

Re: GET or POST method?

Source: <http://coding.derkeiler.com/Archive/PHP/comp.lang.php/2008-01/msg01232.html>

- *From:* The Natural Philosopher <a@xxx>
 - *Date:* Tue, 15 Jan 2008 19:11:11 +0000
-

Michael Fesser wrote:

.oO(The Natural Philosopher)

Either method works: a GET method is slightly insecure, in that an average idiots can fake a URL and maybe get where they shouldn't:

If this can happen, then there's something seriously broken in the scripts. Even if they can get there, they shouldn't be able to do anything.

Its harder to do with POST. There you would have to make up a web page form to submit with POST to the URL you were trying to screw with.

Not necessarily. There are tools that make it very easy to send arbitrary POST data to any script. Even the WebDeveloper toolbar in Firefox has some nice form functions, which allow to change the send method, to modify hidden or read-only fields before sending etc.

And there are some more things about security to consider. Just three little examples, which clearly show why it's a bad idea to use GET to manipulate the server's state:

<http://groups.google.com/group/comp.lang.php/msg/42c80631acf96223>

http://thedailywtf.com/Articles/The_Spider_of_Doom.aspx

The third one happened in my own scripts. I used to have a little form for the users to log out. It simply showed a text like "are you sure..." and a button to confirm. Pressing it sent a POST message to the server, causing the user to get logged out. Worked quite well.

But then someone who uses my framework on his own sites said that this additional confirmation step would be rather useless for his visitors and they should be able to log out immediately by just following the

Re: GET or POST method?

/user/logout link. OK, so I changed it, since in this case the performed action is nothing critical. At least that was what I thought. But then something strange happened in Firefox.

I also use automatically generated link elements in my document's heads to indicate related documents: home, search, index, up, previous and next document and so on. Some browsers show these links as an additional toolbar, which I find quite useful. Firefox takes it a step further and already downloads the next document (if there is one) in the background. The problem was: If the user was on his own profile page /user/profile, the next document in order was /user/logout ... The nice page preload function turned into an auto-logout.

Micha

Nice story Micha! and one I will bear in mind.

All I was really saying was that all a user has to do with a GET variable, is notice what is going on in the URL window, fiddle with it, and maybe do strange stuff.

To do it with POST takes a *bit* more nous. Not a lot, but a bit.

You need to do data validation on both, if you care about data validity :-)

.