

[UNIX] myPHP Forum Unauthorized Access

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-03/0089.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 03/22/05

To: list@securiteam.com

Date: 22 Mar 2005 10:07:43 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

myPHP Forum Unauthorized Access

SUMMARY

" <<http://www.myphp.ws/>> MyPHP Forum, an easy to set up and easy to use MySQL and PHP based forum. It is distributed freely under the GPL license. It was made generally for use on small to medium sized websites which need a clean and efficient forum but without all the bloat that generally comes with other forums."

Lack of validation checks allows myPHP forum user to create new categories and invisible topics. You can also probably hide entire forum on somebody else's site.

DETAILS

Vulnerable Systems:

* myPHP Forum versions 3.0 and prior

Both `forum.php` and `topic.php` files have no validation checks. They are wide open. When visiting forums, click a forum category. In the URL bar, you'll see "fid=n", where n is the topic number. You can change this value to whatever value you want, for example, "fid=999999999".

This will create a new empty forum folder that allows you to click the

Securiteam: [UNIX] myPHP Forum Unauthorized Access

"new topic" link. This means that you can insert a message into forum "99999999" ... while this forum doesn't even exist in the forum index.

The same stands for topic.php. If you click a topic, you'll see "tid=n". It is possible to post topics with arbitrary id numbers, thus hiding them inside the forum.

ADDITIONAL INFORMATION

The information has been provided by <mailto:terencentanio@root32.com> Terencentanio Enache.

=====

This bulletin is sent to members of the SecuriTeam mailing list.
To unsubscribe from the list, send mail with an empty subject line and body to:
list-unsubscribe@securiteam.com
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind. In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.