

[UNIX] phpBannerExchange Directory Traversal

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-03/msg00016.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 7 Mar 2006 19:23:47 +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>

phpBannerExchange Directory Traversal

SUMMARY

<<http://www.eschew.net>> phpBannerExchange is "a PHP/mysql script that allows virtually anyone with minimal knowledge of PHP, mysql and web hosting to run their own banner exchange. This script was inspired by some of the greatest ad rotation scripts on the Internet such as Webadverts and phpAdsNew". A vulnerability has been identified in phpBannerExchange 2.0, which may be exploited by remote attackers to access arbitrary files outside of the webroot directory.

DETAILS

Vulnerable Systems:

- * phpBannerExchange version 2.0

This flaw is due to an input validation error in the script "resetpw.php" that does not properly sanitize the user-supplied input, which may be exploited by remote attackers to retrieve arbitrary files from a vulnerable system.

Proof of concept:

Go to the lost password script (resetpw.php) and type in

[UNIX] phpBannerExchange Directory Traversal

../../../../../../../../etc/passwd as your email address. This shows us the contents of the /etc/passwd file of the system hosting the vulnerable script.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:Rahigley.1989@xxxxxxxxxx>> TiX.

The original article can be found at:

<<http://www.h4cky0u.org/advisories/HYSA-2006-004-phpbanner.txt>>
<http://www.h4cky0u.org/advisories/HYSA-2006-004-phpbanner.txt>

=====

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@xxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====
=====

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.