Subject: privately coded message board [php & mysql]
Posted by lookitzhiep on Sat, 24 Feb 2007 23:45:21 GMT
View Forum Message <> Reply to Message

I've been developing my own message board in PHP and MySQL. I wanted to ask a question before I further my development. Is this a bit safer method to coding my own than to use one such as IPB and vBulletin?

I was thinking since its my own, the exploits would be harder to find since the source isn't available, right?

Another question to pose as well; I'm addslashes()'ing any data being inserted into the database and stripslashes()'ing any data being displayed. Is there any flaw to this as well as a better way to prevent XSS and SQL injections?

Subject: Re: privately coded message board [php & mysql]
Posted by Blazer on Sat, 24 Feb 2007 23:51:46 GMT
View Forum Message <> Reply to Message

I would research how current php exploits work, so that you know how to not make the same mistakes. Most exploits take advantage of SQL injection, or finding a way to pass data so that it is eval'd and executes local shell commands.

Subject: Re: privately coded message board [php & mysql]
Posted by genetix on Sun, 25 Feb 2007 00:11:12 GMT
View Forum Message <> Reply to Message

If you are at the stage in PHP developement where you are relying on addslashes then I wouldn't recommend moving onto a large project such as a forum.

You will want to convert all characters to entities for sure. If you don't do that you will run into trouble. This also makes it so that there aren't any restrictions needed as far as quotes goes.

I would recommend hanging out here for a while first:
http://www.devnetwork.net

Subject: Re: privately coded message board [php & mysql]
Posted by lookitzhiep on Sun, 25 Feb 2007 00:20:02 GMT
View Forum Message <> Reply to Message

genetix wrote on Sat, 24 February 2007 18:11If you are at the stage in PHP developement where you are relying on addslashes then I wouldn't recommend moving onto a large project such as a forum.

You will want to convert all characters to entities for sure. If you don't do that you will run into trouble. This also makes it so that there aren't any restrictions needed as far as quotes goes.

I would recommend hanging out here for a while first:
http://www.devnetwork.net
Thanks for the link, I'm really just a beginner in PHP. I began to learn it as I had interest in coding one myself. I bought a book recently and its just getting me on my feet with the basics so I wouldn't know of such yet.

Entities would be when a character such as "<" appears as "<" right? That seems much better than having to addslashes() and stripslashes() everything! Thanks! Though if I apply this method, would I still need to filter URLs out?

Subject: Re: privately coded message board [php & mysql]
Posted by Cpo64 on Sun, 25 Feb 2007 04:14:46 GMT
View Forum Message <> Reply to Message

Custom forums will keep away the "lazy hacker" or script kiddies.
But unless its actually secure, it won't keep out a determined hacker.

Subject: Re: privately coded message board [php & mysql]
Posted by Goztow on Sun, 25 Feb 2007 09:59:36 GMT
View Forum Message <> Reply to Message

Ask yourself the question: is there a reason someone would attack your forums?

I once coded my own, very basic, forum just for leaving messages with replies. But that was just for auto-study and practise .

Usually if you use a free php-forum, you should be ok as long as you keep up to date. Forums like phpbb also have a huge modification community behind it which allow you to modify a lot of things, including security (www.phpbbhacks.com is a great site).

Subject: Re: privately coded message board [php & mysql]
Posted by lookitzhiep on Sun, 25 Feb 2007 19:42:29 GMT
View Forum Message <> Reply to Message

Goztow wrote on Sun, 25 February 2007 03:59Ask yourself the question: is there a reason someone would attack your forums?

I once coded my own, very basic, forum just for leaving messages with replies. But that was just for auto-study and practise .

Usually if you use a free php-forum, you should be ok as long as you keep up to date. Forums like

phpbb also have a huge modification community behind it which allow you to modify a lot of things, including security (www.phpbbhacks.com is a great site).
My primary focus is to get the forum up and running and then iron out any exploits. I don't really think anyone would attack my forum but I'm a paranoid guy sometimes. x]

Also I prefer to code a message board on my own. I know about phpBB (but it's widely used and unoriginal to me) and I want to see how far I can get into coding in PHP even if I have to code modifications myself. Thanks though.

Subject: Re: privately coded message board [php & mysql]
Posted by Goztow on Sun, 25 Feb 2007 20:20:13 GMT
View Forum Message <> Reply to Message

If you want to use it as exercice, then by all means do so! It will be a good practise.

PHPbb can be modified so u hardly recognise it's phpbb. I modified mine at thekoss2.org/forum bigtime, but u mostly see it when acually using it .

Subject: Re: privately coded message board [php & mysql]
Posted by danpaul88 on Sun, 25 Feb 2007 21:12:40 GMT
View Forum Message <> Reply to Message

Also a fairly new forum system which I personally like a lot better than phpBB is SMF, check it out at www.simplemachines.org

---

Subject: Re: privately coded message board [php & mysql]
Posted by Crimson on Sun, 25 Feb 2007 22:11:21 GMT
View Forum Message <> Reply to Message

If you're paranoid about security for your forum, FUDForum is the way to go. The guy who develops it not only wrote a book on PHP security, but he's also on the team that develops the language of PHP itself. That's why I use it on all my forums.

Subject: Re: privately coded message board [php & mysql]
Posted by Whitedragon on Mon, 26 Feb 2007 05:00:13 GMT
View Forum Message <> Reply to Message

danpaul88 wrote on Sun, 25 February 2007 16:12Also a fairly new forum system which I personally like a lot better than phpBB is SMF, check it out at www.simplemachines.org
SMF is good. I find the code easy to work with and its mod package system is very handy.