Asp.Net Validaterequest False

Asked 15 years, 8 months ago Modified 15 years, 8 months ago Viewed 2k times

3

I'm creating an Asp.Net program UI where users can browse and change information in a database. For this reason, they need to be able to use all forms of chars, but I still need to keep the program HTML and SQL itself secure. For that reason, I'm using a self-built method that replaces dangerous chars such as '<' etc with their html-codes while they're being handled outside of a textbox (issued on page-load so they have no functionality in there).

Now my dilemma: To be able to do this, I have to disable the Validaterequest parameter as per the topic, the program will issue a complaint. What are the possible consequences of setting it to False?

The SQL query is parametirized already, and I filter out the following marks only:

```
& # < > " ' % @ =
```

Question: am I leaving the program open for threats even if I handle the chars above? Basically this is an intranet application where only a few people will be able to access the program. Nevertheless, the information it accesses is fairly important so even unintentional mishaps should be prevented. I literally have no idea what the Validaterequest thing even does.

Edit: Alright, thx for the answers. I'll just go with this then as initially planned.

asp.net validation

Share
Improve this question
Follow

edited Apr 3, 2009 at 8:55

asked Apr 3, 2009 at 8:18

Zan

317 ● 4 ● 8 ● 17

3 Answers

Sorted by: Highest score (default)

4

The main things Validate Request is looking for are < and > characters, to stop you opening your site up to malicious users posting script and or HTML to your site.

If you're happy with the code you've got stripping out HTML mark-up, or you are not displaying the saved data back to the website without processing, then you should be

ok.

Share Improve this answer Follow

answered Apr 3, 2009 at 8:27

Zhaph - Ben Duguid

27k ● 5 ● 84 ● 122

2

Basically validating user input by replacing special characters usually cause more trouble and doesn't really solve the problem. It all depends what the user will input, sometimes they need the special characters like

```
& # < > " ’ % @ =
```

think about savvy users could still use xp_ command or even use CONVERT() function to do a ASCII/binary automated attack. As long as you parametrized all input, it should be ok.

Share Improve this answer Follow

answered Apr 3, 2009 at 8:33

Liwen

937 ● 10 ● 12

1

i think that the problem is not only about SQL injection attacks, but about Cross Site Scripting and JS execution attacks. To prevent this you cannot rely on parametrized queries alone, you should do a "sanitization" of the html the user sends! maybe a tool like html tidy could help.

Share Improve this answer Follow

answered Apr 3, 2009 at 9:22

pomarc

2,224 ● 4 ● 25 ● 30