[mwpugln is a spam user targeting Drupal sites - delete it! (http://www.sandon.it/node/19)](http://www.sandon.it/node/19)

Posted on: Thu, 08/16/2007 - 11:03 **By:** Administrator

Many Drupal sites are being accessed by a user named *mwpugln*. And googling a bit, I saw many administrators wondering what user it is. Well, it's not difficult to find out it's just a bot used to spam Drupal sites, adding comments containint links to the usual spam-advertised products. It looks to be a bot because it uses several different IPs scattered around the world:

56.0.84.23	United States Postal Service
59.106.23.152	SAKURA Internet Inc., Japan
61.164.50.27	ZHEJIANG Polytechnic University of Technology&Arts, China
125.46.36.223	China Network Communications Group Corporation, China
193.111.198.56	fast IT GmbH, Germany
194.202.236.102	UUNET, Great Britain
196.209.251.3	Internet Solutions, South Africa
201.216.247.77	NSS S.A., Argentina
202.74.244.13	Global Online Services Limited, Bangladesh
202.96.189.45	CHINANET Guangdong province network, China
221.1.217.169	CNCGROUP Shandong province network, China
222.139.214.146	CNCGROUP Henan province network, China

(these data are from my logs, and do not imply any of IP owners endorses the spammer, IPs may be sub-assigned and could belong to compromised machines, whois as of 2007-08-16) It's just the usual spam technique to get more visibility in search engines. Unluckily, looking at Google many Drupal web sites have been left open to this spammer. If you find this user registered at your site, delete it and create an access rule to block it.

Lately I also find other kinds of bots, a couple trying to exploit the Drupal contact form, one from a mail sender named Sandra-xx , where xx changes from message to message, another using sender addresses containing the string *openbsd*. Another bot tried to create several users with more sensible names (i.e. ThomasYoung, NicholasMoore), all using email addresses made using a bird name + a number, all @yandex.**ru**, a bit uncommon for all this [WASP (http://en.wikipedia.org/wiki/White_Anglo-Saxon_Protestant)](http://en.wikipedia.org/wiki/White_Anglo-Saxon_Protestant) looking names to use a web site in Cyrillic ;) The increasing popularity of Drupal sites will make them more appealing to spammers as well. My advice is approve new users (if your site is not large), and to use the [captcha module (http://drupal.org/project/captcha)](http://drupal.org/project/captcha) where possibile - let's keep the Internet clean :)

* [Log in (http://www.sandon.it/user/login?destination=/comment/reply/node/19/comment_node_blog%23comment-form)](http://www.sandon.it/user/login?destination=/comment/reply/node/19/comment_node_blog%23comment-form) to post comments

Source URL: *http://www.sandon.it/node/19*