

Re: Form Security

Source: <http://coding.derkeiler.com/Archive/PHP/comp.lang.php/2006-03/msg00772.html>

- *From:* Scott <nospam@xxxxxxxxxx>
 - *Date:* Sat, 11 Mar 2006 22:45:13 -0500
-

Ok, Guys! I didn't mean for this discussion to get so heated!! Shake mice and make up!

Now, back to the task at hand. Here's what I have so far...

This is a simple contact form. I have the following fields: name, company, email, phone, subject (which is chosen from a dropdown list), and message (a textarea field). I am also using a hidden field called originator which contains the random code, as well as assigning that same value to `$_SESSION['code']` as discussed earlier.

The form contents are to be emailed, and possibly stored in a database. We'll just worry about email for now.

When the form is submitted, the first thing I do is ensure the hidden field matches the session variable. If it does, the form processing begins.

The form processing script so far does the following:

- 1) Take each of the text fields, run them through `trim()` and `strip_tags()`, and assign them to a variable. That variable is then checked against a regular expression. If they do not match the expression, an error message such as "Please re-enter your email address." will be displayed along with the form, and with all of the information they just entered.
- 2) The subject must match one of the options in the drop down list. For now, if it doesn't, I'm just pulling the plug with `exit()`, because this obviously isn't valid data.
- 3) With the message, I want to be fairly flexible, mainly because this is a contact form for potential customers to contact me, and I don't want to annoy them into going elsewhere. I am running it through `trim()` and `strip_tags()`, but haven't decided yet on a regular expression to use, or even if I really need to.

After all this, if no error message has been generated, the form contents are emailed to me. Since this data is being passed to a `mail()` function, spam was pretty much my main concern. However, I'm wondering also, would you deem it necessary to use `escapeshellcmd()` on this data as well? I'm no Linux guru, so I don't know what someone could do to cause problems with this script, other than spam me.

What further steps would you take on this script?

Scott

Jerry Stuckle wrote:

Re: Form Security

Chung Leong wrote:

Jerry Stuckle wrote:

Chung Leong wrote:

Jerry Stuckle wrote:

And I wasn't interpreting it in the "worst of light". I was interpreting it in the light of simple security.

What he's proposing is false security – which is worse than no security at all. At least with the latter you know you have potential vulnerabilities.

I really don't know what to say. The OP proposed a method for stopping one type of cross-site scripting attack and here you are insisting that it's crap because it doesn't stop bots.

And it doesn't stop what he's trying to stop!

How so? Because...it doesn't stop bots?

You can't see your solution is total trash? I'm sorry for you – and even more so for your customers. I hope I never have to take over a site you've worked on.

I'm not even going to bother to continue this discussion.

Re: Form Security

You go ahead and give people a false sense of security. I hope no one gets hurt by your poor advice.

Meanwhile – I'll continue a conversation with the original poster – but you're not worth the time.