

[UNIX] XOOPS myheader.php Cross Site Scripting Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-12/0083.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 12/24/03

To: list@securiteam.com

Date: 24 Dec 2003 15:04:12 +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>

XOOPS myheader.php Cross Site Scripting Vulnerability

SUMMARY

<<http://www.xoops.org/modules/news/>> XOOPS is "a dynamic OO (Object Oriented) based open source portal script written in PHP. XOOPS supports a number of databases, making XOOPS an ideal tool for developing small to large dynamic community websites, intra company portals, corporate portals, weblogs and much more". The weblinks module contains a file named "myheader.php" in /modules/mylinks/ directory, this module contains a cross-site scripting vulnerability.

DETAILS

Vulnerable systems:

* XOOPS version 2.0.5.1

Vulnerable code:

The code of the file is as follow:

```
include "../mainfile.php";
$url = $HTTP_GET_VARS['url'];
$lid = intval($HTTP_GET_VARS['lid']);
.
```

Securiteam: [UNIX] XOOPS myheader.php Cross Site Scripting Vulnerability

```
.  
.br/>< td class='bg4' align='center'><small>  
< a target='main' href='ratelink.php?cid=<? echo $cid; ?>&lid=<? echo  
$lid; ?>'><? echo _MD_RATETHISSITE; ?></a> | < a target='main'  
href='modlink.php?lid=<? echo $lid; ?>'><? echo _MD_MODIFY; ?></a> | < a  
target='main' href='brokenlink.php?lid=<? echo $lid; ?>'><? echo  
_MD_REPORTBROKEN; ?></a> | < a target='_top' href='mailto:?subject=<? echo  
$mail_subject; ?>&body=<? echo $mail_body; ?>'><? echo _MD_TELLAFRIEND;  
?></a> | < a target='_top' href='<? echo XOOPS_URL; ?>'>Back to <? echo  
$xoopsConfig['sitename']; ?></a> | < a target='_top' href='<? echo $url;  
?>'>Close Frame</a>  
</small>  
.br/>.
```

The value for variable "url" is used in line `< a target='_top' href='<? echo $url; ?>'>Close Frame` without being sanitized. Thus, an attacker can pass a JavaScript code as a value for variable 'url' and get it executed as soon as the victim clicks the "Close Frame" link.

Exploit:

By clicking on the link:

`http://[target]/modules/mylinks/myheader.php?url=javascript:alert(document.cookie);`, the victim gets directed to a page containing a link "Close Frame" which is actually the JavaScript code inserted by the attacker. A cookie captured can be used by an attacker to login with the hijacked user's (including admin) privileges.

ADDITIONAL INFORMATION

The information has been provided by `<mailto:chesschintan@hotmail.com>`
Chintan Trivedi.

=====

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.