

[UNIX] JShop page.php Cross Site Scripting

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-08/0076.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 08/22/04

To: list@securiteam.com

Date: 22 Aug 2004 18:47:39 +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>

JShop page.php Cross Site Scripting

SUMMARY

JShop is "a e-commerce system designed for servers that support both PHP and MySQL. Featuring a wealth of features for high-end e-commerce systems, such as customer accounts, stock control and order processing, JShop is designed for those companies wanting to offer a greater level of service to their on-line customers".

Due to inadequate filtering of user provided data, a remote attacker can insert third-party content to the page returned to the users.

DETAILS

JShop inadequately filters incoming data of the xPage parameter, this allows attackers to insert HTML and/or JavaScript to the data sent back to the user.

Example:

[http://vulnerable/page.php?xPage=>alert\(document.cookie\)</SCRIPT>](http://vulnerable/page.php?xPage=>alert(document.cookie)</SCRIPT>)

ADDITIONAL INFORMATION

The information has been provided by <<mailto:drponidi@hackermail.com>> Dr

Securiteam: [UNIX] JShop page.php Cross Site Scripting

Ponidi.

The original article can be found at:

<<http://indohack.sourceforge.net/drponidi>>

<http://indohack.sourceforge.net/drponidi>

=====

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.