

[UNIX] XOOPS Quiz Module IMG Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-11/0091.html>

From: support@securiteam.com

Date: 11/24/02

From: support@securiteam.com

To: list@securiteam.com

Date: 24 Nov 2002 23:17:17 +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

XOOPS Quiz Module IMG Vulnerability

SUMMARY

The XOOPS Quiz Module allows users to post pop quizzes online, a vulnerability in the module allows remote attackers to insert malicious HTML and JavaScript code into the quiz.

DETAILS

If the moderating/administrator of this module allows the online development of questions, he takes a risk that someone will post something like this:

```
<IMG SRC="javascript:alert('blocus-zone')">
```

 placed in a multiple answer.

(Note that the code that we have a presented here is not dangerous, however there are some codes much more malicious)

To verify questions elaborated by his member, the moderator or admin goes to visualize before the proposal, even then, a pop up creates a page in his final form to give a visualization to the approver of questions/quiz, and this cause automatically the bug on browser, without that the administrator or the moderator have not been able to perceive him before.

Securiteam: [UNIX] XOOPS Quiz Module IMG Vulnerability

ADDITIONAL INFORMATION

The information has been provided by <mailto:magistrat@blocus-zone.com>
magistrat.

=====

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.