

# [UNIX] Private Message System XSS

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-01/0004.html>

---

**From:** SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

**Date:** 01/01/04

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 1 Jan 2004 12:30:10 +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>

-----

Private Message System XSS

---

## SUMMARY

This based PHP script Private Message System (PMS), suffers from a Cross Site Scripting vulnerability. This can be exploited by including arbitrary HTML or even JavaScript code in the parameter "page", which will be executed in user's browser session when viewed.

## DETAILS

Vulnerable systems:

- \* PMS version 2.2.9 and prior

Immune systems:

- \* PMS version 2.3.0 and newer

Example:

[http://host/index.php?page=%22%3E%3Cscript%3Ealert\(document.domain\);%3C/script%3E](http://host/index.php?page=%22%3E%3Cscript%3Ealert(document.domain);%3C/script%3E)

Solution:

Upgrade to the latest version 2.3.0 or newer.

## ADDITIONAL INFORMATION

Securiteam: [UNIX] Private Message System XSS

The information has been provided by <mailto:iamroot@systemsecure.org>  
David S. Ferreira.

=====

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.