How do I secure a folder used to let users upload files?

Asked 16 years, 4 months ago Modified 14 years, 8 months ago

Viewed 6k times

4

I have a folder in my web server used for the users to upload photos using an ASP page.

Is it safe enough to give IUSR write permissions to the folder? Must I secure something else? I am afraid of hackers bypassing the ASP page and uploading content directly to the folder.

I'm using ASP classic and IIS6 on Windows 2003 Server. The upload is through HTTP, not FTP.

Edit: Changing the question for clarity and changing my answers as comments.

security iis asp-classic iis-6 windows-server-2003

Share

Improve this question

Follow

edited Apr 21, 2010 at 12:18

Peter Mortensen

31.6k ● 22 ● 109 ● 133

asked Aug 22, 2008 at 14:38

Eduardo Molteni

39.4k ● 25 ● 144 ● 210

4 Answers

Sorted by: Highest score (default)

▲

3

▼

✓

also, I would recommend not to let the users upload into a folder that's accessible from the web. Even the best MIME type detection may fail and you absolutely don't want users to upload, say, an executable disguised as a jpeg in a case where your MIME sniffing fails, but the one in IIS works correctly.

In the PHP world it's even worse, because an attacker could upload a malicious PHP script and later access it via the webserver.

Always, always store the uploaded files in a directory somewhere outside the document root and access them via some accessing-script which does additional sanitizing (and at least explicitly sets a image/whatever MIME type.

Share Improve this answer Follow

answered Sep 8, 2008 at 14:35

pilif

12.7k ● 5 ● 36 ● 31

I'm accepting the answer but I'm still not sure if it is a really must having the file in a directory outside the document root. It will add some performance problems I think.
– Eduardo Molteni Sep 11, 2008 at 17:39

if you watch for correctly working caching, the performance problems will be negligible. I've answered how to do this in another question here:

beta.stackoverflow.com/questions/48555/… – pilif Sep 11, 2008 at 18:18

1

How will the user upload the photos? If you are writing an ASP page to accept the uploaded files then only the user that IIS runs as will need write permission to the folder, since IIS will be doing the file I/O. Your ASP page should check the file size and have some form of authentication to prevent hackers from filling your hard drive.

If you are setting up an FTP server or some other file transfer method, then the answer will be specific to the method you choose.

Share Improve this answer Follow

answered Aug 22, 2008 at 15:03

Ben Williams
2,297 ● 2 ● 19 ● 15

yes, I'm using an ASP page to do the upload, but...It is safe to give IUSR write permission to the folder? If a hacker try to post to same folder, IIS will be involved too. – Eduardo Molteni Sep 8, 2008 at 14:23

it's probably the most convenient method. Another solution would be to connect back to the server itself and re-upload the uploaded file via FTP for example, but the security benefit for the trouble is not really worth it. – pilif Sep 8, 2008 at 14:37

You'll have to grant write permissions, but you can check the file's mime type to ensure an image. You can use

0

FSO as so:

```
set fs=Server.CreateObject("Scripting.FileSystemObject
set f=fs.GetFile("upload.jpg")
'image mime types or image/jpeg or image/gif, so just
is instr
if instr(f.type, "image") = 0 then
   f.delete
end if
set f=nothing
set fs=nothing
```

Also, most upload COM objects have a type property that you could check against before writing the file.

Share Improve this answer Follow

answered Aug 23, 2008 at 17:17

chrisofspades
847 ● 1 ● 10 ● 17

You are getting it wrong. I'm asking about hackers bypassing the ASP page. – Eduardo Molteni Sep 8, 2008 at 14:16

You also cannot guarantee that the MIME type is correct since this is passed by the browser (as I recall). One should open the image via something like ImageMagik and check that the dimensions can be read properly. – nlucaroni Sep 8, 2008 at 14:31

0

Your best bang for the buck would probably be to use an upload component (I've used ASPUpload) that allows you to upload/download files from a folder that isn't accessible from the website.

You'll get some authentication hooks and won't have to worry about someone casually browsing the folder and downloading the files (or uploading in your case), since the files are only available through the component.

Share Improve this answer

Follow

answered Sep 16, 2008 at 21:57

user14094

23 ● 3