

[UNIX] XSS Vulnerability in MyMarket

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-10/0114.html>

From: support@securiteam.com

Date: 10/23/02

From: support@securiteam.com

To: list@securiteam.com

Date: 23 Oct 2002 23:36:37 +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

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.

XSS Vulnerability in MyMarket

SUMMARY

<<http://mymarket.sourceforge.net/>> MyMarket is a fully functional online shopping catalog system, built using PHP and MySQL. It was created by Ying Zhang for the purpose of teaching people about the basics of creating an E-Commerce site.

DETAILS

Vulnerable systems:

* MyMarket version 1.71

Exploit:

[http://\[traget\]/templates/form_header.php?noticemsg=<Scr*ipt>javascript:alert\(document.cookie\)</Scr*ipt>](http://[traget]/templates/form_header.php?noticemsg=<Scr*ipt>javascript:alert(document.cookie)</Scr*ipt>)

(without "*")

Solution:

Put this two lines at the begin of form_header.php

----- form_header.php -----

<?

```
$noticemsg = htmlspecialchars($noticemsg);
```

```
$errormsg = htmlspecialchars($errormsg);
```

Securiteam: [UNIX] XSS Vulnerability in MyMarket

...

Vendor response:

qber66 submitted this a week ago, the vendor didn't response yet.

ADDITIONAL INFORMATION

The information has been provided by <mailto:qber66@pandora.be> qber66.

=====
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: "[NT] FlashFXP Local Password Disclosure Vulnerability"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)