Subject: hiding control.inc database connection details
Posted by stephenboey on Sun, 04 Feb 2007 21:59:14 GMT
View Forum Message <> Reply to Message

Hi Tony,

I am not sure where I should post this.

1. Where do you store your port information for 3306? If I have more than one mysql installation how does your code know which one to connect to?

2. Do you know of a way in order not to hardcode the values of:
$GLOBALS['dbusername'], $GLOBALS['dbuserpass'] ? Its quite a big security risk because one these user names will have access to many databases.
Will appreciate any suggestions.

Subject: Re: hiding control.inc database connection details
Posted by AJM on Sun, 04 Feb 2007 23:48:47 GMT
View Forum Message <> Reply to Message

It is not usual to have more than one MySQL server on a single PC, which is why I have never implemented that option. You could try creating a new variable called $GLOBALS['dbport'] and adding that to the argument list in the connect() method. Let me know if it works and I'll add it to the standard code.

The values for $GLOBALS['dbusername'] and $GLOBALS['dbuserpass'] have got to be maintained somewhere, but to keep them secure on a public server you should put your INCLUDES directory (which contains the CONFIG.INC file) outside of your web root.

Subject: Re: hiding control.inc database connection details
Posted by stephenboey on Mon, 05 Feb 2007 08:57:38 GMT
View Forum Message <> Reply to Message

Looked through your connect method. Seems like there is a $dbhost variable for mysql_connect.

So I did a 'host:port' and it works.

I think there was an article you wrote about encryption.
The thing about php is, source codes are revealed and the $key has to be somewhere.

Usually if there is an IT audit, the first question asked is where do you store the $key?

I had to encrypt the key as well with another key stored in one of the variables in VB. VB programs are compiled, so no worries there....

Subject: Re: hiding control.inc database connection details
Posted by AJM on Mon, 05 Feb 2007 09:15:41 GMT
View Forum Message <> Reply to Message

If the CONFIG.INC file is stored outside the web root then nobody can access it through the web server. If they have direct access to your PC (and malicious intent) then database passwords are the least of your worries.

PHP is interpretted, not compiled, so no binaries are involved. All the files are plain text and can be viewed and modified with any text editor.