

RE: Secure Form Script?

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-linux/2004-05/0020.html>

From: Bryce Porter (*bporter_at_heart.net*)

Date: 05/14/04

Date: Fri, 14 May 2004 16:40:30 -0500
To: "Stephen Samuel" <samuel@bcgreen.com>

Stephen,

Yes, Net::SMTP supports MIME just fine. I have not tested pushing a single line with a '.' on it to an array to be sent to \$smtp->data, but I do not think it would work like that.

Also, what if you call sendmail directly, but quote it wrong? Someone could send an email with '; cat /etc/passwd' or whatever they wanted in it, and have it be executed with the same permissions the script is running as. Directly executing anything is a big risk no matter how you look at it, as far as I'm concerned.

Regards,

Bryce Porter
Network Administrator
Heart Technologies, Inc.
bporter@heart.net
<http://www.heart.net/>
309.633.2800 Technical Support
309.634.2282 Direct
309.634.2382 Fax

-----Original Message-----

From: Stephen Samuel [mailto:samuel@bcgreen.com]
Sent: Friday, May 14, 2004 4:34 PM
To: Bryce Porter
Cc: focus-linux@securityfocus.com
Subject: Re: Secure Form Script?

Bryce Porter wrote:

> *Stephen,*
>
> *When calling a binary directly, you run a lot of risks, especially*
> *format string vulnerabilities.*

SecurityFocus Linux: RE: Secure Form Script?

>
> *I agree about using the fixed To: address, but I think he was originally*
> *wanting that to be flexible. If not, fixed is most definitely the way to*
> *go.*

My understanding is that he was looking for something to replace mailto: links and that didn't expose your email address to spammers, (and didn't allow spammers to hijack your server).

A fixed destination on the CGI helps towards both of those. At that point the only user-input that goes into the header should be the Subject: field -- and you can move that into the body if you want to.

Once you're dealing with the body, the only thing that you really have to worry about is making sure that you don't send a line with a bare '.'. From what I can see you may have to worry about the same thing with Net:SMTP .

From where I sit, feeding /usr/sbin/sendmail directly is pretty much the same as talking to localhost:25, and Net::SMTP is (if you're sending to/via localhost), just a prettied-up way of doing the same thing. (it doesn't even seem to directly support MIME).

It does, however, get more useful if you want to talk to a remote server and/or play a bit with the TCP/IP options, etc.

In my case, my CGI scripts punts the Email to a second script which does a bit more pre-processing, then calls sendmail with the result. It could have just as easily used Net::SMTP *and I may just play with doing that for the exercise).

--

Stephen Samuel +1(604)876-0426 samuel@bcgreen.com

<http://www.bcgreen.com/~samuel/>

Powerful committed communication. Transformation touching
the jewel within each person and bringing it to light.