Script Injection: File Upload Using a Subdomain

Posted At : September 21, 2009 10:12 AM | Posted By : Mark Kruger
Related Categories: Coldfusion Security

If you read my post on the script injection attack that has been going around you will note that I suggest four solutions or remedies to protect your server (upload off the web root, use cfcontent, disable script and execute permissions on certain directories, and remove superfluous handlers). A fifth solution was pointed out to me that is somewhat related to uploading off of the web root.

The idea would be to create a subdomain just for user resources. So, for example, you could have "www.ilovemoles.com" and "pics.ilovemoles.com". User uploads would go the share for the "pics" subdomain and be served from there. You would still vet the content to make sure it was ok, but the "pics" domain would not allow ColdFusion (or PHP or ASP or any scripts or executable at all). I can see some issues that you might run into - chiefly that you are not really "securing" the content from unauthorized access. I believe that still makes it suitable for public resources, but not able to be fully integrated into an application without a lot of run around. Still it seems an elegant solution.