

Securiteam: [UNIX] phpBB Still Suffers From a Cross Site Scripting Vulnerability (Edit)

[UNIX] phpBB Still Suffers From a Cross Site Scripting Vulnerability (Edit)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-03/0106.html>

From: support@securiteam.com

Date: 03/23/02

From: support@securiteam.com

To: list@securiteam.com

Date: Sat, 23 Mar 2002 22:24:38 +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.

phpBB Still Suffers From a Cross Site Scripting Vulnerability (Edit)

SUMMARY

After a similar bug was discovered in phpBB 1.4.2, the authors fixed the bug that would allow JavaScript to be inserted by using an [IMG] tag like:
[img]javascript:alert('bla')[/img]

But there was only a check for that only when you posted new messages. If you just edit an existing message, you still can use the bug to insert JavaScript.

DETAILS

Vulnerable systems:
phpBB version 1.4.4

There is no check in the edit function of phpBB 1.4.4 whether JavaScript or other unwanted code is written within IMG-tags.

Exploit:

Create a new topic or answer to an existing one. Then, after posting your message, click on the "edit button" and enter anywhere in your posting:

Securiteam: [UNIX] phpBB Still Suffers From a Cross Site Scripting Vulnerability (Edit)

[img]javascript:alert(document.cookie)[/img]

After posting the message, you should see the contents of the cookie matching to the site you are visiting at the moment.

Solution:

Update to newer versions (phpBB2 seems not to be vulnerable) or just implement a routine which checks if at the beginning of [IMG]-tags stands a "http://".

ADDITIONAL INFORMATION

The information has been provided by
<mailto:BlueScreen@IT-Checkpoint.net> BlueScreen.

=====

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: "[EXPL] Exploiting the Zlib Bug in OpenSSH"
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)