Subject: Re: OWASP standards vs. Radicore Framework
Posted by andy on Thu, 29 Jun 2006 16:09:28 GMT
View Forum Message <> Reply to Message

Hey Tony,

you are on top things, that was one fast reply

I am onboard with using extensions to differentiate file usage, it makes sense to me. However, my employer (as a company) is security paranoid (obsessed, maybe).

Your instructions do clearly layout the usage of non-web path placement of the includes folder.

But nonetheless, one must consider the programmers daily battle against the "idiot factor". Even that the idiot may be the next developer, who may not configure a server correctly.

I don't quite get this point,

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.

... when I did a simply unzip and drop into my web root, the "includes/config.inc" is readily viewable. The only thing stopping a text display of the is the .htaccess setttings.

IF (the bit about .inc files is omitted)you_have == trouble;

Don't get me wrong, I'm not trying to bash. I'm a fan of your work, have been for some years now. Just seems to me that by using the .php extensions, with entry point checks (not to get off on a tangent) one could have a framework that is secure regardless of server configurations.