

Re: [PHP] Out source files

Source: <http://coding.derkeiler.com/Archive/PHP/php.general/2007-03/msg01379.html>

- *From:* manuel.vacelet@xxxxxxxx ("Manuel Vacelet")
 - *Date:* Wed, 21 Mar 2007 10:36:25 +0100
-

2007/3/21, Richard Lynch <ceo@xxxxxxxx>:

On Tue, March 20, 2007 4:37 am, Manuel Vacelet wrote:
> 2007/3/20, Richard Lynch <ceo@xxxxxxxx>:
>> One common pattern in PHP is to not put the file in the web tree at
>> all, and write a PHP script with 'readfile' (or fopen/fread/echo
>> loop
>> for larger files).
>>
>> You can then control access to the file, and log any kind of stats
>> you
>> need about accessing the file.
>
> Yes I already do that with all my scripts that are dealing with files.
>
>> Once you have that, then you can also put the files on some other
>> server, and use URL fopen to read them, if you like.
>
> Is it considered as secure ?

as secure as what? I don't think you've established a baseline for comparison...

It's a typo I wanted to write (more simple though) 'Is it secure ?'
In several PHP security recommendation we can read "Do not let PHP open URLs through fopen,".
I think it's mostly related to crapy php applications that could be let users do what they want but is there any other problems with this practice ?

Assuming you control the other server, you can make it as secure as you like...

The server is fully under my control and I can order other servers if I can highlight that's a better approach to ensure the security of the data we serve.

Re: [PHP] Out source files

That server can also reject any requests that aren't from your web server IP (or list of IPs for a web-server farm).

It's an approach but if my front-end is under the control of a cracker it will be unfortunately useless.

You could set it up with SSL and use curl instead of url fopen -- You'd probably not want to waste \$\$\$ on a CA, so you'd need the CURLOPT stuff to not check the peer stuff.

I don't imagine using SSL without trusted CA.

How secure is secure enough?
Depends what your data and application are, more than any external factor.

I cannot speak about the kind of data I have to protect on a public ML but data are confidential and I have to propose something to guaranty a vulnerability of the application doesn't expose all the data to the cracker.

I'd also consider curl before FTP, personally, as it is more flexible if you decide later to use something other than the FTP protocol.

You are right.

>> It depends more on what you are trying to secure, and why, than it
>> does on any sort of general principle, really... And just personal
>> preference on how to do this sort of thing... And your performance
>> needs are a big factor, sometimes.
>
> Security is the major point (before performances).

It's not that simple...

Would you be happy with a web server that requires a human to review each HTTP request and sign off a form in triplicate before the HTTP response went out?

:) that's an idea.

Re: [PHP] Out source files

I maybe should add in the requirement that the service should be usable :)

Note: I don't mandate the service to be easy to use though. I fully accept constraints to access to the data if it's worth it.

- > The mains goal is to be still protected if their is an element under
- > attack on the application server, for instance a vulnerability in
- > apache (or even php according to the March month ;).

What data are you protecting?

See above.

It's not just the picture of my last week-end (I don't even host images ;) !

- > I want to be protected against:
- > – cracker uploads a file and use a vulnerability to execute it on the
- > server (I can avoid it with a partition mounted without exec rights or
- > with another server that hosts the files).

Sure.

Or you could just put them outside the webtree and not write stupid PHP code that lets them get executed.

An attacker can use a vulnerability of either apache or php to gain apache user rights and make files executable and even run it (or run it with another vulnerability in another application required on the server).

And you could check the upload files for validity, to insure that they meet certain criteria of non-executable files in the first place.

Unfortunately, I cannot restrict the file type I accept. I would say that one of the goal of the application is to delivery binaries (executable).

- > – cracker uses a vulnerability and obtains the same rights than the
- > web server (due to mod_php) she will be able to access to all the
- > files (at least in read mode) because the user who runs apache have to
- > be able to read them.

Is this on a shared server?

Re: [PHP] Out source files

No it's not.

We are talking about a dedicated box in a DMZ with all the network security devices tailored.

Is your PHP binary reading script dumb enough to allow them to access the files they shouldn't be accessing?

I don't think so (code was audited) but I cannot guaranty there is no bugs in my application.

> There are probably other things I don't imagine but I think the usage
> of another server to host data is a good approach.

I think it's a great approach, if the data being secured warrants it and the web application is well-written.

I think it's a waste of time if the data being secured is not worth securing or the PHP script is so badly-written that jumping through the second-server hoop is no barrier at all, or, worse, opens up even MORE vulnerabilities.

I fully agree with you.

I (still) have no idea which camp you are in, no offense intended.

I see no offense at all. You ask the right question and with the little information I gave to you, you cannot assume what my context is.

I try to explain a bit more:

- It's an enterprise context and data are worth to protect them.
- I have an existing application used to share data per groups of users.
- Obviously, people from one group must not have access to data of the other group (I can have a lot of groups).
- I trust the security model of this application.
- The application already follow common security rules for PHP apps that server files:
 - data not in the application tree.
 - apache don't have direct access to the files
 - we enforce the files to be not executable.
 - ...

My main question is "What happens if there is bug in my application, if someone exploit a vulnerability of php or apache?".

Re: [PHP] Out source files

Re: [PHP] Out source files

First threat:

Due to the usage of PHP as an apache module, a vulnerability in one of these 3 elements can let cracker by pass the application security model (by pass the group access rights) because I cannot have protection at the OS level (because to be able to server the file for all groups my application must be able to read all the data whatever the protection is).

Second threat:

As I already explained, a cracker could upload with standards procedure a dangerous executable and with some vulnerabilities makes it executable and runs it.

I hope this clarify my needs,
regards,
Manuel

.