CUNY Academic Commons - Bug #2338

commonsinabox.org PM spam

2012-12-10 02:59 PM - Boone Gorges

Status:	Resolved	**Start date:**	2012-12-10
Priority name:	Normal	**Due date:**	
Assignee:	Boone Gorges	**% Done:**	0%
Category name:	commonsinabox.org	**Estimated time:**	0.00 hour
Target version:	Not tracked		

Description

Last night a spammer signed up for commonsinabox.org and sent out some spam PMs. I'd like to have a brief discussion here about how to avoid this in the future, and deal with it when it does happen. The immediate concern is commonsinabox.org, but if there are general takeaways for Commons In A Box, let's discuss that too.

First, I do have in place a couple lines of defense against bot-spammers on commonsinabox.org. I changed the signup slug from 'register' to 'signup'. I installed a simple honeypot plugin (the one written by Pixel Jar). And I extended the honeypot to do some are-you-human checking, using a couple of questions. Here's the code, which the devs should have access to: https://github.com/cuny-academic-commons/commonsinabox-org/blob/master/wp-content/mu-plugins/buddypress-honeypot.php I think that this is about as good as we're going to get in terms of blocking bot spam, though I'll be happy to hear Ray and Bowe's thoughts about it. (Also, I'd be happy to hear your thoughts about whether adding something like this to Commons In A Box is a smart idea.)

My guess is that last night's spammer was not a bot, but was an actual human being, maybe a Mechanical Turk type of thing. As long as we have open registrations, we leave ourselves open to this sort of thing.

A couple ideas for mitigating damage:
- Disable PMs - are they really useful on commonsinabox.org?
- Require that users be signed up for a certain period of time before being able to send PMs. Or some other minimum number of friends, amount of activity, etc
- Disable email notifications of PMs

Other ideas?

Finally, when we do get hit with spam like this, we should have a cleanup policy. I see that someone has already deleted the user. In the future, it would be nice just to mark the user as Spam, so that the user remains in the database. As far as the spam content, I can easily delete all the spam PMs from the database, but then I should also delete the "You have a new message" notifications. And if I delete them both, people who click through on the links in their emails will see a 404, which might be more confusing than having the spam PM.

History

#1 - 2012-12-10 03:01 PM - Boone Gorges

- Status changed from New to Assigned

#2 - 2012-12-10 06:13 PM - Raymond Hoh

I've written a PMs for Friends Only plugin:
http://wordpress.org/extend/plugins/buddypress-private-message-for-friends-only/

It's a little old, but I've heard reports that it still works. Could use some testing. Could be extended to add some additional features as well.

#3 - 2012-12-10 06:27 PM - Boone Gorges

That's a thought. The problem is that friend notifications can be as much of a pest as spam PMs, at least if they're coming from spammers. But I guess it's a deterrent, like nofollow etc. Ray, maybe you could give your plugin a quick test against the latest cbox to see if it's working OK, and we can throw it up on commonsinabox.org (and discuss separately whether it should be a cbox plugin)

#4 - 2012-12-10 06:38 PM - Matt Gold

Thanks, Boone. A few thoughts:

-- I have no problem disabling PMs or restricting them to users who have been members for a certain amount of time
-- I think it's too early to move to a system where we we require approval of registration, but we may want to reevaluate the idea of open registration if this becomes consistent problem

-- Good points on the cleanup policy.
-- Can you replace the actual text of the spam messages (as viewed on the website) with some kind of notice that this was spam content, please ignore?

#5 - 2014-05-06 11:27 AM - Boone Gorges

- Status changed from Assigned to Resolved

The Messages component has been disabled on commonsinabox.org for some time now. I haven't heard any complaints.

As for other sorts of spam, let's please handle them on a case-by-case basis. When you find a spammer, please report it to me or to Scott, and we can do any necessary investigation before marking the user as a spammer and doing whatever cleanup is necessary. That seems like enough policy for the moment (given that it's not a huge problem). Thanks to all.