

Re: Email Forms – Blocking Spammers

Source: <http://coding.derkeiler.com/Archive/PHP/comp.lang.php/2004-10/1101.html>

From: Gordon Burditt (gordonb.7tqgp_at_burditt.org)

Date: 10/20/04

Date: 20 Oct 2004 02:08:58 GMT

*>As far as I know, spammer's aren't scouring the web for feedback /
>contact-us forms.*

Spammers seem to find insecure versions of programs like "formmail" with frustrating rapidity.

*>I moved to a "email form" and haven't gotten any
>spam from it. Likewise, I moved my employer's email to a "form" and
>they haven't gotten any spam either.*

The threat here is using your web server to spam the world, incidentally getting mail from the web server blocked by a lot of ISPs. They don't usually spam the webmaster as that would give away the security hole.

One of the most important things about your form is: DON'T allow input from the browser to specify a destination address. DON'T put the To: address in a hidden field on the form. DON'T put the To: address in a cookie. Preferably, hard-code it as a fixed string that points at one of YOUR mailboxes.

Also: DON'T allow input from the browser to specify a From: address. (It's better to make that a fixed string, also.) DON'T allow input from the browser to do anything to the headers or body that might cause a bounceback to the From: address (e.g. attach a virus, excessive length, cusswords, etc.)

DON'T mail something back to an email address entered on a form.

You can relax some of these rules if using the form requires a login and a password that can't be obtained just by filling in another form (e.g. it waits a few days for the credit card payment to clear before permitting use).

Gordon L. Burditt