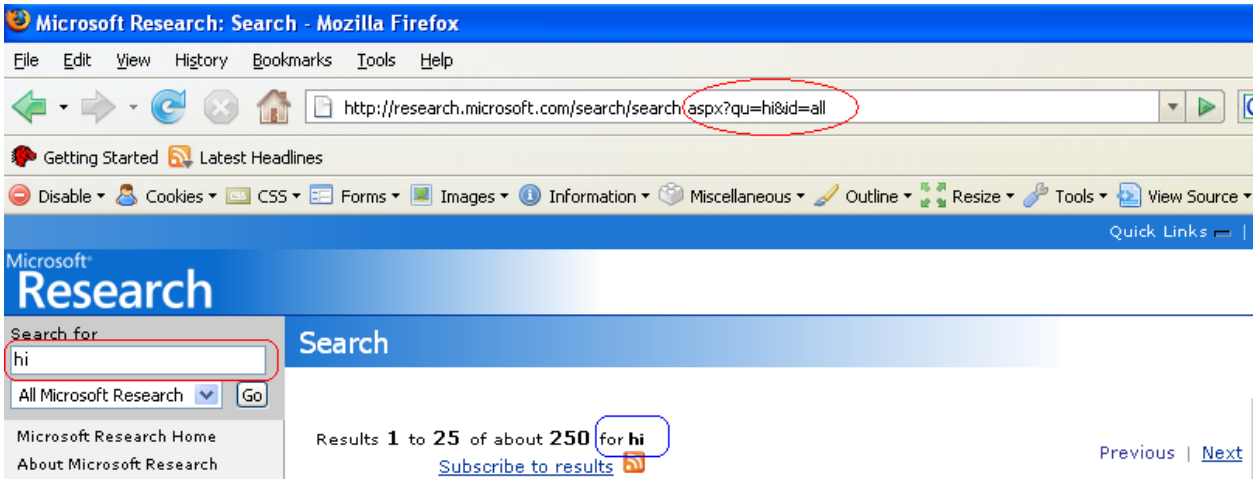
ID	NAME	METHOD	ACTION
			/search/search.aspx

Elements

INDEX	ID	NAME	TYPE	VALUE	LABEL	SIZE	MAXIMUM LENGTH
0	qu	qu	text				255
1		id	select				
2			submit	Go			

The form is sending GET request to /search/search.aspx with two query string parameters, “qu” and “id”, where “qu” contains the search text which you’ve entered to search and “id” contains the region.

So, if you write “hi” in a search box, the URL will be,



http://research.microsoft .com/search/search.aspx?qu=hi&id=all

So, web server fetches the search text from “qu” parameter of the query string and location value from “id” parameter of the query string. Web server searches search text (“hi”) into a database and returns results back to the browser.

And, if you look at response in an image with blue border, it displays same search text (“hi”) also in a response which you’ve entered to search, so web server returns search text also along with the results. So, from that you can imagine that there can be a possibility of “Cross Site Scripting” XSS attack, if server doesn’t validate and encode search text.

So, modify “qu” parameter value to, “<script>alert(“hi”);</script> in a browser address bar itself, So URL will be,

http://research.microsoft.com/search/search.aspx?qu=%3Cscript%3Ealert(%22hi%22);%3C/script%3E

And, if you hit enter, web server fails to validate the search text and return the same script along with results in an html response and you’ll get “hi” alert box on your browser.

Countermeasure:

Cross Site Scripting (XSS) is a very well known attack. Proper input validation and html encoding of response parameters prevents this attack.

References:

http://support.microsoft.com/kb/252985
http://www.asp.net/faq/RequestValidation.aspx

DISCLAIMER

THE INFORMATION CONTAINED IN THIS ADVISORY IS THE COPYRIGHT (C) 2007 OF NET-SQUARE SOLUTIONS PVT. LTD. AND BELIEVED TO BE ACCURATE AT THE TIME OF PRINTING, BUT NO REPRESENTATION OR WARRANTY IS GIVEN, EXPRESS OR IMPLIED, AS TO ITS ACCURACY OR COMPLETENESS. NEITHER THE AUTHOR NOR THE PUBLISHER ACCEPTS ANY LIABILITY WHATSOEVER FOR ANY DIRECT, INDIRECT OR CONSEQUENTIAL LOSS OR DAMAGE ARISING IN ANY WAY FROM ANY USE OF, OR RELIANCE PLACED ON, THIS INFORMATION FOR ANY PURPOSE.