Subject: Re: OWASP standards vs. Radicore Framework
Posted by AJM on Thu, 29 Jun 2006 17:17:03 GMT

View Forum Message <> Reply to Message

By default the INCLUDES folder in the zip file is within the same directory as all the other files for the simple reason that the unzip facility can only create a single directory structure. I cannot force the INCLUDES folder to be outside the web directory, but I do advise it when the software is installed on a publicly-accessible web server.

You must also bear in mind that the software is a development tool and should be installed on a development server to begin with. When developing and testing on either of my two Windows PCs, a desktop and a laptop, the INCLUDES folder is not outside the web root, but this does not cause a security issue.

I assume that developers who are going to deploy software on a publicly-accessible server are aware of all the security implications and know what steps to take. It is not my responsibility to educate developers on how to configure and use a web server, how to configure and use PHP, or how to configure and use a DBMS. I assume they already have this knowledge.

I should also point out that if a web server is mis-configured enough to send back a .inc file as plain text it can also do the same thing to a .php file. Any file which is accessible to the web server has the *potential* to be sent back without being processed, so if your web server is mis-configured you are likely to spot it very quickly. Saying that it only applies to .inc files is a little naive.