

[UNIX] myPHPnuke SQL Injection (\$aid)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-09/0076.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 09/21/03

To: list@securiteam.com

Date: 21 Sep 2003 14:24:17 +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>

myPHPnuke SQL Injection (\$aid)

SUMMARY

<<http://sourceforge.net/projects/myphpnuke>> myPHPNuke is a content management system written in PHP. An SQL Injection vulnerability in the product allows remote attackers to insert malicious arbitrary SQL statements into those used by the product allowing compromise of the server and database.

DETAILS

Vulnerable systems:

* myPHPnuke version 1.8.8

Vulnerable code:

In the auth.inc.php file:

```
if ((isset($aid)) && (isset($pwd)) && ($op == "login")) {  
if($aid!="" AND $pwd!="") {  
$q="select pwd from ".$mpnTables['authors']." where aid='$aid';  
$result=mysql_query("select pwd from ".$mpnTables['authors']." where  
aid='$aid');  
list($pass)=mysql_fetch_row($result);  
if ($pass == $pwd) {  
$pwd1 = md5($pwd);
```

Securiteam: [UNIX] myPHPnuke SQL Injection (\$aid)

```
mysql_query("update ".$mpnTables['authors']." set pwd = '$pwd1' where
aid='$aid'");
$pass = $pwd1;
} else {
$pwd1 = md5($pwd);
}
if($pass == $pwd1) {
$admin = base64_encode("$aid:$pwd1");
setcookie("admin", "$admin", time()+2592000, "", "", ""); // 1 mo is
2592000
}
}
}
```

As you can see \$aid is not checked. Therefore, you can run the query like:
select pwd from mpn_authors where aid='mad' into outfile
'/filepath/file.txt'

When you enter:
aid=mad' into outfile '/filepath/file.txt'

Workaround:
This vulnerability will not work if magic_quotes_gpc is set to on.

Fix:
Find the line:
if ((isset(\$aid)) && (isset(\$pwd)) && (\$op == "login")) {
if(\$aid!="" AND \$pwd!="") {

And add to it:
\$aid=addslashes(\$aid);

ADDITIONAL INFORMATION

The information has been provided by <mailto:lifofifo20@yahoo.com> Lifo
Fifo.

=====

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.