

# [UNIX] JShop Cross Site Scripting

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-01/0131.html>

---

**From:** SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

**Date:** 01/31/05

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 31 Jan 2005 09:12:08 +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>

-----

JShop Cross Site Scripting

---

## SUMMARY

<<http://www.jshop.co.uk/>> JShop Server is "a PHP and mySQL driven e-commerce system that can provide everything from customer accounts to gift certificates, from stock control to advanced pricing options, from reports and statistics to order management and dispatch tracking".

Due to improper filtering done by JShop an attacker can insert arbitrary HTML/JavaScript into the pages returned by the product.

## DETAILS

Vulnerable Systems:

- \* JShop Server version 1.2.0 and prior

Immune Systems:

- \* JShop Server version 1.3.0 or newer

A vulnerability has been identified in JShop Server, which can be exploited by malicious people to conduct Cross-Site Scripting attacks. The vulnerability is caused due to missing validation of input supplied to "xProd and xSec" parameters in "product.php". This can be exploited by including arbitrary HTML or script code in the parameters, which will

Securiteam: [UNIX] JShop Cross Site Scripting

cause it to be executed in a user's browser session when viewed.

Exploit:

<http://vulnerable/product.php?xSec=1&xProd=7>"><script>alert(document.domain);</script>  
<http://vulnerable/product.php?xSec=1>"><script>alert(document.domain);</script>&xProd=7

ADDITIONAL INFORMATION

The information has been provided by <mailto:smok3f00@gmail.com> SmOk3.

The original article can be found at:

<<http://www.systemsecure.org/wwwboard/messages/225.html>>

<http://www.systemsecure.org/wwwboard/messages/225.html>

=====

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.