

## Re: Error

**Source:**

<http://www.derkeiler.com/Newsgroups/microsoft.public.dotnet.framework.aspnet.security/2003-04/0275.html>

---

**From:** Victor Garcia Aprea [MVP] ([vga@NOobiesSPAM.com](mailto:vga@NOobiesSPAM.com))

**Date:** 04/23/03

From: "Victor Garcia Aprea [MVP]" <[vga@NOobiesSPAM.com](mailto:vga@NOobiesSPAM.com)>

Date: Tue, 22 Apr 2003 20:44:04 -0300

Hi Jeff,

>>>> *"You should double check the decision of disabling this as  
>>>> its usually not a good idea"*

This is really important and I think you're mixing things a bit, let me try to explain it:

Security rule #1: Check your inputs. Any application (web or not) should check its inputs. In ASP.NET 1.0 there was not built-in feature to do this, which meant you had to code it for yourself for any real web application deployed, for example I added this feature to our custom web app framework. Then came ASP.NET 1.1 with this built-in feature (turned on by default) so any application will have stronger security settings right out of the box. In our case we're not currently using it because we've already coded a similar one. If you were not watching for this in 1.0 then you were actually risking the security of your customers websites. ASP.NET 1.1 is just trying to make people aware of this issue and providing a built-in feature to help in its implementation.

>>> *the decision to disable any security feature is a major decision.*  
Sure it is. Its very important that you understand what this feature is about: checking the content posted in forms, querystring and cookies collection. This content should always be checked against, in 1.0 bits you had no choice, the checking had to be performed by you; now in 1.1 bits you may want to let ASP.NET do the checkings for you (of course you can still use our own checking).

>>> *So the bottom line is:*

>>> *1. Risk customer attack (never)*

You're already risking it if you haven't coded such a feature in ASP.NET 1.0. If you're already protecting yourself from dangerous content then you may not need the 1.1 feature.

>>> *2. Stay on 1.0*

Re: Error

microsoft.public.dotnet.framework.aspnet.security: Re: Error

In 1.0, without any additional code from your part for preventing dangerous content from being posted you may be already risking the security of your customer website.

>>> *3. Rewrite tons of code.*

I don't see any reason for a rewrite here.

>>> *"Ya dot.net only runs if you turn off all the security*