

Re: Database security – PHP code

Source: <http://coding.derkeiler.com/Archive/PHP/comp.lang.php/2004-10/0845.html>

From: Michael Fesser (*netizen_at_gmx.net*)

Date: 10/14/04

Date: Thu, 14 Oct 2004 19:44:11 +0200

.oO(Dariusz)

>I have been reading a little that you should secure your PHP code to
>prevent SQL injection into a database (MySQL in my instance), mainly by
>checking the type of data to be put into a database, and if text, to
>addslashes() the data.
>
>What I have not managed to find out, is does SQL injection threaten the
>input of data into a database

Yep.

>, ie a guestbook, or the reading of a database
>where the user would not know if the data is being read from a database?

Not directly, but the problem is more complex.

An example: It could be possible for an attacker to insert SQL-code into the database. The application escapes all quotes, so it does no harm on input. But even if the code made it "defused" into the database doesn't mean the problem is solved. The injected code could still start its malicious work when the application fetches the data from the db and uses it again in another query. Usually no one escapes data obtained from the db, because it's considered "safe" ...

>Is there anything else to consider to make a database more secure?

Even if the data is already in the system, it should `_not_` be used directly in other queries without validating/escaping it again.

And some SQL servers are vulnerable to a lot more and different variants of SQL injection (Google for "advanced SQL injection").

>In particular, I have read here a few months back that it's a good idea to
>keep the username / password of the connection outside the root of the
>website. How would I access the password file then? What I mean is, if I
>want a certain file in my site I could access it by writing:

comp.lang.php: Re: Database security – PHP code

>

>www.mysite.com/password.php

Why would you want a password be accessible with HTTP?

>*But as it would now be outside the root, how would I be able to get to the*

>*password.php file?*

PHP is able to access files directly through the filesystem.

Micha