

[UNIX] Moodle Cross Site Scripting Vulnerability (post.php)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-08/0038.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 08/11/04

To: list@securiteam.com

Date: 11 Aug 2004 18:02:45 +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>

Moodle Cross Site Scripting Vulnerability (post.php)

SUMMARY

" <<http://www.moodle.org>> Moodle is a course management system (CMS) – a software package designed to help educators create quality online courses."

Moodle suffers from a cross-site scripting vulnerability due to handling of user supplied parameters in an unsafe manner.

DETAILS

Vulnerable Systems:

- * Moodle versions 1.3 and prior

Immune Systems:

- * Moodle version 1.3.3

The cross-site scripting (XSS) vulnerability is caused by un-filtering the \$reply variable. Here is an excerpt from the original code:

```
/* Begin of vulnerable code */
```

Securiteam: [UNIX] Moodle Cross Site Scripting Vulnerability (post.php)

```
} else if (isset($reply)) { // User is writing a new reply

    if (!$parent = forum_get_post_full($reply)) {
        error("Parent post ID was incorrect ($reply)");
    }
    if (!$discussion = get_record("forum_discussions", "id",
$parent->discussion)) {
        error("This post is not part of a discussion! ($reply)");
    }
    if (!$forum = get_record("forum", "id", $discussion->forum)) {
        error("The forum number was incorrect ($discussion->forum)");
    }
    if (!$course = get_record("course", "id", $discussion->course)) {
        error("The course number was incorrect ($discussion->course)");
    }

    if (!forum_user_can_post($forum)) {
        error("Sorry, but you can not post in this forum.");
    }

    if ($cm = get_coursemodule_from_instance("forum", $forum->id,
$course->id)) {
        if (groupmode($course, $cm) and !isteacheredit($course->id)) { //
Make sure user can post here
            if (mygroupid($course->id) != $discussion->groupid) {
                error("Sorry, but you can not post in this discussion.");
            }
        }
        if (!$cm->visible and !isteacher($course->id)) {
            error(get_string("activityiscurrentlyhidden"));
        }
    }
}

/* End of vulnerable code */
```

The bug can be specifically traced to the following snippet of code:

```
if (!$parent = forum_get_post_full($reply)) {
    error("Parent post ID was incorrect ($reply)");
}
```

A proof of concept HTTP request that will pop up an alert dialog in the victim's context:

[http://www.vulnerable.com/moodle/mod/forum/post.php?reply=%3Cscript%3Ealert\(document.cookie\);%3C/script%3E](http://www.vulnerable.com/moodle/mod/forum/post.php?reply=%3Cscript%3Ealert(document.cookie);%3C/script%3E)

Vendor Status:

The vendor has been contacted and a new version is available for download.

ADDITIONAL INFORMATION

The information has been provided by <mailto:javierubilla@spymac.com>
Javier Ubilla Brenni.

Securiteam: [UNIX] Moodle Cross Site Scripting Vulnerability (post.php)

=====

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.