

# [NEWS] PHP Authentication Suit for DreamWeaver XSS Vulnerability

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-08/0014.html>

---

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

**Date:** 08/05/03

To: list@securiteam.com

Date: 5 Aug 2003 14:30:34 +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

Get Thawte's New Step-by-Step SSL Guide for MSIS

In this guide you will find out how to test, purchase, install and use a Thawte Digital Certificate on your MSIS web server. Throughout, best practices for set-up are highlighted to help you ensure efficient ongoing management of your encryption keys and digital certificates. Get your copy of this new guide now: <http://ad.doubleclick.net/clk;5903126;8265119;j>

-----  
PHP Authentication Suit for DreamWeaver XSS Vulnerability  
-----

## SUMMARY

The

<[http://www.macromedia.com/software/studio/productinfo/devnet\\_resource\\_kit/](http://www.macromedia.com/software/studio/productinfo/devnet_resource_kit/)> PHP User Authentication Suite "consists of four server behaviors for restricting access to websites: Log In User, Restrict Access to Page, Log Out User, and Check New User Name". A vulnerability in the product allows remote attackers to include arbitrary HTML and JavaScript code into existing web pages (allowing them to capture existing and new sessions).

## DETAILS

Vulnerable systems:

\* DreamWeaver MX version 6.0

The XSS vulnerability is in the variable that returns the response whenever access has been denied:

[http://\[TARGET\]/\[PATH\]/\[LOGIN PAGE\].php?\[ACCESS DENIED](http://[TARGET]/[PATH]/[LOGIN PAGE].php?[ACCESS DENIED)

Securiteam: [NEWS] PHP Authentication Suit for DreamWeaver XSS Vulnerability

VARIABLE]=%2F[DIR1]%2F[DIR2]%2F[DIR3]%2F[FORBIDDEN PAGE]

Whenever access is denied to a certain site, you are redirected to a page where the [LOGIN PAGE] is included inside one of the variables being displayed.

Generic Example:

http://[TARGET]/[PATH]/[LOGIN PAGE].php?[ACCESS DENIED VARIABLE]="><script>alert('::\|\NSRG-18-7|\|/::');</script>

Site Specific Example:

<http://www.victim.foo/secrets/login.php?accessdenied=%2Fsecrets%2Findex.php> <- (/secrets/index.php)

Solution:

Replace in your login page code:

```
$FF_authFailedURL = $FF_authFailedURL .
$FF_qsChar . "accessdenied=" . urlencode($FF_referrer);
```

With:

```
$FF_authFailedURL = $FF_authFailedURL .
$FF_qsChar . "accessdenied=Your attempt was recorded";/\ \
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:novappc@novappc.com> Lorenzo Hernandez Garcia-Hierro.

=====

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.