

# [NT] ACS Blog Cross Site Vulnerability

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-03/0131.html>

---

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

**Date:** 03/28/05

To: list@securiteam.com

Date: 28 Mar 2005 10:17:33 +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>

-----

ACS Blog Cross Site Vulnerability

---

## SUMMARY

" <<http://www.asppress.com/index.asp>> ACS Blog is is free for personal, non-commercial use post manager."

A vulnerability found in ACS Blog, can be exploited by malicious people to conduct cross-site scripting attacks.

## DETAILS

Vulnerable Systems:

- \* ACS Blog version 1.1b and prior

Input passed to the "search" parameter in "search.asp" isn't properly sanitised before being returned to the user. This can be exploited to execute arbitrary code in a remote user's browser in context of the vulnerable site:

<http://example.com/search.asp?search=%22%3Cbr%3E%3Ciframe+src%3D%22http%3A%2F%2Fgoogle.com%22%3>

## ADDITIONAL INFORMATION

The information has been provided by <<mailto:farhadkey@yahoo.com>> farhad koosha.

Securiteam: [NT] ACS Blog Cross Site Vulnerability

=====

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.