

Re: [PHP] Spam Post Defense / ID spam form posts

Source: <http://coding.derkeiler.com/Archive/PHP/php.general/2007-08/msg01244.html>

- *From:* stuttle@xxxxxxxxxx (Stut)
 - *Date:* Fri, 24 Aug 2007 10:31:50 +0100
-

Instruct ICC wrote:

Because that means messing with the recipient list – that's donkey work your client should do, hence my use of reply-to-all.

Wouldn't gmail thread it but still have 2 copies?

I could send email TO/CC/BCC the list to a specific folder, but I'd still get the copy to me directly in another folder. What should I train my donkey to do? I reply to all, then I only let the list address survive and make sure it is in the TO field.

If your mail client can't resolve two copies of the same email down to one, change your mail client.

Attacking a server with the express intention of preventing it from working correctly is in most countries. It's the technological equivalent of getting prosecuted for assault because you defended your property from a burglar.

Now I'm thinking I should inform the attacking server of the situation by shutting them down until they address the issue. It may need new laws on the books to cover my ass. But what do you think? Either a "YOU'VE BEEN PWND BY THE GUARDIANS because you are either running hijacked services for an attacker, (likely on an MS Windows flavor -- upgrade your OS to a non-MS OS), or you are the actual attacker. When you patch your security holes, THE GUARDIANS will consider your petition to re-enter the superhighway." or some such. If the HTTP_USER_AGENT hasn't been spoofed, they all seem to be Opera/9.0 (Windows NT 5.1; U; en), since I began tracking. If the server could be shutdown and reported to an authority that would re-evaluate their access to the net, it could help catch the attacker or in the least, stop attacks on other "innocents".

Well, if the hijacked service is down, it will "hurt" the attacker. If the "innocent's" server is down, they could learn about the need to be a better net citizen while at the same time not providing services to the attacker.

I'm assuming (and hope) you're being somewhat sarcastic, but you seem to misunderstand where these "attacks" are coming from. Most will not be coming from other servers, but from desktop machines belonging to the Joe Bloggs of this world. Bringing down their machines just because they were ignorant enough to get compromised seems like cruel and unusual punishment to me.

Re: [PHP] Spam Post Defense / ID spam form posts

You're essentially talking about needing a license to use the Internet. This has been talked about before on this list and all over the 'net, but it will likely never happen because it goes against the principles upon which it has been built and the people involved in running the core infrastructure.

The point I was trying to make is that your first step should be to find out why he has that position, educate him as to the benefits of the CAPTCHA and the complications that any other approach might have.

He holds that position because he does not want the user to have to enter any additional keystrokes or mouse clicks (or think more?) while they are becoming a sales lead. Not unlike your repulsion to cut and paste to send only to the list perhaps?

I don't have a repulsion toward modifying recipient lists, but I send too many emails to be bothered to do it. My toolset works, it de-dupes correctly and I've never had a problem with other people sending an email to several addresses that end up at the same mailbox.

Now, to get back to your original question... I now understand that this form you're dealing with is a contact form on a website? Your solution is simple. Put a note above the form stating that they cannot send URLs, HTML or BBcode. Then in your form handler check the following...

- * Single line fields do not contain carriage returns (used by spammers in an attempt to inject their own headers in emails)
- * No fields contain URLs, HTML or BBcode.
- * If you're asking for an email address check it against one of the many regular expression patterns out there.

You may also want to consider naming your form fields non-descriptively. For example, if you call the email field email an automated bot will know to put an email address in there. If you name it field2 it won't and your email address validation will catch it out.

With those steps you can easily cut out the majority of spam that will come through a contact form.

-Stut

<http://stut.net/>

.