Subject: Re: OWASP standards vs. Radicore Framework
Posted by AJM on Thu, 29 Jun 2006 15:48:26 GMT
View Forum Message <> Reply to Message

I use the .inc extension to indicate that that a file can only be included and not executed in its own right. This is an important difference to most people.

I include in my installation instructions the means to tell Apache not to allow access to any files which end in the '.inc' extension.

Even if these instructions were to be ignored there should be no security issues as all the critical .inc files are held in a directory which is outside the web root and are therefore totally inaccessible even if Apache were to be mis-configured.

Those .inc files which are not outside the web root are in their own separate directories which could easily be password protected or set to be inaccessible via the web server.

The OWASP recommendation does not take these other options into account, so the "security hole" is not as bad as they would make out.