

## Re: OT: security

---

*Source:* <http://coding.derkeiler.com/Archive/PHP/comp.lang.php/2007-10/msg00807.html>

---

- *From:* "Rik Wasmus" <[luiheidsgoeroe@xxxxxxxxxxxx](mailto:luiheidsgoeroe@xxxxxxxxxxxx)>
  - *Date:* Sun, 14 Oct 2007 20:24:43 +0200
- 

On Sun, 14 Oct 2007 19:57:59 +0200, <[william.hooper@xxxxxxxxxx](mailto:william.hooper@xxxxxxxxxx)> wrote:

I also trying to get my hear around:

<http://www.attackers-r-us.com/nastycode>

This translates to <http://www.attackers-r-us.com/nastycode.php> and with `allow_url_fopen` enabled, this remote file will be included into the script and executed. Note that the remote server would have to serve php files as the raw script, instead of processing them with a PHP module first, in order for this attack to be effective, or a script would have to output PHP code ( `readfile(realnastycode.php)` for instance).

Mechanisms such as the above allow attackers to execute any code they desire on vulnerable web systems.

One simple way to prevent this style of attack is to disable `allow_url_fopen`. This can be set in `php.ini`.

The last part is totally over the top. And it is of no concern to you: it would only be a risk if you can have code that includes that code somewhere on your server, which is what must and can be prevented in the first place.

You have to consider what kind of files you want to allow (for instance, only images would easily be checked wether or not `getimagesize()` can make sense of it as an image. Preferably you can validate the types of file you want to allow.

Somewhat less reliable but OK for starters: find out what kind of file-extentions can be executed on your system (`.php`, `.php3`, `.php4`, `.php5`, `.inc`, `.pl`, etc...), and disallow files with that extention to stored. Having some evil code in `randomfile.blup` won't matter as it will never be recognized by the webserver as such, so it won't be executed.

—  
Rik Wasmus

.