Subject: OWASP standards vs. Radicore Framework
Posted by andy on Thu, 29 Jun 2006 15:32:40 GMT

View Forum Message <> Reply to Message

Greetings,

Finally I have the opportunity to review this full release of the Marston web framework. I've been busy working with Python the last few months, giving me a new perspective on things   .

Q: Recently I was taken to task for using extensions such as ".inc" rather than standard ".php". The problem, related to OWASP security recommendations for php applications, is that if your server is not configured correctly then .inc files will dump as plain text to the browser. This is a potential security hole. The premise of OWASP philosophy, for background here, is that one should never trust a server configuration. Being that web application code can be deployed on any server, many of which will be hosted and of course the developer may very likely have no influence on server (Apache) configuration settings.

Wondering why this framework code still uses the ".inc" extension?

Shouldn't the OWASP recommendation be heeded?

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.

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.

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.