

Re: [PHP] is there a problem with php script pulling HTML out of database as it writes the page??

Re: [PHP] is there a problem with php script pulling HTML out of database as it writes the page??

Source: <http://coding.derkeiler.com/Archive/PHP/php.general/2008-07/msg00793.html>

- *From:* stuttle@xxxxxxxxxx (Stut)
 - *Date:* Thu, 17 Jul 2008 17:32:06 +0100
-

On 17 Jul 2008, at 15:41, Daniel Brown wrote:

On Thu, Jul 17, 2008 at 9:55 AM, Stut <stuttle@xxxxxxxxxx> wrote:

Seriously though, I'm wondering if my expectations are too high... I expect them to know that addslashes is not adequate protection against SQL injection. I even had one tell me "SQL injection? I can't remember but I'm sure I've used it before". And I won't even go into the guy who asserted that he's always worked with DB administrators who've dealt with security issues so he'd never needed to learn about it.

1.) It's obvious that addslashes() is not protection against SQL injection attacks. That's why God invented htmlentities() and flatfile databases.

Yup, had that one.

2.) No PHP programmer should ever be required to know anything about databases, server management, mail, or anything. This is because we all know that we'll someday all work in a Google-like atmosphere with enough funding to hire other people to work with databases, servers, HTML, and even a Senior JavaScript Engineer.

I have a ghostwriter who keeps me active on the mailing lists. Best 50p I spend every week!

3.) "SQL injection" is just a buzzphrase. I already know where baby databases come from.

The big Daddy database spends lots of CPU cycles on the big Momma database and she eventually lets him

Re: [PHP] is there a problem with php script pulling HTML out of database as it writes the page?? 1

Re: [PHP] is there a problem with php script pulling HTML out of database as it writes the page??

put his SQL client into her console and their SQL statements intermingle until something magic happens. At least that's what my Daddy told me when I was a little regex.

4.) Any web programmer worth his or her salt knows that PHP, while a great language, is not compatible with all browsers. Especially Microsoft. For people using Windows, you'll need to have an ASP website.

Indeed. And PHP can't be used for foreign language sites, only US English. It makes a complete mess of British English sites.

5.) Never sanitize input. It takes too long, and unless you're dealing with credit cards, no one will ever want to hack your website. If you are taking credit cards, store them in a firewalled database.

You say this, but the person I just did a phone interview with did tell me that security is a cost-benefit calculation in terms of both development time and runtime resources. He said he never bothers escaping input in Intranet sites. True story!

6.) If you need to copy files from one server to another, make sure you use FTP over HTTP. It's more secure.

I use an Oompa-Loompas – much more reliable!

7.) register_globals is your friend.

And I hug her, and kiss her and squeeze her tight. *pop*

8.) The best, most-scalable way to create an expandable website is to use a switch page. Just tack on a `?page=faq.php` query to your GET request, and have PHP automatically ``include($page)`` (see point #7) in your switch file.

Ooh, dangerous. I worry about relative paths, so when I do this it's always with an absolute path... i.e. `?page=/var/www/mywebsite.com/somedir/faq.php`

9.) NEVER store passwords in a PHP script. Instead, store them in a file named ``inc/config.inc`` in the web directory, and include them.

Re: [PHP] is there a problem with php script pulling HTML out of database as it writes the page?? 2

Re: [PHP] is there a problem with php script pulling HTML out of database as it writes the page??

I prefer to use .txt as the extension. Makes opening them in Notepad so much easier.

10.) If running a picture- or file-sharing website, make things easier on your users and yourself. Allow users to delete their files by using a simple link like:
<http://www.example.com/delete.php?file=images/mygraphic.jpg>. Then, in delete.php, have only one line: `<?php unlink($file); ?>` (again, see point #7 --- see how much that's coming in handy now?)

This works best if the web server is running as root. None of those annoying error messages about not being able to open files that I know are there!

11.) The most important rule EVER: if you ever have the slightest problem, DO NOT bother to search the #@\$% web (STFW) or read the #@\$%^ manual (RTFM). There is a mailing list for that. Please ask any and all questions there, including why your MP3's aren't streaming on your AnalogX webserver from your home PC to your buddies in Antarctica after you turn your computer off. "But when I turn my computer off, the rest of the Internet still works! Hlp me pls!!!!!" We are here only to serve you. People on mailing lists are paid to write your code and do your homework for you, and you should expect nothing but the best, immediate answers, 24/7/365. If they don't respond within 90 seconds, please repost your message every 90 seconds until someone does. When in doubt, hijack a thread.

Why do birds suddenly go *poof*, every time, you are near?

-Stut

--

<http://stut.net/>

.