

[UNIX] Yabbse XSS Vulnerability in news_template.php (threadid, msgid)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-01/0018.html>

From: support@securiteam.com

Date: 01/05/03

From: support@securiteam.com

To: list@securiteam.com

Date: 5 Jan 2003 16:52:23 +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

Beyond Security would like to welcome Tiscali World Online to our service provider team.

For more info on their service offering IP-Secure, please visit http://www.worldonline.co.za/services/work_ip.asp

Yabbse XSS Vulnerability in news_template.php (threadid, msgid)

SUMMARY

<<http://www.securiteam.com/unixfocus/5BP061F8US.html>> YaBB SE is a PHP/MySQL port of the popular forum software YaBB (yet another bulletin board). A cross site scripting vulnerability in the product allows a remote attacker to cause the web page to insert malicious HTML and JavaScript into existing web pages.

DETAILS

Vulnerable systems:

* Yabbse version 1.5.0

Examples:

[http://victim/yabbse/index.php?board=1;action=display;threadid=1>alert\(document.cookie\)</S!cript>](http://victim/yabbse/index.php?board=1;action=display;threadid=1>alert(document.cookie)</S!cript>)

<http://victim/yabbse/index.php?board=1;action=reporttm;thread=1;id=0;subject=Welcome%20to%20YaBB%20SE!;p>

Impact:

This can allow attackers to steal Yabb's cookies from other users and hijack their accounts.

Securiteam: [UNIX] Yabbse XSS Vulnerability in news_template.php (threadid, msgid)

ADDITIONAL INFORMATION

The information has been provided by <mailto:nmsh_sa@yahoo.com> NaSsEr M.Sh.

=====

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.