

## CUNY Academic Commons - Feature #2695

### Create Private File Uploads for Blogs

2013-08-11 01:11 PM - Matt Gold

<b>Status:</b>	Resolved	<b>Start date:</b>	2013-08-11
<b>Priority name:</b>	Normal	<b>Due date:</b>	
<b>Assignee:</b>	Boone Gorges	<b>% Done:</b>	0%
<b>Category name:</b>	WordPress (misc)	<b>Estimated time:</b>	0.00 hour
<b>Target version:</b>	1.10		
<b>Description</b>			
As noted on the wp-edu listserv and discussed via email by Matt and Boone, WordPress blogs can be made private, but file uploads are still accessible via direct link, and google apparently indexes PDFs uploaded in that way. This seems like an important oversight with consequences for user privacy. My suggestion was that there be a way for users to trigger a private file upload process during upload that stores files in a more private way (thus avoiding a solution where something is done to make all site files, including images, etc., private, which could slow down site speeds and cause needless annoyances), but Boone notes that fixing this would require an overhaul of how WP handles file uploads. Creating this ticket for future thoughts on the subject.			
<b>Related issues:</b>			
Related to CUNY Academic Commons - Feature #6332: Allow uploaded files to be ... <b>New</b> <b>2016-10-17</b>			

#### History

##### #1 - 2014-06-20 12:20 PM - Matt Gold

I cannot understand how/why this hasn't been addressed in WP core yet. Isn't this a major privacy vulnerability?

##### #2 - 2014-06-20 12:25 PM - Boone Gorges

There is no functionality in WordPress to make a blog private. We add this functionality with the More Privacy Options plugin. That's the first reason.

Limiting file access to logged-in users means diverting all downloads through the WordPress application, rather than letting the fileserver serve them directly. That can create an enormous increase in server requirements, since a single pageload might load WP dozens of times (for each image). This is a second reason.

WordPress also has to deal with a number of different server environments (various versions of Apache, Nginx, IIS, and so forth), all of which handle file protection in different and incompatible ways. On some of these setups (Nginx in particular), there simply is no way to block files in a way that's ad hoc and determined by the PHP application. All such config has to happen at the server config level, which is inaccessible to WP. This is another reason for there being no general solution for this in WP (or elsewhere). Obviously, this is not so much an issue for a site like the Commons, which runs in a specific webserver environment.

##### #3 - 2015-11-09 06:21 PM - Boone Gorges

- Target version changed from Future release to 1.10

I have the beginnings of a tool that I built for the City Tech OpenLab. It automatically protects blog uploads based on the privacy setting of the blog where they're uploaded. It doesn't allow for per-upload or per-post privacy levels for attachments, but it's better than nothing.

##### #4 - 2015-11-12 12:53 AM - Matt Gold

Thanks, Boone. This does sound promising.

##### #5 - 2016-10-17 11:39 PM - Boone Gorges

- Status changed from Assigned to Resolved

I've just spent some time revisiting this.

The solution on the OpenLab has two parts:

1. A plugin I wrote, called dlblock, dynamically generates an .htaccess file that disables direct access to uploaded files belonging to sites with `blog_public < 0`.
2. A custom file handler that replaces `ms-files.php`, and checks each site's `blog_public` before serving `/files/` content.

After some investigation, it looks like 1 is not necessary on the Commons. We don't allow direct access to any of our files: the regex that we currently have in .htaccess catches any request that contains `/files/`, which includes `foo.commonsgc.cuny.edu/files/bar.jpg` **and** `foo.commonsgc.cuny.edu/wp-content/blogs.dir/1234/files/bar.jpg`. So it's enough to write the logic into our own custom file handler, which already exists for the purpose of forum attachment protection.

I've added the protection in <https://github.com/cuny-academic-commons/cac/commit/fac72ac38fa0b63650ebc26e7bf36e41f7d7ff61>. This feature should get a bit of testing by the community team in the lead-up to release, but I think we can mark it resolved until that happens. (I'll open a separate ticket for the more complicated question of how to protect specific uploads in an ad hoc way.)

**#6 - 2016-10-18 09:45 AM - Matt Gold**

This is great, Boone -- thank you!!!

**#7 - 2019-07-18 02:42 PM - Boone Gorges**

- *Related to Feature #6332: Allow uploaded files to be marked as private in an ad hoc way added*