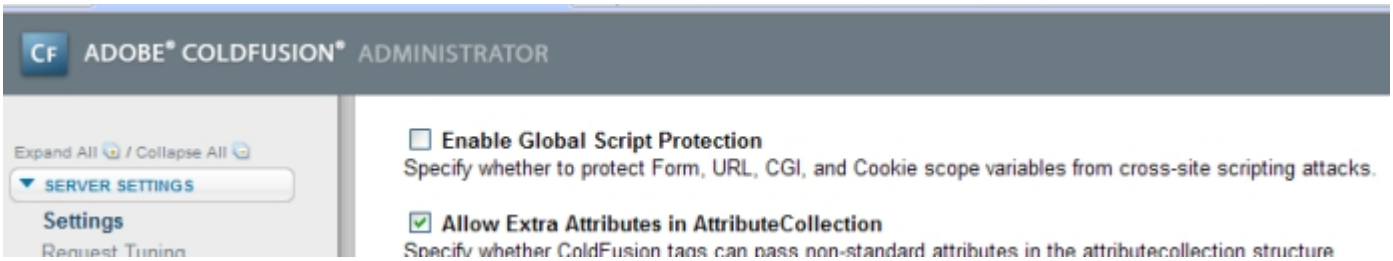
Cross-Site 'ScriptProtect' functionality in CF 7+

Posted At : 8 April 2009 11:30 | Posted By : Shaun McCran
Related Categories: Security, Coldfusion, Best practices

Until recently I was using a variety of method to stop cross-site scripting attacks, including htmlEditFormat() and a few regular expressions in my frameworks to strip out unwanted characters in returning variables.

I wasn't even aware that there was a 'scriptProtect' setting in ColdFusion until I bumped into it whilst writing a new login CFC recently, so I thought I'd take a closer look.

The first, and most 'global' option is in Cf Admin. If you go to the 'settings' screen there is an option, 'Enable global script protection'. This will enable the option for all sites running on that server. Obviously a bit heavy handed, but I'm not seeing a down side to this at the moment.



Secondly you can set this value in your Application code.

For Application.cfc

```
<cfscript>
this.name = "applicationName";
 this.scriptProtext  = "all";
</cfscript>
```

Or for Application.cfm

```
<cfapplication name="applicationName" scriptprotect="all">
```

The values for the scriptProtect variable are:

all
cgi
cookie
form
form,url
form,url,cookie
none
url

Most of these are obvious really. You can set a delimited list of the scopes you want to protect, or specify 'all' or 'none' for more global covering.

So what actually happens with this option enabled? It essentially replaces certain tags, such as script, object, applet, embed, with the text "InvalidTag". (Functionality I've noticed in BlogCFC as a side note.)

So it translates something like:

```
<s cript>alert('Hello world');</script>
```

Into:

```
<InvalidTag>alert('Hello world');</script>
```

There doesn't appear to be any conflict between setting the value in CF Admin, and your Application scopes, so I'd probably do both, it can't hurt.