

Re: Displaying User–Supplied String

Source:

<http://www.tech–archive.net/Archive/DotNet/microsoft.public.dotnet.framework.aspnet/2007–10/msg00431.html>

- *From:* Jesse Houwing <jesse.houwing@xxxxxxxxxxxxxxxxxxxx>
 - *Date:* Wed, 3 Oct 2007 23:29:08 +0000 (UTC)
-

Hello Jonathan,

Right. I tested it by surrounding my input with and . To my surprise, it causes an unhandled exception: A potentially dangerous Request.Form value was detected from the client (ctl00\$ContentPlaceHolder1\$description="Property1").

Not sure yet where the error is being thrown from exactly, but I'm looking into it.

By default any input containing either a piece of javascript code or a html tag will be rejected by ASP.NET from versin 1.1 and higher.

You can switch this automatic validation off from the web.config or the page directive of teh aspx file in question:

http://www.cryer.co.uk/brian/mswinswdev/ms_vbnet_server_error_potentially_dangerous.htm

Jesse

"Jesse Houwing" <jesse.houwing@xxxxxxxxxxxxxxxxxxxx> wrote in message news:21effc90205bd8c9d43b6960ffef@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

Hello Mark Rae [MVP],

"Jonathan Wood" <jwood@xxxxxxxxxxxxxxxxxxxx> wrote in message news:OqKJvmgBIHA.5868@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

Okay, I have a site that displays information based on user input, a couple of the items are plain strings that

Re: Displaying User–Supplied String

the user entered.

I understand the risk here is that they could insert javascript or whatever in their string and, when my page displays it, that script could be executed.

What is the best approach for preventing that?

Are you talking about SQL Injection i.e. the strings supplied by the users are used to look up records in a database?

If so, you need to use parameterised queries or stored procedures.

Google "SQL injection"

There's more than SQL injection at work here. apart from SQL injection there is the risk of cross site scripting as the original poster correctly identified. Best way to prevent that is to call Server.HTMLEncode on each field before displaying it. I usually don't encode the data before putting it into the database as the data might be used in a non–web environment as well (reporting, windows client etc).

So encode before displaying.

—
Jesse Houwing
jesse.houwing at sogeti.nl

—
Jesse Houwing
jesse.houwing at sogeti.nl

.