Program: PHFTP
Version: 4.2 (latest)
Site: http://phftp.sourceforge.net/

Date: April 21, 2011
Credit: Stephen Cartwright <sgcartwr@ucalgary.ca>

Description: Unsanitized POST variables phpftp_host and phpftp_port resulting in XSS vulnerability.

Impact Analysis
A reflected XSS attack requires an external link such as an e-mail message to inject a crafted payload covertly [1]. XSS attacks may utilize GET variables or POST variables [3]. POST variables can be an ideal target for XSS since they are often forgotten by the developers and are less obvious since they are not displayed in the URI. There are several methods of attack that this kind of vulnerability facilitates. These include:

- Session Riding – session variables and authentication may be leveraged to harvest information from active sessions on the client or perform trusted actions [2].
- Information from cookes can be harvested via *document.cookie* [1].
- A fake form can be inserted to convince a user to input sensitive information. The information can then be sent to an external site and an un-altered request forwarded to make it transparent to the user [1].
- Arbitrary JavaScript can be executed. This allows for any attack that is possible via JavaScript. A keylogger for use in XSS attacks has even been proposed [4].

References
[1] The Open Web Application Security Project. Cross-Site Scripting (XSS). https://www.owasp.org/index.php/Cross-site_Scripting_%28XSS%29.
[2] Digger's Blog. How to defeat digg.com ...an introduction to session riding. http://4diggers.blogspot.com.
[3] ha.ckers.org. Exploiting Cross Site Scripting Through Post. http://ha.ckers.org/blog/20060814/exploiting-cross-site-scripting-through-post.
[4] ClsHack.it. Attack with XSS [keylogger,Forms-autocomplete grabber] POST/GET. http://www.clshack.it/en/attack-keylogger-form-autocomplete-xss-post-get-request.html.

NB: A form would be impersonated in much the same way.

Resolution:
The developers have been notified. I am waiting for a response in order to coordinate a disclosure plan with them.